AI, Machine Learning & Big Data

2020

Second Edition

Contributing Editor:
Matt Berkowitz

glg global legal group

CONTENTS

A Framework for Understanding Artificial Intelligence

By Contributing Editor: Matt Berkowitz
Shearman & Sterling LLP

In its simplest form, AI can be described as any intelligence that is exhibited by an artificial system. However, this definition includes everything from the capacity for pocket calculators to recall 10-digit numbers to the ability of drones to recognise and target enemy combatants in the haze of battle. So, how does the layperson practitioner cut through all of that to understand the potential ramifications of AI? And, perhaps, the more important question for practitioners is: how is AI going to change the legal challenges faced by the clients that they represent?

In this overview, we attempt to create a framework for understanding AI from the terminological and technological perspectives, while also touching upon the more immediate legal challenges that the technology poses to the legal practitioner. Although images of bipedal robots with human-like personas can be entertaining, the current advancements in technology provide some very real and immediate concerns relevant to the integration of AI into our society and its laws.

To begin assessing these challenges, we start with a framework to understand the current status of AI and its potential as a technology. We then move to a quick review of the current commercial uses of AI, and finally a cursory examination of the many legal issues that are currently in play for legal practitioners.

Understanding the basics of AI

AI is in and of itself a complex subject matter, with many subcomponents. Phrases like machine learning, natural language processing and neural networks are all technological subsets of AI designed to solve different problems. For example, machine learning technology can refer to a computer learning from interactions with a person in a game, while natural language processing enables computers to understand and extract concepts from random forms of language, and neural networks can be created to predict future outcomes or optimise processes.

It is also worth delineating the differences between assisted intelligence, autonomous intelligence and augmented intelligence. Assisted intelligence refers to AI systems that assist us in making decisions, but are unable to learn from our behaviour. A good example is the digitised steering or automated braking system of current commercial cars, each of which assists the driver in making rapid decisions based on predetermined programs and environmental inputs (*e.g.*, speed, weather conditions). Autonomous intelligence systems are those that can adapt to different situations and that can act autonomously without human assistance. Self-driving vehicles are the most obvious demonstration of applied autonomous intelligence. Augmented intelligence refers to technologies that expand human intelligence capacities and work alongside people while learning from interactions. Google search has vastly augmented the range of personal knowledge, while improving itself through human interactions.

The accessibility and exponential propagation of AI in a globalised environment with differing moral, legal and socioeconomic incentive systems presents many immediate tangible and disconcerting possibilities that need to be understood. Understanding that the development of AI can be constrained and regulated, and can be constructively channelled to advance civil society, helps us focus our efforts toward mitigating real and present dangers (*e.g.*, Cambridge Analytica's influencing of elections across Africa, Europe and North America) *versus* abstract dystopian or sci-fi outcomes.

A framework to understand the nomenclature and the environment in which AI develops helps to focus the legal discussion and analysis on relevant issues that require immediate attention by practitioners.

The rise of the machine

AI influences the way we travel, the knowledge we have access to, and even the way we date. It is unavoidable that AI-based products are disrupting business and everyday life, and will continue to do so in an increasing way in the years to come.

For example, the agriculture industry has found practical uses for AI. Bowery Farming, a vertical farming startup, uses AI innovations to improve efficiency, using light, temperature and humidity data to optimise growing conditions. The use of AI in agriculture is not without controversy, because there is growing concern on the effect of AI on the displacement of human labour. On the one hand, there is the question of job loss, but on the other, there is the potential benefit of resource-efficient and low-cost food production in a variety of environments.

The healthcare industry has also benefited from advancements in AI, which can utilise large amounts of patient data to improve diagnoses and treatment protocols. Freenome is a company that has made significant advancements in data analysis through liquid biopsies (tests performed on samples of blood to detect cancerous cells). Freenome utilises AI to not only detect cancerous cells, but also to identify whether the cancer is benign or malignant. The technology can also locate or provide the likely location of the cancer cell in the body.

Arterys is a company that developed the first FDA-approved cloud-based AI platform. The technology is being used to examine and analyse MRIs. Analysis of MRIs is a task that is often tedious and prone to human error. AI is used to create models based on large datasets of aggregated MRIs and associated prognoses. The models are then used to evaluate difficult-to-assess MRIs to diagnose patients.

The proliferation of satellite images and AI-based visual recognition technology has allowed for the highly accurate tracking of the movement and cargo of tankers to understand the state of various commodities' demand around the world. The output from the AI models allows commodity traders to understand real-time demand in ways that were never previously possible.

The above applications, along with the more obvious daily influences of AI-based internet marketing and personality-tailored news feeds, are illustrative of the fact that the machines are disrupting business as we know it. With that will come new problems, wrought with legal and ethical uncertainties.

Legal challenges associated with AI

The number and complexity of tasks handed over to AI systems will undoubtedly increase in the future. While this development creates wealth, AI will cause, and is indeed already causing, socioeconomic challenges and disruptions to the labour market, which will cause

the displacement and retooling of employees across almost all swathes of the economy. This phenomenon is not new; machines replaced human labour in manufacturing and agriculture during the industrial revolution, causing massive disruptions in the labour market and the concentration of wealth in a new upper class of industrial capitalists. The disruption likely to be caused to aggregate labour utilisation will bring greater focus on the value of human labour as a form of human activity, rather than merely being a means to efficiently achieve traditional capitalist production outcomes.

These previous technological advances during and since the industrial revolution have necessitated changes in the law, in order to optimise productive use of the new technology and minimise public risks caused by it. As an example, the invention of the car made transport faster, cheaper and more comfortable, while also introducing risks in the form of accidents and pollution. Lawmakers therefore faced the challenge of how to design *ex ante* regulations (such as car safety standards, regulations of manufacturer behaviour, testing procedures, emission standards, rules governing agencies responsible for regulating automobile traffic, etc.) and *ex post* regulations for when things have already gone wrong (criminal, tort and administrative rules specific to the driving and handling of cars), to make manufacturing and using cars as safe as possible without unnecessarily stifling innovation. By the same token, the enormous potential of AI and the public risks associated with it will necessitate changes in the law. Below are a few concrete examples of potential risks that will help to create a vivid picture of near-term concerns.

- *Harmful acts*: AI systems controlling physical objects may harm property or people as a result of intentional acts of the user, malfunction, flawed programming or unforeseen actions taken by the AI system. As early as 1981, a factory worker in Japan was killed by a robot. The robot deemed the worker's presence a threat to its mission and that the most efficient way to eliminate the threat was to pin the worker to the adjacent machine, which killed him instantly. In March 2018, the first fatal accident caused by a self-steering car took place. As drones, self-steering cars and other AI-controlled machines gain more autonomy, such risks will be aggravated.
- *Lack of privacy*: AI-driven technologies such as face, voice and behaviour recognition systems that can be connected to cameras and microphones make it possible to follow every step we take in real time, not just when we are using electronic devices. Already today in China, a social credit programme is being tested on a large scale, and in certain instances it is being integrated with highly focused governmental screening and security systems. The programme monitors the participants in real time and creates a "social credit score" based on data on everything from dating behaviour, friends, time spent working out, preferred newspapers and TV channels, smartphone usage, time and effort spent on raising kids, etc. The social credit score is then used for access to schools, ability to take out a mortgage, ability to travel and book hotels, etc.
- *Biased algorithms*: When AI is used as a decision-making tool based on statistical models applied to big data, there is a risk of discriminatory results if either the data or the statistical model, or both, contains a bias. For example, in hiring processes, AI algorithms have been used and found to generate results that are discriminatory against women. As AI becomes increasingly sophisticated, it is plausible to think that it could be used as a decision-making tool in police work, the judiciary, application processes to universities, generating credit scores and countless other examples.
- *Misinformation*: By gathering and analysing data about us, AI systems are able to tailor messages – true or false – that are designed to have maximal impact on our behaviour and opinions. Further, AI can create faces, voices, texts and tweets, and make such content

look as though it is from a particular source. While fake faces and voices are not perfect today, it is only a matter of time before AI systems will be able to fake messages from any person, creating possibilities such as the faking of entire political speeches, making them appear to come from real persons, distributing them via legitimate news outlets, and spreading them to the recipients most susceptible to such messages.

- *Hacking*: AI systems are getting continually better at hacking into systems and breaching encrypted environments. As this development continues, increasingly effective ransomware and other malware will be able to be spread on a massive scale. To counter this development, cybersecurity and encryption techniques must be improved at the same rate. As additional services become connected to the internet, they will become vulnerable to these types of attacks. It is easy to imagine scenarios in which malignant actors take control over self-steering cars to cause harm, or to cause hospital equipment to shut down pacemakers or other life-supporting technology.

As can be inferred from the above, while some of the concerns with AI are common to other technological advances, AI has features that make it more difficult to regulate than previous technologies. The globalised accessibility of the hardware, software/code and basic knowledge required to build successful AI technology in its many permutations has caused a revolutionary proliferation of its applications. This rapid and decentralised growth presents a fundamental challenge to regulating the technology effectively, without stifling the benefits of innovation.

The difficulty of regulating AI

Physical infrastructure made it relatively simple to locate the production of and the actors involved in many technologies. AI, on the other hand, can be developed by a single person or a small team with discrete and limited physical resources. Therefore, it is much easier to develop AI systems in a clandestine fashion than with previous potentially risky technologies. Further, AI systems can, and often are, developed using a combination of individual components (which may be open source, developed by anonymous persons and uploaded to sharing platforms), making all actors involved in the development of a particular AI system difficult to identify. A related issue is that while it may be relatively simple to observe the output of AI systems, it is often harder to understand the black box operation of an AI system or model. This kind of opacity makes it difficult to both identify who is behind the AI system and to assign responsibility for when things go awry.

Another feature of AI that makes it difficult to regulate is its ability to act autonomously, sometimes with unforeseeable results. While every AI system has an initial program containing the objectives of the AI system, the capability of the system to optimise solutions free of the cognitive constraints and biases of the human brain can lead the AI system to solve a problem in a manner unforeseeable even to its creators. This fundamental ability to act autonomously with unforeseeable results, sometimes outside the control of humans, creates difficulties in determining and allocating liability for harmful acts caused by AI systems.

Another fundamental question that is common to any regulation, but particularly difficult in relation to AI, is to define what should be regulated. As technological advances have been made, focus has shifted to definitions that emphasise a machine's ability to work independently and rationally toward goals. However, from a legal perspective, whether a machine is able to rationally pursue a "goal" is not much more specific than to say that a machine is "intelligent". One ambiguous word is simply replaced by another. Likely, a more detailed definition of AI would need to be developed that would be allowed to evolve over time and be derived from what is a desirable reach of the regulatory regime.

In spite of the difficult task, current regulation and modern legal models can be augmented or modified to provide for an effective foundation for the continued development of AI. In fact, such discussions are already under way. We touch upon some of them in this publication.

Models for tort liability

As illustrated, AI systems are capable of causing harm to persons and property. The current tort system is capable of providing remedies for actions taken by robots that make no decisions of their own, but simply follow direct orders of its programmers or users. In these cases, the machine is merely a tool through which the human instructor acts, and as such, the human could bear the burden of civil liability on behalf of the machine. However, if an AI system makes a decision independently of its creator or user and injures another person, it would be difficult under the current regime for the injured to get compensated.

For a successful negligence tort claim, the injured party must show that the defendant had a duty of care towards the injured person, that he or she breached that duty of care, and that the breach caused the injury. In the AI context, assessing the typical elements of a tort presents unique challenges, including how to determine reasonable foreseeability, and proximate causation. Also, when should strict liability apply? Should governments distribute risk by organising pools of money into which AI developers must contribute? Or require insurance? These issues have been widely discussed in the literature, but there is today no directly guiding case law on these matters.

Models for criminal liability

AI systems are capable of causing harm as a result of the developer or user programming or instructing the AI system to cause such harm in a manner that would warrant criminal liability. For example, a self-steering car could be programmed by its developers or instructed by its user to hit a pedestrian, causing physical injury. An AI system could also cause harm in a manner not intended by any human. The self-steering car could, for example, in certain situations calculate that the most efficient way of achieving its programmed objectives is to hit a pedestrian, without such action being intended by its creators or its user. It is also possible that a self-steering car may malfunction because of a computer virus and as a result cause harm. In these situations, in addition to tort remedies for the injured discussed above, should criminal law play a role?

The literature on criminal liability and AI has discussed the degree to which current criminal law theories are applicable to harm caused by AI systems, and in which situations the current criminal legal regime would be insufficient. In the first situation described above, a developer could be held criminally liable if he or she programs, for example, a self-steering car to drive into a pedestrian under the theory of perpetrator-via-another. In this situation, the AI is merely an innocent agent through which the human perpetrator commits a criminal act (*actus reus*) with the criminal intent (*mens rea*) to do so.

However, if a developer of an AI system does not specifically intend to commit a criminal act but is nevertheless deeply involved in the execution of the AI system's tasks, the perpetrator-via-another theory would not be applicable. As an example, an AI controlled self-steering car is about to run out of gas while on an urgent drive, and the driver wishes to stop for gas. The car calculates that the most efficient method of reaching its destination is to run over its driver once he or she gets out of the car and continue the ride. The driver dies. In such a scenario, the developer did not intend to kill the driver and did not specifically instruct the AI system to run over the driver. However, if the programming of the AI system would lead, as a natural or probable consequence, to the AI system running over a driver, the developer could still be

held liable under the current criminal legal regime, even for crimes that require specific intent. The situation is similar to one where a person releases a wild lion into an apartment with the intent to have the lion kill the person in the apartment. The natural-probable-consequence theory is normally used to prosecute accomplices to a crime; if a conspiracy cannot be proven, accomplices can still be held liable if the criminal act of the main perpetrator was a natural or probable consequence of a scheme that the accomplice encouraged or aided.

In a third situation in which neither the developer nor the user intended to commit nor could foresee a harmful act independently committed by an AI system, there is, under today's criminal legal regime, no person who can be held criminally liable. In the literature, the possibility of assigning criminal liability to an AI system itself in these situations has been discussed. This possibility raises a number of conceptually challenging issues: what would be the moral, economic and legal arguments for assigning criminal responsibility to AI systems? To what extent is it appropriate to deem AI systems to be subjects under the law in their own right rather than property or services? How should one think about the role of punishment of AI systems? If traditional concepts of punishment are inapt or inadequate, how can the law adapt to properly ameliorate the underlying problems and the externalities to human societies? While the *actus reus* element of a crime is conceptually simple to establish for AI systems, how should one formulate theories regarding the requisite *mens rea* of AI systems? Although the idea of assigning criminal liability to AI systems may seem conceptually foreign, compelling arguments, and well-reasoned answers to the questions posed above, have been made in the legal literature.

Regulatory issues

Given the above-mentioned difficulties with identifying the actors responsible for harmful acts of AI systems and assigning civil or criminal liability to such actors *ex post*, *ex ante* regulation of the development and use of AI will be an important way of managing the public risks associated with AI. An *ex ante* regulatory regime would promote an order in which AI is being developed by persons with adequate competency and risk awareness in secure environments, and would promote transparency and accountability. Different conceptual models for such a regime are currently being discussed. Like other sources of public risks, such as automobile traffic, financial markets, energy production, etc., governmental agencies with appropriate expertise, tasked with policymaking and oversight of AI development and AI products, could be formed. Such a regime administered by a government agency could, for example, require the certification of developers and AI projects and contain standards for testing environments and ethical considerations. Sanctions that would be effective without unduly burdening innovators need to be designed for AI projects developed outside the approved regime or in violation thereof. Models that have been discussed include bans, use restrictions and higher liability standards for non-compliant behaviour and products. Like other industries associated with public risk, self-regulation and other industry incentives will likely play a role alongside mandatory regulation.

Privacy and data collection in the age of AI

As discussed at the outset of this overview, useful data acquisition has been a key constraint to the development of the technology since the inception of AI models a few decades ago. The exponential propagation of communication technology containing devices that monitor everything from voice interactions to geo-spacial coordinates has created a massive repository of user data. The aggregation and usage of this personal data triggers issues related to an individual's right to privacy. Specifically, individuals should be concerned with the control of data and the potential unknown outcomes of AI analysis related to personal data.

Regarding control, federal statutes addressing data protection and privacy are generally industry-specific and apply to all citizens. The purpose is to regulate how certain data may be used so that there is a balance between personal/individual rights and commercial interests, while also creating standards to ensure data privacy is maintained throughout the commercial value chain. For example, the Gramm Leach Bliley Act protects use of non-public personal information of individuals obtained by banks, insurance companies and other companies in the financial services industry. It imposes requirements on these entities to protect and limit the dissemination of non-public information, while also obligating them to promptly notify an individual whose non-public information has been made public without their consent.

Although some federal privacy laws preempt the enactment of state laws, those statutory laws addressing privacy and data collection concerns that have not been federally preempted often concentrate on the individual consumer and apply to those individuals residing within the state's boundaries. The types of personal data that these state laws seek to protect vary, and although there is some overlap, there is little consistency among states that choose to address the same data collection and privacy concerns. California was the first state to impose requirements on data controllers to inform all affected persons of a data breach that has led to the exposure of their personal information. As of 2018, all 50 states have now enacted laws requiring the disclosure of breaches of personal data to affected individuals.

Outside of the United States, similar implementation has occurred; Article 25 of the GDPR outlines data protection principles of privacy by design and privacy by default. This statute requires AI systems to be designed with built-in boundaries to ensure data protection.

Another key issue is that of AI innovation. In other words, an individual may agree for data to be used for one purpose, but the insights that the AI model provides are both inside and outside of the initial permissioned purpose. Allowing data to be processed by AI technology also means allowing AI to process data in new and unanticipated ways. Regulation of automated decisions that have unforeseen consequences that are potentially harmful to consumers in the commercial context has already begun.

For example, Article 22 of the GDPR lays out the basis and the right of an individual not to be subjected to automated decision-making. A data subject has the right to object to the decision derived from an automated system after that decision has been made. This will allow for continued innovation in AI, but with the opportunity for the consumer to interject in the innovation process if the AI creates an unintended result that is harmful to the consumer. The veracity of the actual implementation of such interactions between businesses that use the data and the users that provide it should be considered, as often users will execute long consent agreements with little understanding of what they are agreeing to.

Intellectual property

The current legal framework for protecting intellectual property rights will also have to be refined to account for the potential of AI to create its own intellectual property. Currently, in the United States, copyrights and patents are only granted to human authors or inventors. However, these norms were designed when computing processing power was still in its relative infancy, and AI technology had not advanced to the extent it has today. The argument made then was that computers are mere tools and do not contain the capacity for the creative spark so integral to the creative or inventive process. Although AI has yet to produce entirely original creations or inventions that are worth monetising, many have begun to consider frameworks for understanding how to regulate AI inventions.

Most current frameworks advocate a kind of look-through approach to determine authorship or invention by looking at either the programmer or user of the AI technology. This view assumes that the AI is a tool in the hands of creative individuals, rather than a creative individual in and of itself. This is likely the most realistic approach given the current capabilities of the technology and its uses. However, this method is not without challenges, as the contributions of the creator of the AI (*i.e.*, the programmer) and the user of the AI are entangled together in the output of the technology. One could look at the AI as a kind of software tool, much like a word processing software, where a programmer is merely providing a passive tool for the creative author. There are a few difficulties that arise with this approach. For example, the fact that the AI provides a degree of autonomous insight that can seriously influence the creative directive of the user makes it difficult to know where the creative efforts of the author or artist begin and end. Does this creative influence emerge from the programmer and is it powerful enough to be considered a contribution to a creative work, or is it a source of inspiration to the author that remains the sole human creative element? Another challenge relates to authorship: as mentioned above, most AI models are open-source black box designs; in other words, they are designed by many programmers working collectively in the public domain with machinations that are not easily understood or accessible. The abstract notions related to AI creative interference and the distributed development of AI models are examples of what could fog the look-through approach.

Antitrust

As mentioned above, many applied AI models rely on big data, whether geographical, personal, financial or otherwise, to be able to function. Uber's or Google Maps' use of geographical data given to it by its customers and drivers, Facebook's data on personal preferences and opinions given to it by its users, Spotify's data on music tastes and other preferences (when to listen to which kinds of music, etc.) are just a few examples of data that is key to maintaining a competitive edge for the aforementioned businesses. As in other industries the potential for collusion, concentration of market power and oligopoly arise in relation to data ownership and monetisation.

The question as to whether the large-scale availability of data will eventually reduce the marginal value of each additional data point is beyond the scope of this chapter. Nonetheless, we should assume that data is a scarce resource insofar as insight-laden data is difficult to acquire (*e.g.*, Uber's or Google Maps' user data is proprietary and unique to each platform). Assuming the scarcity of data in light of its associated competitive advantages, one can begin to see that data monopolisation is a very real problem. If useful data is contained in the hands of the biggest acquirers, then there are serious barriers to entry that prevent competitive threats to monopolising incumbents. Courts have dealt with the monopolisation of scarce resources that are impractical to imitate, but are necessary for viable competition, since the implementation of cross-country railways; *i.e.*, this is not a new issue. However, the challenge in determining the appropriate policy towards those companies that produce and monopolise these types of scarce resources has persisted.

Most recently, the attempt has been to adopt current antitrust doctrines to accommodate the vagaries of data as a scarce commodity. Margrethe Vestager, the EU Commissioner for Competition, recently stated in a speech that the EU will need to "to keep a close eye on whether companies control unique data, which no one else can get hold of, and can use it to shut their rivals out of the market". The implication that the EU could take a kind of *essential facilities doctrine* approach to the problem has been received by legal scholars with some

enthusiasm. Some are suggesting that augmenting the analysis to not only assess the effect of data monopolisation on competitive pricing, but also on continued innovation (which has had a profound effect on commercial and social processes), will make for a more relevant and clear lens of analysis.

Concluding remarks

This guide is intended to contribute to the ongoing discussion in many jurisdictions as to the role of AI in civil society, and the manner in which the law will rise to the new challenges presented by AI.

We are privileged to have worked with the many contributing authors to this guide and are grateful to our partners and colleagues for their generous and thoughtful contributions.

Matt Berkowitz
Tel: +1 650 838 3737 / Email: matt.berkowitz@shearman.com

Matt Berkowitz is a partner in Shearman & Sterling's Litigation practice. His practice focuses on patent litigation in federal district courts and the International Trade Commission (ITC), as well as post-grant proceedings in the US Patent and Trademark Office. Matt has experience across a broad spectrum of technologies, including consumer electronics, memory systems, hybrid vehicles, pre-collision vehicle systems, aircraft components, and pharmaceuticals.

Matt has been named one of the "Top 40 under 40 Intellectual Property Lawyers" by the *American Society of Legal Advocates* as well as a 2015 New York Metro Rising Star by *Super Lawyers*. In 2016 and 2018, *Benchmark Litigation* recognised Mr. Berkowitz in its "Under 40 Hot List".

Shearman & Sterling LLP

599 Lexington Avenue, New York, NY, 10022-6069, USA
Tel: +1 212 848 4000 / URL: www.shearman.com

Considerations in Venture Capital and M&A Transactions in the AI Mobility Industry

Alan Bickerstaff, K. Mallory Brennan & Emma Maconick
Shearman & Sterling LLP

Introduction

The rise of autonomous machines in recent years has been enabled, in part, by the advances made with respect to "big data" aggregation and analytics. Without the ability for machine learning algorithms or natural language processors to access historical data and update their own functions as new data is collected, the capabilities and applications of Artificial Intelligence ("AI") would be significantly hindered. The power to collect and analyse large volumes of varied data has led to the commercial implementation of drones and robots, along with the advent of the Internet of Things ("IoT") ecosystem of interconnected devices. Practical applications of AI in the various industries have also emerged, and research expenditures in the area are steadily increasing.[1] For example, the transportation industry (including mobility-as-a-service) (collectively, the "mobility industry") has been going through and will continue to go through a significant transition to a new business model, driven in large part by the rise of AI and AI-related and AI-enabling technologies. Over the last five years or so, traditional automobile manufacturers have begun to shift their long-time business model by investing in various transportation services,[2] such as ride-sharing models, monthly subscription models,[3] micro-mobility (last mile urban transportation) models,[4] and the development of autonomous vehicle technologies,[5] through M&A[6] activities and investments[7] in venture capital ("VC")-backed companies. VC investments in the mobility industry have grown dramatically since 2009, with 2017 and 2018 being standout years, while M&A activity has been sporadic since 2011, with 2017 being a standout year.[8] For companies[9] to continue to conduct M&A and investment activity, and to develop and innovate in this space, they will need to be increasingly cognisant of the array of legal implications which arise from a system that is designed, controlled and sometimes even built by autonomous machines. It will be important to understand and anticipate the transactional and regulatory risks surrounding AI implementations, in particular the crucial role intellectual property ("IP") protections play in the commercialisation of these technologies.

Transactional considerations

With the significant financial investments most companies make in developing or obtaining access to AI technologies, the ability to secure IP protection for those developments and to maintain freedom to operate ("FTO") is paramount to ensuring a return on those investments. For example, a software algorithm capable of analysing anonymised data sets could be protected under a patent, a copyright or pursuant to trade secret laws. How a company decides to protect its IP related to AI algorithms may be informed by the capabilities and expertise the company has, those it lacks, and the availability of any development or commercialisation partners across its supply chain. Thus, understanding how to think of the various components

of an AI algorithm from a contractual rights perspective is an increasingly necessary skill for businesses looking to compete in industries leveraging AI technologies.

Before a company can use an AI algorithm in a commercial context, it must first gain access to large quantities of "raw" data, which will be analysed by the algorithm ("AI Inputs"). Generally, this data comes from one or more of the following three sources: (1) publicly available information (from government or academic data sets, or which may be "scraped" off the web, typically using specialised software); (2) voluntarily from "data subjects" themselves (by obtaining legally valid consent); or (3) pursuant to a business-to-business ("B2B") contractual relationship (such as a data processing, licence or data transfer agreement). How a company obtains this raw data is important, as the scope of IP rights a company receives to such raw data impacts the manner in which a company is able to use the data, and ultimately whether a company may be able to derive revenue from the AI algorithm it owns or controls. The output of the AI algorithm, the "AI Outputs" or "processed data", will be valuable commercially (e.g., as part of a software-as-a-service ("SaaS") business model) and have value for the internal development and improvement of the algorithm itself (i.e., enabling the AI to "learn" and improve performance or efficiency). Since the processed data often constitutes a derivative work of the raw data, the scope of rights each party receives to the raw and processed data is a point of focus during negotiations. Matters of IP ownership and FTO may be further complicated by joint development efforts between the parties, which risk enabling a collaborator to become a competitor. When entering into any transaction regarding the collection and transfer of big data to be analysed using AI technologies, the following questions should be considered:

- What rights does each party need to the pre-existing IP of the other party (if any) in order to commercialise and achieve its ultimate business goals?
- Does either party need to impose any field of use, purpose, territorial or other limitations on licences to any pre-existing IP contributed to the transaction?
- How will the parties enforce their rights in IP, e.g., which party(ies) can enforce which rights in which jurisdictions?
- Are limitations needed on the licensee's right to sublicense or transfer the IP rights granted under the agreement?
- Will the counterparty require access to information or technology which constitutes a trade secret?
- Does the contract draw clear lines between disparate pieces of IP contributed (and not contributed) by each party?
- What rights will each party have in any jointly developed IP? E.g., will the parties be able to compete against each other using any jointly developed IP, and to what extent will each party be able to further develop any jointly developed IP?
- What is the exit strategy? What happens if one party decides to stop aiding IP development or wants to end the relationship?
- What happens if the AI technology itself generates IP without human intervention that is valuable or otherwise protectable under IP laws? Which party should bear the risk of an AI application's infringement of third-party IP?

The final question above, regarding the ability for an AI program itself to create new IP, highlights issues over whether existing IP legislative and regulatory frameworks are suited to address the myriad implications of AI-driven business models. For example, under current U.S. laws, non-humans cannot be the author of a copyrightable work nor the inventor of a patentable invention; this foundational tenet of U.S. IP law is inherently at odds with the burgeoning applications for AI technologies. As governmental authorities work to either adapt existing IP frameworks or build entirely new frameworks regarding the impact AI has

on the creation of IP, it is increasingly imperative that companies approach IP contracts for AI applications with fresh perspectives and innovative drafting if they want to mitigate the risks to IP posed by the escalating adoption and implementation of AI technologies.

Intellectual property considerations in transactions

Companies should carry out a comprehensive due diligence investigation of the target's intellectual property, as is always the case, but the following are some IP considerations unique to AI. Companies should identify and understand the fundamental AI asset that is driving the value and premise of the transaction. An AI system may be comprised of algorithms/software, the AI inputs and AI outputs, or a combination of both. Knowing which of these components is the value driver will allow companies to focus their IP due diligence accordingly. Companies should understand the target's product functionality, the extent to which it "learns", boundaries or precautions that are in place on the AI's ability to act independently, and processes for updating the AI systems. Companies should also take a careful look at the target's IP protection practices, which should include identifying the inventors and contributors to the AI.

Algorithms/software. Algorithms and processes should be subject to trade secret protection, whether or not the algorithms and process may be patented, as long as they are kept confidential and derive independent economic value from not being generally known. Thus, it is important to examine the target's treatment of algorithms in contracts and its trade secret protection practices. With respect to algorithms/software, companies should seek to understand (i) the extent to which the algorithm/software is derived from open-source or third-party software, and (ii) whether the target has taken reasonable efforts under the circumstances to protect the secrecy of this information, as required by U.S. law, to achieve trade secret protection.[10]

AI inputs. With respect to AI inputs, companies should seek to understand (i) the source of the data, (ii) how the data is used, (iii) whether the target has the appropriate rights to use the data to train its algorithm/software, and (iv) if the data is personal data, whether the target has obtained appropriate consents to use that data.[11] Note that some AI inputs may use publicly available data sets. While the underlying publicly available data may not be legally protectable, the employer's manipulation, interpretation, and uses of that data may be protectable. For example, certain jurisdictions, particularly in Europe,[12] provide *sui generis* database rights which are similar to, but distinct from, copyright protections. Companies should be mindful of this if a target has used web scraping software or other automated means to aggregate publicly available information from the Internet to use as training data for a machine learning algorithm, as the target's automated processes may have unwittingly run afoul of these database laws in the course of their data collection.

AI outputs. With respect to AI outputs, companies should seek to understand whether the target owns the AI outputs. This can often be determined through a review of the target's commercial contracts, but in some cases may require the analysis and application of intellectual property ownership laws.[13] Like algorithms, AI outputs may be subject to trade secret protection, so companies should examine the target's trade secret protection practices and the public accessibility of the AI outputs.

Review of IP agreements. Companies should review the target's inbound supply and development agreements, outbound licence agreements, actual IP protection practices and the terms of the target's form of proprietary information and inventions assignment agreement ("PIIAA"). In addition to customary provisions, companies should review the target's licence agreements for use specifications and limitations and, within the permitted use, the definition of product failure and the consequences of failure to achieve any specified objectives.

While the processes, algorithms, and data related to AI technologies are likely encompassed within the general definition of confidential information, it may be wise for the target's (and the buyer's) form of PIIAA and its third-party contractor agreements, as well as its various other licence agreements, to include a more tailored definition of AI information. At a minimum, the definition of confidential information should include:

- Processes, data analytics processes, algorithms, analyses, data, data compilations, metadata, device configurations, embedded data, and technologies.

Although the following terms are probably covered by the broader definition, some employers may want to add more specific terms, such as:

- System elements, neural networks, training sets, parameters, rules, ensemble methods, generated code and decision trees.

Similarly, to the extent the PIIAA includes a non-compete, it is important to ensure the scope of the non-compete encompasses the foregoing definitions.

Companies should make sure that the definitive agreements relating to the transaction have the appropriate representations and warranties, as further described below under "Liability matters".

Cybersecurity considerations

In addition to thinking through the contractual rights in IP created or incorporated into AI technologies, companies also need to be cognisant of the shifting regulatory landscape regarding data privacy and exposure that may result from inadequate security measures. The issue of how parties allocate the risks of data breaches, including enforcement actions by regulatory bodies and resulting consumer class actions, is becoming increasingly salient in the field of big data and analytics. As the demand for data increases, and as the type of data collected may be viewed as increasingly invasive (such as biometric information or consumer profiling), demands have similarly increased for the implementation and enforcement of regulations regarding the collection, storage, processing and transfer of data, including data which constitutes the personally identifiable information ("PII") of data subjects.

Indeed, increasingly burdensome and restrictive regulations concerning data privacy and cybersecurity are being enacted across the world to protect data subjects from unauthorised access or misappropriation of PII and other sensitive information.[14] Consumers' increasing understanding of the risks of data breaches, their control (or lack thereof) over aggregated data and PII, and the potential for misuse of such personal information has also driven further growth and sophistication of consumer class actions based on data security breaches. As a result, companies looking to leverage big data and AI technologies must proactively implement and maintain robust cybersecurity frameworks to mitigate the risk of a potential data breach, and to mitigate damages if a data breach is suffered. A careful review of a company's cybersecurity compliance posture, and whether the company's approach is appropriate in light of the risks of a data security breach, is a bare necessity in light of these legislative developments. Contractual mechanisms are useful to allocate these risks and liabilities between parties in privity with one another, but they will not relieve a party of its independent legal obligations. Contractual protections may also be inadequate to cover the costs of defending and resolving class action suits. A more holistic approach to cybersecurity is necessary to ensure the success of an AI-driven, data-reliant business venture. Implementation of "privacy by design" concepts can help avoid data breaches resulting from design decisions, and other precautions, such as procuring cybersecurity insurance, can help mitigate the damage of a successful data breach.

By adopting a privacy by design framework, a company can adopt a systems engineering approach which inherently enhances the privacy protections of their products or services. The seven foundational principles of privacy by design[15] are specifically tailored to maximise privacy by ensuring that PII and other sensitive data are protected by default within a given IT system, product or business practice. Policies and protocols adopted in accordance with the privacy by design principles become embedded across the entire lifecycle of a product or service. Privacy by design is often followed in accordance with various international or industry-specific standards that have been promulgated, such as ISO/PC 317 (promulgated by the International Organization for Standardization)[16] or the Payment Card Industry Data Security Standard (promulgated by the PCI Security Standards Council),[17] but can also be applied independently and adapted to a company's processes. For example, a company can use various "differential privacy" software tools and statistical techniques to analyse usage or other patterns of a large number of users without compromising individual privacy.[18] The privacy by design methodology may be used to decrease the risk that a data breach occurs; however, it does not necessarily help a company deal with the aftermath when a data breach does occur.

As discussed below in "*Liability considerations – contractual risk allocation*", contractual mechanisms can be useful for allocating risks and liability amongst business partners leveraging big data and AI technologies, but tensions can arise between contracting parties in the aftermath of a data breach. It can be difficult and expensive to conduct a root cause analysis pinpointing the source of a data breach in order to determine the degree of fault each party should bear for the breach. Additionally, the typical indemnities, limitations of liability and contractual remedies for breach of representations and warranties or confidentiality obligations usually included in a contract may be insufficient to adequately protect a company from liability stemming from a data breach, or one party to a contract may simply not have the resources to fully indemnify the other party in the event of a data breach. As a result, many companies obtain cybersecurity insurance to cover the gaps in risk exposure which cannot be addressed through normal contractual provisions. Cybersecurity insurance can provide additional comfort that a company is reasonably protected from the damages of a data breach; however, it is important to understand the full scope of coverages, and any carve-outs or exceptions to the insurer's coverage obligations. Companies which purchase cybersecurity insurance should make certain to notify their insurer of any attempted data breach in accordance with their policy requirements (whether there was unauthorised access to data or not), and keep their insurer apprised of any plans to expand the business into new jurisdictions. A company that proactively communicates with its insurer can be more confident that its insurance policy is sufficient in scope to cover any potential data breach and the resulting exposure, which may result from historical security events or future business plans.

Ultimately, however, as AI-driven services become increasingly pervasive and invasive, the legal system's demands for transparency and accountability will also increase.

Regulatory considerations

As of the date of this chapter, no unified regulatory framework has been put into place regarding autonomous vehicles, which potentially leaves investors a little bit in the dark about how to analyse regulatory compliance issues in connection with an investment. Autonomous vehicles have been operating under a patchwork of state[19] rules with limited federal oversight, but over the last few years there have been several proposals and developments that have the industry heading in the direction of a national regulatory framework. Attempts at developing a federal regulatory approach to autonomous vehicles include:

- *The Volpe Center FMVSS Review*.[20] The United States Department of Transportation ("USDOT") commissioned the Volpe National Transportation Systems Center to identify instances where the existing Federal Motor Vehicle Safety Standards ("FMVSS") may pose challenges to the introduction of automated vehicles. It identifies standards requiring further review – both to ensure that existing regulations do not unduly stifle innovation, and to help ensure that automated vehicles perform their functions safely.
- *USDOT Data for Automated Vehicle Integration (DAVI)*.[21] The USDOT launched DAVI as a multimodal initiative to identify, prioritise, monitor, and – where necessary – address data exchange needs for automated vehicles integration across the modes of transportation.
- *USDOT Request for Comment on V2X Communications*.[22] The USDOT requested comment on how recent developments in core aspects of the communication technologies that could be associated with connected vehicles, including vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communications, collectively referred to as "V2X" communications, could impact both V2X in general and the USDOT's role in encouraging the integration of V2X.
- *National Highway Traffic Safety Administration (NHTSA) Federal Automated Vehicles Policy*.[23] The NHTSA published a preliminary statement of policy concerning automated vehicles in order to harness the benefits of automated vehicle technology by providing a framework for doing it safely, which was updated in September 2017.[24]
- *SELF DRIVE Act*.[25] The "Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution" or "SELF DRIVE" Act was passed by the House in September 2017, and includes a broad preemption of the states from enacting legislation that would conflict with the Act's provisions or the rules and regulations promulgated under the authority of the Act by the NHTSA. The Act empowers the NHTSA with oversight of manufacturers of self-driving cars by enacting future rules and regulations that will set the standards for safety, and govern areas of privacy and cybersecurity relating to such vehicles.
- *AV START Act*.[26] On October 4, 2017, the Senate Committee on Commerce, Science, and Transportation unanimously approved its own version of the SELF DRIVE Act, the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act. The bill remains pending in the Senate.

CFIUS and export controls. Investors may also need to take into account recent legislation relating to CFIUS and export controls laws when considering investments in AI. The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"),[27] passed in August 2018, overhauled the US law governing CFIUS national security reviews. In October 2018 regulations, CFIUS implemented new rules that extend CFIUS jurisdiction to certain non-controlling foreign investments in certain US "critical technologies", and by subjecting those investments, whether controlling or not, to a mandatory short-form CFIUS declaration.[28] While the new CFIUS rules do not explicitly call out AI as one of the enumerated "critical technologies", AI may be directly or indirectly implicated or relevant to some of those enumerated "critical technologies". In addition, the Export Control Reform Act of 2018, which was enacted as part of the same legislative package as FIRRMA, requires the President to start an interagency process to identify "emerging and foundational technologies" that "are essential to the national security of the United States" and not already included in existing definitions of critical technologies. On November 19, 2018, the US Commerce Department published a notice seeking comment on the criteria for determining which "emerging technologies are essential to national security" under the Export Control Reform Act of 2018, and explicitly called out several categories of AI and machine learning for

consideration in that notice.[29] Accordingly, companies should determine whether CFIUS and/or export controls regulations are implicated in connection with its transaction.

Liability considerations

There are a myriad of possible liabilities that arise from AI in the mobility industry, as discussed in detail in the "*Who's to blame?*" section below, but these risks generally arise from IP infringement, privacy laws and product liability. An investor and the target may allocate the risk of these possible liabilities primarily through contractual allocation of risk and through insurance.

Contractual risk allocation

Representations and warranties. The definitive agreement should have appropriate representations and warranties (including sufficiently broad IP definitions) regarding: IP ownership; validity; non-infringement; sufficiency of rights; IP assignments by employees and contractors; IP protection; ownership of or appropriate licences to data sets and databases; encumbrances on IP (including third-party licences); absence of defects; absence of viruses; routines or components allowing access or damaging data; failures or losses; compliance with privacy and data security laws and disclosure of government inquiries, claims experience, breaches or non-compliance with such laws; protection of personal data; and disclosure of security breaches and unauthorised access. Knowledge qualifications in these representations lessen investor protection if the product violates a representation (particularly the non-infringement representation) without the knowledge of the "knowledge group".

Covenants. Consider whether pre-closing covenants regarding remedial actions would be appropriate. Companies should also consider whether AI could affect affirmative and negative covenants with its actions. Should an action taken by AI be a breach of a covenant, whether or not the action is known to the target?

Indemnification. Companies should consider customary indemnification provisions, including: survivability of representations, warranties and covenants; extended survival periods to the extent warranted; and indemnification baskets and caps. Companies should factor into account due diligence analysis, specific industry considerations, the target's AI products and how they are used, in determining whether it should require specified line item indemnification provisions, such as contracts not adequately mitigating risk to the target, any strict liability issues and damages that may be caused by the actions of the AI.

Insurance risk allocation

Companies may also mitigate and allocate risk relating to AI through a combination of the target's and companies' own first and third-party insurance policies. As part of the due diligence process, companies should consider the adequacy of the target's insurance for actions that occur prior to the closing, and should assess the sufficiency of its own insurance coverage for AI matters post-closing. Companies and the target should have in place third-party insurance coverage for errors and omissions, security privacy, regulatory matters, and media liability coverage and first-party coverage for breach response, network interruption, data restoration and cyber extortion. In some cases, it may be appropriate to also consider product liability insurance and employer practices liability insurance. Finally, *in lieu* of contractual indemnification, in an M&A transaction it may be appropriate to obtain a representation and warranties insurance policy for companies. The terms of these products shift regularly because the product is so new; thus, companies should review the coverage carefully to ensure companies will be adequately protected.

Who's to blame? Liability in the (coming) age of autonomous vehicles

In 2016 and 2017, more than 37,000 roadway deaths were recorded in the United States.[30] The NHTSA reports that "[d]angerous actions" by drivers "such as speeding, distracted driving, and driving under the influence" are the primary causes of these fatalities.[31] Indeed, the NHTSA attributes 94% of serious crashes to human error.[32] One of the goals of autonomous vehicles is, of course, a world in which sophisticated technology reduces the number and severity of accidents, because the AI is better equipped than humans to avoid accidents.[33] Unless AI technology becomes so advanced that car accidents can be avoided entirely, however, the inevitable question of liability remains: when a self-driving vehicle is involved in an accident, whose fault is it?

The short answer is that it depends. As discussed in the "*Regulatory matters*" section above, the statutory framework surrounding the use of AI in the mobility industry is still developing.[34] Given the rate at which technology is advancing, and companies' ongoing testing of self-driving vehicles (like Uber) and sale of vehicles equipped with automated driving systems, or "ADS" (like Tesla), the development of a statutory framework addressing liability will inevitably trail the occurrence of accidents in which liability is disputed. Accordingly, participants in the autonomous vehicle industry should be mindful of how courts may evaluate the allocation of liability in the absence of laws that dictate who bears the burden of legal responsibility for accidents. Indeed, these same considerations may well shape the development of the statutes and regulations that are ultimately put in place.

The discussion below considers the potentially liable actors, outlines legal standards and factual considerations that may be taken into account when allocating fault among those actors, and evaluates how liability might be allocated in two case studies drawn from real-life events.

Who are the potentially liable actors?

When an autonomous vehicle is involved in an accident, traditional legal theories might allocate liability to the owner and driver of the AI-equipped vehicle,[35] the manufacturer of the vehicle that includes AI, or the manufacturer of component parts of the vehicle (e.g., the manufacturer of the radars used to gather information about the driving environment that is used by the AI to make driving decisions). Where the ADS controlled the driving decisions at the time of the accident, and those decisions arguably caused the accident, a fourth actor could also face liability – the AI itself.

Which actor should bear responsibility for an accident depends upon not only the specific facts giving rise to the accident, but also the legal theory that is applied. Various theories for how allocation of liability should be determined have been explored to fill the void that presently exists, due to a dearth of legislation and little case precedent that is directly applicable. For example:

- *Vehicle owner/driver*: Some authors argue that the owner of an autonomous vehicle should be liable for any accident caused by the vehicle, even if the ADS is controlling the car, because the owner has assumed responsibility for any harm caused by the vehicle by purchasing it.[36] This is most consistent with the traditional allocation of liability to vehicle owners and the accompanying insurance regime.[37] However, allocating harm based purely on ownership could have unintended consequences, creating substantial disincentives to owning autonomous vehicles.[38]
- *Vehicle manufacturer/AI programmer*: As vehicles become more autonomous, and ADS ultimately become equipped to make value-based decisions derived from programming inputs designed by the AI manufacturer, others have theorised that because the manufacturer of the vehicle is the ultimate decision-maker, the manufacturer should

be held liable for accidents that occur when the ADS controls the vehicle (even if the ADS functioned properly and made the "correct" decision in an unavoidable accident).[39] This theory of liability can be likened to a product liability theory,[40] except without the traditional considerations of manufacturer defect, failure to warn, and design defect.[41]

- *AI*: Although the AI ultimately makes the decision as to how to respond to external stimuli, even in those instances where the AI's decision is the direct cause of harm to persons injured in an accident (whether the occupants of the vehicle or third parties), holding the AI itself liable is challenging for the obvious reason that it is not an independent actor.[42] Some authors have argued that the AI is effectively the agent of the manufacturer because, even though it is the "actor", the AI carries out functions as prescribed by the manufacturer.[43] Under such a theory, ultimate liability for the AI's actions would flow to the manufacturer as principal.[44]
- *Components manufacturer*: To the extent an accident is caused by a failure of one of the component systems that works together with the AI, such as radars employed by the AI to inform the AI about its surroundings, liability may be extended to the components manufacturer under a traditional theory of product liability.

Control as the proxy for liability

The evaluation of where to place liability is of course developing in parallel with ADS technology itself. Cars are not yet fully autonomous, and thus drivers of AI-equipped vehicles retain a degree of control over the vehicle and thus some responsibility for any accident.[45] As cars become more autonomous and drivers exercise less control, the responsibility imposed on owners/drivers may diminish over time, but the imprint of the framework derived from the intervening years – i.e., the actor exercising control bears greater liability – may well influence the analysis of the circumstances under which liability may be imposed on drivers of even fully autonomous vehicles.

This differentiation is apparent in the six-tiered framework presently used by the NHTSA to classify autonomous vehicles, which was adopted from SAE International in September 2016.[46] The framework takes into account whether the "human operator or the automated system is primarily responsible for monitoring the driving environment":[47]

- Primary responsibility for controlling driving tasks falls to driver:[48]
  a. Level Zero: no automation. Driver performs all driving tasks, even if assisted by enhanced warning systems or similar technology.
  b. Level One: driver assistance. Driver controls majority of driving tasks, with some assistance by automated systems, such as stability control.
  c. Level Two: partial automation. Vehicle is equipped with some autonomous system controls (e.g., steering and acceleration), but driver retains control of all other driving tasks.
- Primary responsibility for controlling driving tasks falls to AI ("Highly Autonomous Vehicles"):
  a. Level Three: conditional automation. Vehicle controls majority of driving tasks, monitors environment, and gathers data from that environment to respond to changes therein; driver must be ready to take control of the vehicle at all times (e.g., to intervene in emergency situations).
  b. Level Four: high automation. Same autonomous controls as Level Three; driver has discretion as to whether to intervene in an emergency situation (can but is not required).
  c. Level Five: full automation. Vehicle controls all aspects of driving functions at all times and under all conditions.

Applying these considerations in real life: two accident case studies

The first fatal accident involving a self-driving car occurred in March 2018 in Tempe, Arizona, when an autonomous vehicle being tested by Uber struck a pedestrian with a bicycle crossing the street in front of the vehicle. According to the NTSB's preliminary report, Uber had equipped the vehicle (manufactured by Volvo) with "developmental" self-driving technology that functioned in two modes, computer control and manual control.[49] When the vehicle was in computer control mode, automated emergency braking technology (installed by Volvo) was disabled to prevent erratic vehicle behaviour.[50] The vehicle was not programmed to alert the operator when the vehicle perceived that emergency braking was necessary, even though the system relied upon the operator to exert manual control to stop the car in such circumstances.[51]

The vehicle detected the pedestrian six seconds before impact and, at just over one second before impact, determined that emergency braking was necessary. The driver did not apply the brakes until just after impact with the pedestrian. The NTSB concluded that the ADS was operating normally, as it was designed to do, just after the crash. A later-issued report by the Tempe Police Department concluded that the driver of the test vehicle was watching a television show on her phone at the time of the crash.[52] The report also concluded that the driver could have avoided the accident had the driver been watching the road.

In this example, the driver could be held liable under a negligence theory for both failing to watch the road and failing to exert control as required in order to safely drive the autonomous vehicle. An argument could also be made that Uber should be held liable under a design defect theory of product liability. "A design defect occurs when a product is performing as intended but presents an undue risk of harm."[53] Here, one might argue that because Uber restricted the functionality of the automated emergency braking technology but did not create a corresponding alert system to advise drivers when the vehicle perceives that emergency braking is necessary, Uber's design presented an undue risk.[54]

Tesla vehicles equipped with the manufacturer's "Autopilot" feature have been involved in several crashes, including an October 2018 incident involving a 2017 Tesla Model S. In that accident, the Tesla crashed into a stationary vehicle that was stalled in the left lane of a highway at a speed of approximately 80 mph when the Autopilot – a paid upgrade feature – was engaged but did not detect the vehicle.[55] The owner and driver sued Tesla, asserting claims of strict liability for design defect, negligence for breach of the duty of care, breach of implied warranty, misrepresentation/misleading advertisement, and violation of Florida's Deceptive and Unfair Trade Practices, on the theory that the Autopilot system failed and is not as capable and safe as marketed by Tesla.[56]

Tesla has moved to dismiss the case, arguing that the driving manual for the Model S makes clear that the Autopilot function is not capable of detecting stationary objects when the vehicle is traveling at highway speeds (at more than 50 mph).[57] Indeed, this limitation has also been reported by news media and has been described as a well-known limitation of the existing technology for self-braking systems for Tesla and other manufacturers that use the technology, because the system cannot yet distinguish between stationary objects in the road – such as a fire truck – and stationary objects above the road, like an overpass.[58] Tesla vehicles also provide alerts when drivers' hands have been off the wheel for more than a few seconds to remind them that their attention is required.[59]

The stationary-object limitation of the Tesla is arguably different from the vehicle modification imposed by Uber, which was designed to eliminate a technologically available protection. With respect to the Tesla accident, the restriction arguably derives from an existing technological limitation, meaning that the design cannot – at this stage in development,

with existing technology – be corrected or improved upon. To the extent that Tesla can establish that the warnings provided with the Model S were sufficient to alert the driver, or that the limits of the technology were widely known, it is arguable that the driver assumed the risk by driving the Tesla. One could also argue that, assuming the driver was aware of the limitations of the technology, which his lawyer seems to have acknowledged in speaking to the press, the driver's failure to pay attention to the road would support an argument that, just like in the Uber accident, the driver should ultimately bear the liability.

Conclusion

Due to the shifting regulatory landscape and the iterative nature of design and innovation, companies seeking to expand or improve their business operations by leveraging AI technologies, whether through development, acquisition or strategic investments, should be as proactive as possible in addressing the numerous business and legal complexities presented by autonomous machines and big data analytics. The subjects discussed in this chapter constitute one part of what should be a holistic approach to conducting due diligence, mitigating the risks and maximising the benefits of acquiring, investing in, or developing and commercialising any AI-based technologies.

* * *

Endnotes

1. P&S Intelligence Prvt. Ltd., *AI in Transportation Market Overview*, available at: https://www.psmarketresearch.com/market-analysis/ai-in-transportation-market (last accessed Feb. 16, 2019).
2. Mike Ramsey, *Ford Says It Will Focus More on Transportation-Services Sector*, Wall St. J. (Jan. 5, 2016, 12:49 PM), available at: https://www.wsj.com/articles/ford-says-it-will-focus-more-on-transportation-services-sector-1452016172.
3. Michael J. Coren, *There's a New Subscription Business Model Arriving For Cars*, QZ.com (Nov. 30, 2017), available at: https://qz.com/1142296/a-new-subscription-business-model-is-arriving-for-cars-thanks-to-volvo-ford-porsche-and-silicon-valley-startups/.
4. Joshua Brustein, *Ford Acquires Electric Scooter Startup Spin*, Bloomberg (Nov. 7, 2018, 5:10 PM), available at: https://www.bloomberg.com/news/articles/2018-11-07/ford-is-said-to-buy-scooter-startup-spin.
5. Jack Stewart, *Mapped: The Top 263 Companies Racing Toward Autonomous Cars*, Wired.com (May 10, 2017, 7:30 AM), available at: https://www.wired.com/2017/05/mapped-top-263-companies-racing-toward-autonomous-cars/.
6. *See* Brustein.
7. Mike Isaac, *General Motors, Gazing at Future, Invests $500 Million in Lyft*, N.Y. Times (Jan. 4, 2016), available at: https://www.nytimes.com/2016/01/05/technology/gm-invests-in-lyft.html.
8. Pitchbook, 2019 Emerging technology Outlook (2018), available at: https://files.pitchbook.com/website/files/pdf/PitchBook_2019_Emerging_Technology_Outlook.pdf.
9. For the purposes of this chapter, "company" or "companies" generally include and refer to companies attempting to commercialise these technologies, companies and private equity investors engaging in M&A activity for AI technologies, and companies and investors acquiring equity in companies developing AI technologies.

10. *See* Uniform Trade Secret Act § 1(4) (Unif. Law Comm'n 1985) and Economic Espionage Act of 1996 § 101(a), 18 U.S.C. § 1839(3).
11. For example, Facebook recently had its Apple enterprise licence revoked for collecting personal data on iPhones in contravention of Apple's policies. *See* Tom Warren and Jacob Kastrenakes, *Apple Blocks Facebook From Running Its Internal iOS Apps,* The Verge (Jan. 30, 2019, 10:27 AM), available at: https://www.theverge.com/2019/1/30/18203551/apple-facebook-blocked-internal-ios-apps.
12. *See* Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31996L0009.
13. U.S. IP law has historically refused to credit works to non-human agents. *See* Naruto V. Slater, No. 15-cv-4324, 2016 WL 362231, at *3-4 (N.D. Cal., Jan. 28, 2016) (challenging the standing of an animal to raise a copyright infringement claim); *see* Russ Pearlman, *Recognizing Artificial Intelligence (AI) as Authors and Investors Under U.S. Intellectual Property Law,* 24 Rich. J. L. & Tech. no. 2, 2018.
14. *See* General Data Protection Regulation (EU) 2016/679 (EU/EEA); California Consumer Privacy Act, Cal. Civ. Code § 1798.198(a), as amended by SB-1121 (2018) (State of California, United States); Lei Geral de Proteção de Dados Pessoais, Law No. 13.709/2018 (Brazil).
15. Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles,* Information and Privacy Commissioner of Ontario (2011), available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (last accessed Feb. 16, 2019) (setting forth the following principles of systems design: (1) proactive not reactive, preventative not remedial; (2) privacy as the default setting; (3) privacy embedded into design; (4) full functionality – positive-sum, not zero-sum; (5) end-to-end security, full lifecycle protection; (6) visibility and transparency; and (7) respect for user privacy by making it user-centric).
16. Available at: https://www.iso.org/committee/6935430.html (last accessed Feb. 16, 2019).
17. Available at: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last accessed Feb. 16, 2019).
18. *See Differential Privacy*, Harvard University Privacy Tools Project, 2014, available at: https://privacytools.seas.harvard.edu/differential-privacy (last accessed Feb. 16, 2019).
19. *See Autonomous Vehicles: Self-Driving Vehicles Enacted Legislation,* Nat'l Conf. of States (Nov. 7, 2018), available at: http://www.ncsl.org/research/transportation/autonomous-vehicles-self-drivingvehicles-enacted-legislation.aspx.
20. Kim, Anita, David Perlman, Dan Bogard, and Ryan Harrington, *Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles Preliminary Report,* Cambridge, Mass.: U.S. Department of Transportation, John A. Volpe National Transportation Systems Center, March 2016.
21. *Data for Automated Vehicle Integration (DAVI),* U.S. Dep't of Transportation, available at: https://www.transportation.gov/av/data (last accessed Feb. 20, 2019).
22. Notice of Request for Comments: V2X Communications, 83 Fed. Reg. 66,338 (Dec. 26, 2018).
23. National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy: Accelerating the Next Revolution In Roadway Safety* (Sept. 2016).
24. National Highway Traffic Safety Administration, *Automated Driving Systems 2.0: A Vision for Safety* (Sept. 2017).
25. H.R. 3388, 115th Cong. (2017), available at: https://www.congress.gov/bill/115th-congress/house-bill/3388/text.

26. S. 1885, 115th Cong. (2017); *see also* Press Release, U.S. Senate Committee on Commerce, Science and Transportation, Senate Commerce Approves AV START Act, Other Bills and Nominations (Oct. 24, 2017), available at: https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=BA5E2D29-2BF3-4FC7-A79D-58B9E186412C.
27. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), H.R. 4311, 115th Cong. (2017), was integrated into the John S. McCain National Defense Authorization Act of 2019, Pub. L. No. 115-232, which was signed by the President on August 13, 2018. The John S. McCain National Defense Authorization Act of 2019 also integrated the Export Control Reform Act of 2018, H.R. 5040, 115th Cong. (2018).
28. Provisions Pertaining to Certain Investments in the United States By Foreign Persons, 83 Fed. Reg. 51,316 (Oct. 11, 2018) (to be codified at 31 C.F.R. pt. 800).
29. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (Nov. 19, 2018) (to be codified at 15 C.F.R pt. 744).
30. Nat'l Highway Safety Admin., U.S. Dep't of Transp., *USDOT Releases Fatal Traffic Crash Data* (Oct. 6, 2017), available at: https://www.nhtsa.gov/press-releases/usdot-releases-2016-fatal-traffic-crash-data; Nat'l Highway Safety Admin., U.S. Dep't of Transp., *USDOT Announces 2017 Roadway Fatalities Down* (Oct. 3, 2018), available at: https://www.nhtsa.gov/press-releases/us-dot-announces-2017-roadway-fatalities-down.
31. Nat'l Highway Safety Admin., U.S. Dep't of Transp., *USDOT Announces 2017 Roadway Fatalities Down* (Oct. 3, 2018), available at: https://www.nhtsa.gov/press-releases/us-dot-announces-2017-roadway-fatalities-down.
32. Nat'l Highway Safety Admin., U.S. Dep't of Transp., *Automated Vehicles for Safety*, available at: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety (last accessed Feb. 28, 2019).
33. *See* Nat'l Highway Safety Admin., U.S. Dep't of Transp., *Automated Vehicles for Safety*, available at: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety (last accessed Feb. 28, 2019); *accord* Knowledge@Wharton, "Autonomous Car Crashes: Who – or What – Is To Blame?" (Apr. 6, 2018), available at: http://knowledge.wharton.upenn.edu/article/automated-car-accidents/.
34. The NTHSA has suggested that the allocation of tort liability rests with States, which creates the potential for a patchwork of inconsistent regulations. *See* U.S. Dep't of Transp., *Automated Driving Systems 2.0: A Vision for Safety* (Sept. 2017) at 24, available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
35. This discussion assumes for the sake of simplicity that the owner and the driver are the same person. To the extent the driver of the autonomous vehicle that is involved in an accident is not the owner, that may introduce additional complexity to evaluating liability. For example, traditional questions of agency may arise where the driver of the vehicle is an employee of the company that owns the vehicle.
36. *See* Moolayil, Amar K., *The Modern Trolley Problem: Ethical and Economically-Sound [sic] Liability Schemes for Autonomous Vehicles*, 9 Case W. Reserve J. L. Tech & Internet 1, at 15–16 (2018).
37. *See, e.g.*, Crane, Daniel A., Kyle D. Logue, and Bryce C. Pilz, *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 Mich. Telecomm. & Tech. L. Rev. 191, at 256–257 (Spring 2017).
38. *See, e.g.*, Cowger, Alfred R., Jr., *Liability Considerations When Autonomous Vehicles Choose the Accident Victims*, 19 J. High Tech. L. 1, at 53–54 (2018).
39. *See* Okun, Jill J. and Ryan Rawlings, *OEMS: Mitigating Potential Liability Posed by Autonomous Vehicle Crash Optimization Systems*, 60 No. 11 DRI for the Def. 63 (Nov.

2018); *accord* Cowger, Alfred R., Jr., *Liability Considerations When Autonomous Vehicles Choose the Accident Victims*, 19 J. High Tech. L. 1, at 54–55 (2018).

40. *See, e.g.*, Bogost, Ian, "Can You Sue a Robot?", *The Atlantic*, Mar. 20, 2018, available at: https://www.theatlantic.com/technology/archive/2018/03/can-you-sue-a-robocar/556007/.
41. *See* RESTATEMENT (THIRD) OF TORTS: CATEGORIES OF PRODUCT DEFECT § 2(a) (AM. LAW INST. 2012) (outlining the different categories of product defects).
42. *See* Moolayil, Amar K., *The Modern Trolley Problem: Ethical and Economically-Sound [sic] Liability Schemes for Autonomous Vehicles*, 9 Case W. Reserve J. L. Tech & Internet 1, at 18-19 (2018).
43. *See* Moolayil, Amar K., *The Modern Trolley Problem: Ethical and Economically-Sound [sic] Liability Schemes for Autonomous Vehicles*, 9 Case W. Reserve J. L. Tech & Internet 1, at 18-20 (2018).
44. *See* Moolayil, Amar K., *The Modern Trolley Problem: Ethical and Economically-Sound [sic] Liability Schemes for Autonomous Vehicles*, 9 Case W. Reserve J. L. Tech & Internet 1, at 18-20 (2018).
45. One study performed in August 2018 concluded that even in accidents involving self-driving vehicles in California, where many companies test autonomous vehicle technology, humans continue to be the leading cause of accidents. *See* Kokalitcheva, Kia, "People cause most California autonomous vehicle accidents", Axios (Aug. 29, 2018) available at: https://www.axios.com/california-people-cause-most-autonomous-vehicle-accidents-dc962265-c9bb-4b00-ae97-50427f6bc936.html.
46. SAE International, *Automated Driving* (2014), https://www.smmt.co.uk/wp-content/uploads/sites/2/automated_driving.pdf.
47. Nat'l Highway Safety Admin., U.S. Dep't of Transp., *The Federal Automated Vehicle Policy* (Sept. 2016) at 9.
48. U.S. Dep't of Transp., *Automated Driving Systems 2.0: A Vision for Safety* (Sept. 2017) at 4, available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
49. National Transportation Safety Board, "Preliminary Report Highway HWY18MH010", at 2, available at: https://www.ntsb.gov/investigations/Accident Reports/Reports/HWY18MH010-prelim.pdf.
50. National Transportation Safety Board, "Preliminary Report Highway HWY18MH010", at 2, available at: https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.
51. National Transportation Safety Board, "Preliminary Report Highway HWY18MH010", at 2, available at: https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.
52. Korosec, Kristen, *TechCrunch.com* "Uber safety driver of fatal self-driving crash was watching Hulu, not the road", available at: https://techcrunch.com/2018/06/22/uber-safety-driver-of-fatal-self-driving-crash-was-watching-hulu-not-the-road/.
53. Okun, Jill J. and Ryan Rawlings, *OEMS: Mitigating Potential Liability Posed by Autonomous Vehicle Crash Optimization Systems*, 60 No. 11 DRI for the Def. 63 (Nov. 2018).
54. Depending upon how well-informed the driver was concerning the necessity of braking, one could also imagine liability arising under a failure-to-warn product liability theory. Uber could also be potentially liable under traditional theories of principal/agent liability because the driver of the vehicle was employed by Uber.

55. Davies, Alex. *Wired*, "A Florida Man Is Suing Tesla for a Scary Autopilot Crash", Oct. 30, 2018, available at: https://www.wired.com/story/tesla-autopilot-crash-lawsuit-florida-shawn-hudson/.
56. *See Hudson v. Tesla Inc., et al*., Case No. 2018-CA-011812-O (Cir. Ct. Fla. Oct. 30, 2018).
57. The manual reads in relevant part: "Traffic-Aware Cruise Control cannot detect all objects and may not brake/decelerate for stationary vehicles, especially in situations when you are driving over 50 mph (80 km/h) and a vehicle you are following moves out of your driving path and a stationary vehicle or object is in front of you instead." Davies, Alex. *Wired*, "A Florida Man Is Suing Tesla for a Scary Autopilot Crash", Oct. 30, 2018, available at: https://www.wired.com/story/tesla-autopilot-crash-lawsuit-florida-shawn-hudson/.
58. Lee, Timothy B., "Another Tesla with Autopilot Crashed into a Stationary Object – the Driver Is Suing", Oct. 30, 2018, available at: https://arstechnica.com/cars/2018/10/man-sues-tesla-says-autopilot-steered-him-into-a-stalled-car-at-80-mph/.
59. *See* Davies, Alex. *Wired*, "A Florida Man Is Suing Tesla for a Scary Autopilot Crash", Oct. 30, 2018, available at: https://www.wired.com/story/tesla-autopilot-crash-lawsuit-florida-shawn-hudson/.

Alan Bickerstaff
Tel: +1 512 647 1903 / Email: alan.bickerstaff@shearman.com

Alan Bickerstaff is a partner in the Emerging Growth, Capital Markets and Mergers & Acquisitions practices at Shearman & Sterling LLP.

He represents entrepreneurs and public and private emerging growth companies on private equity and venture capital financings, public offerings, mergers & acquisitions, formation, operations and corporate governance matters and securities law reporting and compliance matters.

Alan represents companies in the technology, media, telecommunications, medical device and life sciences, consumer products, energy and renewable energy industries. He also represented numerous institutional investors in venture capital financings and private equity transactions as well as underwriters in public securities offerings.

K. Mallory Brennan
Tel: +1 212 848 7657 / Email: mallory.brennan@shearman.com

K. Mallory Brennan is a partner in the Litigation practice at Shearman & Sterling LLP.

Mallory focuses on representing global financial institutions and corporations in mergers & acquisitions litigation and transactional disputes, securities litigation, and other complex commercial disputes, including bankruptcy and antitrust actions. She also has experience counseling multinational corporations in connection with both internal and regulatory investigations. In 2018, Mallory was named in the *Benchmark Litigation* "40 & Under Hot List", and in 2017 and 2018, Mallory was recognised by *The Legal 500* as a "Next Generation Lawyer" for M&A Litigation Defense.

Emma Maconick
Tel: +1 650 838 3704 / Email: emma.maconick@shearman.com

Emma Maconick is a partner in the Intellectual Property Transactions Group at Shearman & Sterling LLP. She focuses on intellectual property, data protection, privacy and security issues for major technology clients engaged in data and innovation intensive activities.

Emma represents corporate clients as well as lenders, emerging companies, research and development entities and universities. Emma focuses on representing clients in a range of technology sectors including FinTech, big data and analytics, cloud and edge computing, "as a service" businesses, consumer platform operators, artificial intelligence, machine learning, advanced virtual and augmented reality, autonomous mobility, and semi-conductor, hardware and software product designers and manufacturers.

Emma has extensive experience with the IP, data and IT aspects of transactional matters including mergers & acquisitions, strategic alliances, joint ventures, capital markets transactions and corporate and financial investment.

Shearman & Sterling LLP

599 Lexington Avenue, New York, NY, 10022-6069, USA
Tel: +1 212 848 4000 / URL: www.shearman.com

AI Changes Society. Society Changes the Law. The Bright Future of the Smart Lawyer

Gabriele Capecchi & Giovanna Russo
Legance – Avvocati Associati

AI and the 4th industrial revolution

Everyone knows it nowadays. We are living in an unprecedented period of technological innovation. Artificial intelligence (AI) has been available for a number of years, however its development is now increasing at a furious pace.

Over the past few years, you may have heard someone drop the term "big data", "machine learning", "block-chain", but only a few chosen minds deeply understood those words. Now, examples of AI and machine learning applications are used and can be found everyday everywhere: Apple's Siri or other assistants based on speech recognition technology, chatbot and conversational interfaces; and recommendations made by online services Amazon and Netflix or automatic credit ratings by banks just to mention a few, but we also have the Fintech market, cryptocurrency, self-driving vehicles, as well as facial recognition technology used for biometric identification which – through the use of machine learning – creates a digital document-free identity. The catalogue of other AI applications (such as in the medical care, health monitoring and healthcare system analysis, environment, energy, transport, insurance and legal services sectors) is, moreover, impressively broad.

Many factors have boosted this incredible growth: the large data sources granted by mobile phones, e-commerce tools and navigation systems gathering data over the world, and the consequent immense availability of data, literally used as fuel for machine learning tools; the increased reliability of algorithms; and the virtually unlimited and incredibly fast computational power thanks to cloud availability (not even mentioning quantum computing).

And this is only the beginning.

An increasing number of AI start-ups have been established globally during the past five years, and the leading technology giants (Alibaba, Amazon, Google, Facebook, Microsoft and Tencent) are focusing more and more on AI. Many countries such as the US and the PRC as well as the EU are investing in AI facilities and research. The European Parliament, in its 2019 resolution on AI and Robotics European Industrial Policy, has defined AI as the "*key to turning Europe into a 'start-up continent' by exploiting the latest technologies to generate growth in Europe*".

The 4th industrial revolution is definitively in place, and the social implications cannot be ignored. The way we work, the way we live is changing forever.

Several improvements and benefits to people's lives and the economy can be attributed to this AI revolution, and there is an ever-increasing number of foreseeable advantages. However, when using this powerful technology serious risks need to be taken into account; for example, privacy and data protection infringements, discriminatory conduct or unfair treatment due to

algorithms' bias or difficulty to explain the decisions made on the basis of black-box algorithms (the lack of so-called "*explainability*"), restrictions to other fundamental rights and freedoms of individuals through perception manipulation practices (the very famous Cambridge Analytics case in connection with election outcomes) or programs used as "emotional surveillance".

Protection should also be sought from a national security perspective for the increasing threats by sophisticated hackers. It is necessary to create a safe cybersecurity perimeter, as in some way done in Italy in November 2019, through the extension to the cybernetic field of the special powers granted to the Italian Government in case of national security threats by private business developments (the so-called "*Golden Powers*"), including the right to impose particular tests for security standards and specific notification duties.

The legal framework in a changing world

In order to address the aforementioned risks, rules and legal remedies are of the essence.

As of today, legal advisors, researchers, consumers, manufacturers and stakeholders are doing their best to adapt the existing rules to the emergent AI reality. For instance, the EU General Data Protection Regulation – according to which companies are required to first obtain consent of EU citizens before processing their data and personal data processing for statistical purposes (including AI training) is required to remain as aggregate data and shall not be re-applied to individuals – or the Product Liability Directive – which to a certain extent can apply to defective robots and AI.

However, extensive interpretation of the existing framework is not always the best solution. Indeed, in the event of product liability, persons suffering damages may find it very burdensome to prove defects of AI products or the existence of a causal link between such products and damages – as requested by the aforementioned EU Directive – in case of autonomous self-learning and decision-making AI, also given the asymmetric flow of information between producers and customers and the difficultly of human control over AI activities under certain circumstances.

The current legal framework needs to evolve. However, this is not an easy task. Technology is opaque and fast-moving, faster than lawmakers can even understand.

Following this view, the UK Financial Conduct Authority (FCA) offers an interesting example on how regulators and technology can walk together. Given its task to regulate and supervise one of the world's biggest financial centres, the FCA has partnered with the Alan Turing Institute – the UK's national institute for data science and AI created by leading UK universities – to analyse current and future uses of AI across the financial services sector and the relevant emerging requests in terms of ethics and regulation, so as to elaborate potential focused strategies accordingly and with a practical approach.

In addition, there is a growing consensus around the idea that creating an ethical framework for AI can also be a viable solution – basically to avoid infringements of human fundamental rights and freedoms as well as to create a solid environment which could improve the trust of producers, service providers and customers of AI applications.

To support the implementation of this vision, the European Commission established the High-Level Expert Group on Artificial Intelligence, an independent group requested to draft a guideline for AI ethics, which in April 2019 developed the Ethics Guideline for Trustworthy AI, aimed at promoting a trustworthy AI.

In particular, according to such guideline, AI applications – to be trustworthy – shall be: (i) *lawful*, hence complying with applicable law and regulations (EU Treaties and secondary law,

such as on data protection and product liability, anti-discrimination, consumer law and safety and health at work, and EU Member State laws as applicable); (ii) *ethical*, hence ensuring adherence to ethical principles and values (including respect for privacy, quality and integrity of data, access to data, traceability, "explainability" and communication, avoidance of unfair bias, accessibility and stakeholder participation); and (iii) *robust,* from both a technical and social perspective, hence cyber-resilient to security attack, assuring backup plans and general safety, accuracy, reliability and reproducibility.

In general terms, such guidance offers an interesting path for regulators to act with flexibility and adaptability in enacting a new legal framework and enhancing the existing one, in order to properly and proportionately handle the AI technology risks.

Challenges for today's lawyer

The above is the general technological and legal framework that lawyers need to address in their current day-by-day work life.

And it is definitively evident that the traditional way of considering the legal profession needs to be urgently revised.

First, technology will always outstrip the law. Lawyers, instead, are required to be prepared and to constantly update their technological knowledge. Only by understanding the technological background of the specific cases and of the clients' needs can they correctly interpret and apply the existing rules and propose, where necessary, new specific law enactment.

Further, the current industrial revolution has also impacted legal work. Now the legal services market requires more efficiency, faster replies and lower costs. If lawyers and law firms wish to be and remain at the cutting edge of the worldwide legal offering, they must learn to use AI tools to do more and better.

With this view, several AI technological applications, known by the general name *Legaltech*, have been created for lawyers.

Among others, we can mention AI and machine learning document review tools – which, through a data-trained algorithm, analyse a huge amount of legal documents and can be used for due diligence purposes. Also very useful are document and contract management platforms – which can streamline the drafting process by creating a first draft of standardised contracts or of legal documents in few seconds, after answering a brief questionnaire on the specific matter at issue.

In addition, another challenge that today's lawyer shall face due to the new technological environment is competition. Not only with other lawyers, but also with AI applications.

In particular, certain AI technological applications are products for clients. Sometimes they are labelled under the different name *Lawtech,* and among them we can mention, for instance, certain legal chatbots which are becoming quite widespread among individual customers and can also be used in companies' legal departments. They consist of AI and machine learning tools which allow users to get quick answers to basic legal inquiries in a chat or messenger. Further, online marketplaces – *i.e.*, digital platforms helping potential clients to find a lawyer quickly, inspired by the Uber model – are also now in use.

All the above technological innovations have the potential to lead in the very near future to new and more responsive legal services with improved accessibility, positive consumer outcomes and more competition. However, this is a definitively hostile environment for traditional lawyers.

As in the past industrial revolutions where some jobs were totally replaced by new work roles, we could expect that non-technological lawyers be adversely affected by the incredible AI innovation wave we are experiencing now.

However, working against automation or technological progress would be completely useless. The only alternative option is to be ready with updated knowledge and new legal solutions aimed at providing a more efficient product, tailored to the new advanced technological needs of clients.

In conclusion, the advent of the massive current wave of AI innovation and the consequent incredible change in our daily life is far from being an apocalyptic event for the smart lawyer. On the contrary, by gaining new expertise in using the new legal technological tools as well as basic knowledge of AI products used in clients' businesses, the smart lawyer would be in the right position to take advantage of the tremendous opportunity offered by the impressive growth of AI.

This is the time for lawyers to believe in this wave of technological innovation, leaving the most repetitive, time-consuming and less challenging work to intelligent machines so as to play as main characters on the legal services stage.

Gabriele Capecchi
Tel: +39 02 89 63 071 / Email: gcapecchi@legance.it

Gabriele deals with M&A transactions and is co-head of our Real Estate Department. He practises in corporate finance and has also developed a sophisticated expertise in real estate, assisting primary investors in any kind of real estate project. In 2017, Gabriele was named "Real Estate Lawyer of the Year" at the TopLegal Industry Awards. He is regularly mentioned in *Chambers & Partners* as a leading lawyer in his field.

Gabriele is member of the Strategic Committee and is the Country Partner for China and Singapore. He is also leading "Quantum Leap", an innovative AI contract automation project which our firm originally conceived for internal use and which we are now sharing with our clients.

Giovanna Russo
Tel: +39 06 93 18 271 / Email: grusso@legance.it

Giovanna assists Italian and non-Italian companies, financial institutions and private equity funds in major M&A transactions in the Italian market, including mergers, demergers, acquisitions, spin-offs, divestitures and joint ventures. She also has an extensive experience with regard to commercial agreements, including supply, distribution and service contracts, and assists clients during the entire corporate history of Italian legal entities, from incorporation to possible winding-up, including capital increases, also in kind, issue of particular classes of shares and of participating financial instruments. She has also acted, on an ongoing basis, as Secretary of the Board of Directors of joint-stock companies.

She graduated *cum laude* in 2004, was admitted to the Italian Bar in 2007, and in 2010–2011 she worked as a Foreign Lawyer at a leading American law firm based in New York.

Legance – Avvocati Associati

Milan, Via Broletto no. 20 / Rome, Via San Nicola da Tolentino no. 67, Italy
Tel: +39 02 89 63 071 (Milan office) / +39 06 93 18 271 (Rome office) / URL: www.legance.com

AI and the Evolution of Payment Services

Bas Jongmans & Xavier Rico
Gaming Legal Group

Introduction

The financial services industry can hardly keep up with current developments, as new smart services with different angles are introduced on an almost daily basis. Are national regulators up to the task of keeping these services in check with acceptable standards for customer protection, market integrity, the prevention of Base Erosion and Profit Shifting ("**BEPS**") as well as the prevention of money laundering? Or should financial regulators follow the global trend of evolving in a global regulatory framework which shall allow them to be better equipped to deal with these multiple objectives? What role shall AI-based applications play in all of this?

Gaming Legal Group's Bas Jongmans, attorney at law and Xavier Rico, forensic consultant discuss the current worldwide trends of these developments from an industry perspective, as well as the developing regulatory principles.

Neobanking and other trends in the development of financial services

The 2008 financial crisis lead to the common understanding amongst nations that it was time to reform regulations of the consumer credit market, aimed at enhancing protection of consumers. As one of the first nations to do so, the United Kingdom introduced a more robust, proportionate regulatory system on 1 April 2013.[1] Tailored to the characteristics of the consumer credit market, a two-tier authorization (or "limited permission") approach for credit activities should suit the diverse nature of the consumer credit market. Bringing a focus *"from the boardroom to the point of sale and beyond, to put the well-being of their customers at the heart of how they run their businesses and to promote behavior, attitudes and motivations about good conduct above anything else"*.[2] Although the vision and ambition of these reforms is clear, at the time it remained to be seen how the Financial Conduct Authority and other financial regulators would in practice approach regulation of the UK's banking and financial services industry.

These new regulations helped to stimulate the rise of the so-called *"challenger banks"*. A new type of smaller retail bank, an independent form of *"neobanking"*, independently running on a "self-owned" licence, set up to compete directly with the longer-established banks in the UK, sometimes by specializing in areas underserved by the "big four" banks. The Bank of England even set up the New Bank Start-up Unit, guiding firms through the application process.[3]

This new breed of banks heavily relies on technology-focused initiatives, and has an edge over traditional banks. Neobanks have the potential to offer far better and more customised services than traditional banks. For instance, neobanks have the ability to forecast cash flows or encourage savings through a virtual piggy bank account.[4]

Typical for these next generation banks is a ring-fencing strategy, established by a separation of traditional investment banking from retail banking. *Atom Bank*, the first smartphone app-based bank of its kind, launched in April 2016. It was keen to adopt machine learning and artificial intelligence technologies whilst not being constrained by legacy systems of traditional banking competitors. *Atom Bank* does not have any traditional online banking outlets.[5] On 9 March 2017, the bank experienced over 5,000 new customer sign-ups in one day. The surge led to the end of a special interest rate offer, which created controversy in some financial publications.[6]

Another new model of banks conceptualized by the Reserve Bank of India – so-called *"payment banks"* – were set up in India as of 2013. Payment banks distinguish themselves from historic banks by not giving out loans and setting a limit on deposits per client.[7]

Prior to the 2008 credit crunch, *Fidor Bank*, operating in Germany (since 2007) and Russia, used social media to overcome the cost and complexity of traditional banking, while increasing customer trust through an online community.[8]

Evolution has not been restricted to financial institutions only. Over time, payment service providers teamed up with merchants on a software-as-a-service basis ("**SaaS**"). Working with SaaS allowed the offering of more advanced payment services via an electronic portal, a payment gateway. Already in 2005, the Dutch company *Currence iDEAL B.V.* introduced *"iDEAL"* in the Netherlands, allowing a direct contact, a "live" payment, executed between customers, merchants and their banks. It also allowed recurring payments without the necessity of the merchant storing customer-sensitive information, highly increasing protection against identity theft-related fraud. SaaS also allowed for a "live" risk analysis on transactions as well as to make an AML risk calculation on the origins of the payment.

The gambling industry received a big boost in popularity when the electronic processing of payouts to end users was introduced. Combining SaaS with mobile points of sale, further enhanced by object recognition technology such as quick response ("**QR**") codes, resulted in the offering of the cardless, digital wallet. Combining these technologies with a crypto-based currency eliminated the necessity for customers and merchants to hold a traditional account, connected to any individual or company, eliminating all together the necessity for a bank and even for cash to be involved in a transaction. After all, a cryptocoin holds its own value. Bitcoin, for example, has properties that make it similar to gold. The developers of the core technology limited the production of Bitcoin to a fixed amount, 21 million BTC. It therefore does not resemble cash. The term *"Digital Gold"* seems more appropriate.[9]

WeChat Pay and *Alibaba*'s payments arm *Alipay* dominate China's mobile payments landscape, which is considered by many experts as one of the most advanced in the world. Until recently, both platforms required users to have a Chinese bank account to make payments. These evolutions also almost "obliterated" the need for cash payments. As a next step, facial and fingerprint recognition is now replacing QR technology in that nation. In August 2019, *WeChat Pay* introduced its *"Frog Pro"* system that allows customers to make payments by simply scanning their faces, without the use of their mobile phones. The technology is now being tested in several Chinese retail chains and came after *Alipay* rolled out its own facial recognition payment system, the *"Dragonfly"*, last year.[10]

Evolution of substance

Evolution of payment services also sheds new light on what is to be perceived as "substance of transaction". Substance is "key" for many reasons. Distribution of taxation rights between nations hinges on substance. It is also an essential tool in combatting money laundering.

By request of the G20 international forum for governments and central bank governors ("**G20**") in 2013, the Organization for Economic Cooperation and Development ("**OECD**") produced its 15 standards (also referred to as "**Actions**") on BEPS in 2015. These Actions are aimed at enhancing an international "level playing field" by, for example, introducing obligations in legislation to provide for "substance": to have an actual presence and/or establishment as a requirement to claim favorable tax features. Since then, its *"framework members"* have been in the process of implementing these Actions; such implementations are subject to *"peer review"*.[11]

Economies shifting towards pure digital trade cannot escape redefining minimum substance criteria. A clear example of this struggle to keep the innovation going may be found in the efforts of the government of Malta.

In the Malta chapter of the first (2019) edition of *AI, Machine Learning & Big Data*, we quoted Steve Tendon, a former strategic adviser (in 2016) for the Ministry of Economy, Investment and Small Business ("**MEIB**") and the first Chairman of the Blockchain Malta Association ("**BMA**").

Malta held its first long-anticipated Malta Blockchain Summit in 2018.[12] The nation set out to present an ambitious National Blockchain Strategy ("**NBS**"), consisting of six separate key projects, aimed at transforming the island into an economic superpower in the emerging Crypto Global Economy.

Tendon notes on his website that *"crypto-economy"* should not be limited to cryptocurrencies alone, but to the broader new dimension of economic enterprises that can work on top of cryptographic technologies, which typically are blockchain technologies. By creating a legal environment where such enterprises can thrive, the idea is to attract those kinds of businesses to Malta.[13] Such enterprises do not necessarily require a physical presence, or "classic" substance so to speak. Regulators may follow the blockchain/publicly accessible ledger of whatever qualifying cryptocurrency and the chain of transfer thus not needing *per se* to access paper files and records from various intermediaries. *Ergo*: no need for substance as one used to be familiar with.

On the contrary, such demands would lead to "fake" substance. If regulators fail to redefine the said substance criteria, this would stimulate the "scam artists" of the future, suppliers of empty office buildings, filled with a surrogate staff, all in the name of pretense.

In the view of Tendon, Malta's development into the "Blockchain Island" seems to have gone stale. In a fascinating and brutally honest article about the birth of the blockchain island concept, Tendon claims that Malta completely *"missed the point"* of the power of cryptocurrencies.

The opportunity of shifting services to the digital realm was "lost" by forcing companies to put down a physical presence on its shores. The nation seems to have fallen into the trap of following its "classic" existing model for success: attracting foreign investments and making companies set up a physical presence on the island.

Tendon aimed to create an entirely virtual jurisdiction. This could then serve to connect cryptocurrencies and blockchain technologies to the rest of the global financial system. Cryptocurrencies do not just offer multiple advantages when it comes to sending cross-border payments, peer-to-peer transfers or reducing fees. That, he argues, is just scratching the surface. However, this was "a bold move which Malta was ultimately unwilling to take".[14] The idea of becoming a dominant player in the fully virtual *crypto-sphere* has in his view been lost. The country's insistence on crypto-companies setting up a physical presence is in

his view entirely unsustainable. It would be a constant drain on the island's limited resources. Based on this view, Malta could soon become even more heavily overpopulated with a searing housing crisis, an insufficient infrastructure, and a diminishing quality of life for its people. Tendon claims that it is hard to overstate the innovative potential of cryptocurrencies. From a financial perspective, cryptocurrencies offer a number of clear and unique advantages over existing technologies and currencies, including almost real-time, cross-border, peer-to-peer transfer and settlement of values at affordable fees.

Tendon seems to have found a new partner in the Republic of the Marshall Islands ("**RMI**"). Ironically, a nation even smaller in (geographical) size than Malta. The capital Majuro is a 13 km^2 strip of land surrounding a 300 km^2 lagoon.

Tendon: *"RMI truly encapsulates the 'blockchain island' problem: a situation of extreme isolation and an urgent need to forge connections - connections which are not rooted in the constraints of geography, space and physical resources."*

RMI introduced the Marshallese sovereign ("**SOV**"). It is a unique *"crypto-fiat"* currency, in the view of Tendon aimed at creating prosperity not for just one nation, but having a greater impact on the world. It is about social responsibility and even changing the very fabric of society with a deep concern about sustainability issues, social justice and distribution of wealth.[15]

Nevertheless, fiat money is a currency without intrinsic value that has been established as money by government regulation. Therefore, fiat money has value only because a government maintains its value, or because parties engaging in exchange agree on its value. That, however, may not have to pose a problem. Not unlike traditional cash, only until 1971, the value of bearer-demand notes used to be guaranteed by an equivalent of its value in gold.

Regulatory developments and AI

In an attempt to keep up with the rapid developments, the Fifth EU Anti-Money Laundering Directive ("**5 AMLD**") was adopted on 19 April 2018.[16] It amends the Fourth EU Anti Money Laundering Directive.[17] It introduces a further requirement for transparency by publication of large amounts of data. However, at the same time, this may lead to privacy concerns. How will the additional information be processed and by whom? Shall regulators be able to process such an abundance of information? Shall these amendments therefore actually lead to enhancements in the combatting of money laundering?

The beneficial ownership registers for legal entities, such as companies, will be public. This wider access to part of the beneficial ownership information is meant to enhance public scrutiny and to contribute to preventing the misuse of legal entities for money laundering and terrorist financing purposes. Furthermore, access to data on the beneficial owner of trusts will be accessible without any restrictions to competent authorities. These public national registers on beneficial ownership information will be interconnected directly to facilitate cooperation and exchange of information between Member States. In addition, Member States will have to put in place verification mechanisms of the beneficial ownership information collected by the registers to help improve the accuracy of the information and the reliability of these registers.

Member States will only by exception have a limited possibility to allow the anonymous use of electronic money products. Oversight under 5 AMLD shall furthermore be extended to entities which provide services that are in charge of holding, storing and transferring virtual currencies. Under 5 AMLD, these entities will also have to identify their customers and report any suspicious activity to the local so-called Financial Intelligence Units ("**FIUs**"). These

FIUs will have access to more information through centralized bank and payment account registers or data retrieval systems. Member States will be required to set up centralized bank account registers or retrieval systems to identify holders of bank and payment accounts. These systems should be set up in such a way that they can be interconnected.

EU Member States are required to implement these new rules into their national legislation by 10 January 2020. The EU shall target and, if necessary, blacklist third countries with low transparency on beneficial ownership information.[18]

As said, 5 AMLD mostly facilitates the call for more data, more information. That classic approach – hardly "AI" inspired – may not necessarily lead to more transparency, a clearer view. On the contrary, complex operations such as cross-border gaming structures that typically consist of many services working together (affiliates and marketing, payment services and gaming providers) may prove very difficult to properly price services at market value.

Although obviously seen by the authors of 5 AMLD as the "enemy" of transparency, blockchain technology may just prove useful in combatting money laundering. Its (optionally) decentralized, distributed and public digital ledger can be used to record transactions across many computers so that any involved records cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A decentralized blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. Decentralized smart contract technology could be digitally enforced, contract rules verified and regulations and its governed transactions tracked and made irreversible. In the decentralized setup, the smart contract technology is key, as it is required to run without any centralized authority. It would provide an independent level of confidence, as the end user retains independent, unalterable ownership of payments, without third parties involved.[19]

Conclusion

It does not seem that regulators are "up to the task" of keeping the rapidly evolving payment services in check with acceptable standards for customer protection. Also the chosen approach in collecting more and more information by means of 5 AMLD is hardly inspiring. We do not see any future in a global regulatory framework. The EU's call to simply "blacklist" non-EU third countries that do not sufficiently comply makes that clear. Instead, the world could benefit from technology that shall be tamper-proof (*"Provably Fair Technology"*).

Within this respect, we expect and also advise the payment services industry to pivot from custodial to non-custodial SaaS setups, in which regular transactions shall no longer be (mainly) controlled by a human factor. New technologies, although potentially harmful, may prove highly beneficial when applied in a responsible manner. Eliminating the human factor may benefit PSPs even more, as AML-related risks are mitigated while at the same time cutting costs, improving efficiency and boosting the prevention of fraudulent behavior.

* * *

Endnotes

1. "*A new approach to financial regulation: transferring consumer credit regulation to the Financial Conduct Authority*", HM Treasury, June 2013.
2. "*Financial Services Act 2012: A New UK Financial Regulatory Framework*", Harvard Law School Forum on Corporate Governance and Financial Regulation.

3. "*A new approach to financial regulation: transferring consumer credit regulation to the Financial Conduct Authority*", UK Government, 16 January 2014.
4. "*The changing face of digital banking*", Gopal Iyer, hedgehoglab.com, 24 March 2016.
5. https://www.atombank.co.uk.
6. "*The app-based bank that has too many customers*", *The Times*, David Byers, 18 March 2017.
7. "*Operating Guidelines for Payments Banks*", Reserve Bank of India, 6 October 2016.
8. "Six challenger banks using IT to shake up UK retail banking", Karl Flinders, *Computer Weekly*, 21 January 2015.
9. "*A Global Overview on the Evolution of Payment Services*", Bas Jongmans and Xavier Rico of Gaming Legal Group, *The International Comparative Legal Guide to: Gambling,* Sixth Edition.
10. "*Forget the QR code. Facial recognition could be the next big thing for payments in China*", Yen Nee Lee, *CNBC*,19 November 2019.
11. "*A Global Overview on the Evolution of Payment Services*", Bas Jongmans and Xavier Rico of Gaming Legal Group, *The International Comparative Legal Guide to: Gambling,* Sixth Edition.
12. https://ccn.com/malta-does-europes-blockchain-island-really-live-up-to-the-hype.
13. https://chainstrategies.com/2018/02/18/maltas-national-blockchain-strategy-the-big-picture.
14. "*Here's Why Malta Falls Short of Being 'The Blockchain Island'*", CFN Network, 4 October 2019.
15. "*Will the Real Blockchain Island Please Stand Up!?*", Steve Tendon, chainstrategies.com, September 2019.
16. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
17. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
18. Factsheet: "*Strengthened EU rules to prevent money laundering and terrorism financing*", Directorate-General for Justice and Consumers, 9 July 2018.
19. "*A Global Overview on the Evolution of Payment Services*", Bas Jongmans and Xavier Rico of Gaming Legal Group, *The International Comparative Legal Guide to: Gambling,* Sixth Edition.

Bas Jongmans
Tel: +31 20 262 98 95 / Email: bas.jongmans@glglitigation.com

Bas Jongmans, attorney at law, studied tax litigation at Leiden University, specializing in the offset of tax losses. After working for several years within several international and litigation tax practices, he launched "Gaming Legal Group", a symbiosis between the law firm "GLG Litigation" and "GLG Compliance". Bas is a member of the "Dutch Order of Tax Advisors" (Dutch: "*Nederlandse Orde van Belastingadviseurs*", or "NOB"), the "Dutch Bar Association" (Dutch: "*Nederlandse Orde van Advocaten*", or "NOVA"), the "Dutch Order of Mediators" (Dutch: "*Nederlands Mediation Instituut*", or "NMI") and the "Dutch Association of Attorneys and Tax Litigators" (Dutch: "*Nederlandse Vereniging van Advocaten-Belastingkundigen*", or "NVAB"). Bas has produced various scientific publications within various areas of expertise, available for download at gaminglegal.com.

Xavier Rico
Tel: +356 2778 1475 / Email: xavier.rico@glgcompliance.com

Xavier Rico, originally from Curaçao, completed his education in psychology and artificial intelligence at the Radboud University of Nijmegen in the Netherlands. As a highly valued systems analyst within the gaming sector, he worked on substantial technical projects for several master licence holders on the island of Curaçao before joining GLG Compliance as a technical compliance officer. Xavier is a native Dutch speaker but is also fluent in English, Spanish and the local language Papiamento.

Gaming Legal Group

Suikersilo West 35, 1165 MP, Halfweg NH, P.O. Box 17426, Netherlands
Tel: +31 20 671 54 85 / URL: gaminglegal.com

Australia

Anthony Borgese, Jonathan Thompson & Alice Scamps-Goodman
MinterEllison

In brief

The adoption of AI, Machine Learning and Big Data is gaining significant momentum and is an increasing focus of the market and regulators. Australia continues to lag behind many G20 nations in adoption.

Technological developments continue to outpace industry and regulators within Australia (partly reflected in few AI-related patent filings). Further domestic law concerning ownership and use is still largely determined on the basis of existing principles relating to intellectual property, consumer rights, and privacy – though this may change due to new regulatory initiatives. This is also occurring in the competition space as authorities complete a review of the practices of large technology companies, and the challenges presented by emerging technologies. Developing law has already raised challenges for board members who must increasingly consider the implications of protections, including privacy legislation, and ensure they possess an appropriate understanding of technologies used, to discharge obligations.

Overall Australia retains a predominately "soft" regulation model for these technologies relying on "frameworks" and "roadmaps" for adoption and self-regulation. There is increasing investment in building a regulatory framework and adopting a coordinated industry approach. This is further motivated by new ethical and policy challenges raised by these technologies; accordingly, influential regulatory bodies have increasingly focused on advocating for further measures. While Australia's disparate human rights and anti-discrimination statutes provide protections, challenges experienced in development and deployment have increased the likelihood of reform in the near future.

Trends

What is machine learning, artificial intelligence (AI) and big data?

Machine learning is the ability of technology to learn new skills without actively being programmed. Computers iteratively learn from new data via a set of algorithms. Sectors with significant volume of work, or work that has standardised procedures, are increasingly benefitting from machine learning. Machine learning is, in fact, a part of AI.

AI is a set of algorithms that can analyse vast quantities of data. AI deals with algorithms, deriving value from various facets of natural intelligence. It consists of executing tasks that usually require human intelligence, such as information extraction, speech recognition, and decision making. Varying levels of automation are already being adopted in the healthcare, manufacturing, transportation and finance sectors to bring about innovation, increased productivity and cost savings.

Big data is data that is so voluminous that traditional data processing software cannot manage it. Big data is used to train the algorithms for machine learning and AI. Gartner has defined big data as the three V's: "high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation."[1] According to this definition, big data encompasses three dimensions: volume (the amount of data); velocity (the speed of data capture and processing); and variety (the use of different data types and sources). Big data has changed the way businesses identify trends and challenges, by analysing large data sets, often from a variety of sources, quickly. Together with advances in machine learning and AI, big data has the potential to lead to many new breakthroughs.

How are AI and big data impacting the competitive landscape?

AI and big data are reshaping the competitive landscape by generating new waves of technical capabilities and innovation. By allowing companies to make decisions faster, extract hidden insights and optimise processes to complete tasks more efficiently,[2] new perspectives are facilitating strategic competition across a multitude of industries.

Many industries working with large amounts of data recognise the value of big data and machine learning technology. By gathering insights from big data (often in real time), organisations can work more efficiently or gain a competitive advantage. For example, when a website recommends items you might like to buy based on your previous purchases, that company is using machine learning or AI algorithms to data mine your purchase history. Similarly, in the healthcare industry, AI is gaining traction due to the wealth of medical data that can be mined and analysed to find patterns in the diagnosis and treatment of a range of medical conditions.

More visible to consumers is the automotive industry that is embracing proponents of AI, in terms of autonomous cars and in-car virtual assistants. In addition to the driverless car phenomenon, manufacturers (BMW, Mercedes-Benz and Kia) are inserting AI services (Google Home and Amazon Alexa) into vehicles to enable passengers to control the car's technology through their natural voice commands.

How are companies maximising their use of data for machine learning and AI results?

Any application of machine learning or AI will only be as good as the data that is collected and used. Companies are therefore seeking to maximise their use of data for machine learning by improving the quality of their data by ensuring that their data is up to date, in a consistent format, and in the correct quantity to ensure that the machine can process the data. While having the correct data is important, in order to maximise the results from AI, companies also need to engage the right talent to manage this data.

There is widespread acknowledgment that effective use of big data can significantly benefit companies by increasing the rapidity of processing, supporting decision making, improving efficiency, and creating new methods and solutions. This can be seen across a multitude of industries such as health, medical care, scientific research, education, sustainable development, agriculture, transport and security. These benefits must be balanced against the significant challenges that AI and big data pose for businesses and consumers. Key risks exist as a result of holding ever larger volumes of data, the matching and re-identification of data held within, or shared between organisations and the re-purposing of data for unintended uses.

What are the key legal issues that are arising out of adoption of AI/big data/machine learning?

The adoption of AI, big data and machine learning enlivens significant issues in relation to privacy, data security and liability based on the automatic nature of the systems. Regular, day-to-day activities that in the past would not have involved digital interaction may now leave both individuals and organisations exposed to more legal risks and ethical issues.

A key privacy risk arises when an individual's personal information is collected and processed by AI in Australia. In these circumstances, personal information must be treated in accordance with the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988* (Cth) (**Privacy Act**). Accordingly, the personal information must only be used for the purpose for which consent has been obtained. If the AI technology is using data that is identifiable as personal information, then the AI capability may create information that individuals did not intend to be collected or know existed (beyond the scope of its authorised use) which will be in breach of the APPs and attract significant penalties. The government has recognised that privacy measures need to keep up with AI capabilities,[3] and as such the Office of the Australian Information Commissioner (**OAIC**) is continually assisting in developing standards for the use and implementation of AI in step with privacy law.[4]

Another key legal issue is the data security risk stemming from organisations holding larger volumes of data. This risk is significant where data matching and re-identification is required or if data is shared with other organisations. In these circumstances, data may be re-purposed by other organisations for unintended uses, resulting in a breach of the organisation's confidentiality and potentially fiduciary obligations to its customers.

A growing legal risk of AI is determining who is liable for the output of the AI if the AI system leads to a decision that results in harm. For example, what happens if an autonomous vehicle injures an individual, which recently happened in Arizona where a woman was struck and killed by a "self-driving" Uber.[5] Within Australia, there is currently no regulatory (or legal) framework to determine the liability in these circumstances between the AI owner, user, manufacturer and insurer. As such, utilising highly or wholly automated vehicles is currently not permitted in Australia, other than for approved trials, however regulations are rapidly developing in this regard.[6] Nonetheless, it remains imperative that responsibility for loss or damage caused by the use of AI should be consistent in any contract in relation to AI services to avoid any unintended additional liability.

What is the government view with respect to the adoption of AI?

The Australian Federal Government is increasingly embracing the use and development of AI. Recently the Federal Budget for 2019–20 committed $25 million in additional funding for the Cooperative Research Centres (**CRC**) programmes to support AI-related projects. This funding is consistent with the Federal Government's allocation of $29.9 million over four years to strengthen Australia's AI and machine learning capability in the 2018–19 budget which has continued to date.[7]

The government has targeted their support of AI innovation in the areas of digital health, agriculture, energy, mining and cyber security. For example, funding was allocated to the CRC programme to address the skills deficit in the areas of AI and machine learning and AI projects.[8] Grants under this scheme also supported a core initiative by the Australian Council of Learned Academics to conduct research resulting in "*The effective and ethical development of artificial intelligence: An opportunity to improve our wellbeing*"[9] report published in 2019, which outlined Australia's AI capabilities and highlighted key considerations for the development of future regulations and industry coordination.

Relevantly, in March 2020, Standards Australia, which is officially recognised as the peak non-government standards development organisation in Australia, released a report: "*Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard"*, commissioned by the Department of Industry, Science, Energy & Resources, to assist in further guiding industry and regulatory development in the space.[10]

Similarly the data innovation network "Data61" of the Commonwealth Scientific and Industrial Research Organisation (**CSIRO**) has drafted key policy documents concerning best ethical practices for the use and implementation of AI through the release of its discussion paper "*Artificial Intelligence: Australia's Ethics Framework*" and subsequently the release of the AI Ethics Framework,[11] intended to help identify opportunities in AI and machine learning for Australia and its responsible development. Central to this framework is the development of Australia's eight core AI Ethics Principles.[12] These are designed to reinforce the centrality of social wellbeing, respect for diversity, autonomy and human rights, accountability, transparency and privacy, among other values, and to reinforce a governmental approach to guiding strategic and ethical best practice development of AI domestically.

More recently, in November 2019, the CSIRO's Data61 network in conjunction with the Department of Industry, Science and Technology hosted the "Techtonic" summit for over 100 industry leaders focusing on the future of AI in Australia.[13] This accompanied the release of Data61's AI technology roadmap "*Artificial Intelligence: Solving problems, growing the economy and improving our quality of life*".[14] The roadmap highlighted Australia's current AI capabilities and identified three areas of AI specialisation that it suggested Australia had a competitive advantage in – namely in the fields of: health, aged and disability care; mining and resource management; and urban planning and infrastructure – prioritising further development in those areas.

At the State level, governments have also begun to directly support and embrace AI. For instance, the New South Wales government held an "AI Thought Leaders Summit" in November 2019 to discuss policy support for and factors influencing the regional implementation of AI systems.[15]

Ownership/protection

When a company creates an AI algorithm, who is the owner?

An AI algorithm is any form of automated instruction given to an AI program to enable it to process and analyse data and generate a response. To the extent that an AI algorithm is software, then it is protected by copyright. If a company creates an AI algorithm using its employees, then the company will generally own the algorithm. If a contractor working for a company develops the algorithm, then in the absence of an agreement, the contractor will own the copyright in the algorithm. For this reason, there should be appropriate IP clauses in all contractor agreements concerning AI.

The AI algorithm may also be patentable if an individual incorporates an invention into the machine which carries out a scheme or method.[16] The US, China and Japan have the highest AI patenting activity.[17]

The ownership scenario may differ where a company uses cloud-based machine learning algorithms, which are made available as-a-service, or other third-party components. An example of such a cloud-based service provider is Google's TensorFlow, which is an open source AI library that uses data flow graphs to build models. In this way, TensorFlow offers companies the tools to build their own AI algorithms, allowing ease of access to what might otherwise be regarded as complex and unattainable technology. The use of this software is governed by the Apache 2.0 open source licence terms.

The majority of machine learning/AI providers (particularly those that are cloud-based) want to retain the ownership of AI models created on their platform, even though the models are not based on their data. The ownership of the algorithm will therefore depend on the terms and conditions, privacy and user licence agreements that apply to the particular provider.

Companies using these services should carefully review these terms to consider the ownership in any algorithm they develop.

As briefly discussed above, a related issue is how current liability laws will apply to AI technology. In Australia, liability can arise under the law of negligence if a duty of care is found to be breached, for example in circumstances where an AI algorithm poses a real threat of damage or harm to property. However it is more common for liability to be regulated at the contractual level, subject to applicable statutory conditions such as those found in the Australian Consumer Laws (**ACL**), and the laws relating to unfair contract terms. Liability can also be clearly established under the Australian product liability laws found within the ACL, for example manufacturers may be required to compensate a customer where a safety defect is the cause of loss or damage, including as a result of injuries suffered by an individual or the destruction to other goods.[18] Businesses supplying goods and services are likewise governed by certain consumer guarantees, for example, a requirement that their goods are of acceptable quality[19] and fit for the applicable purpose.[20] The current definition of "goods" in the ACL contemplates computer software,[21] and as the use of AI algorithms increases and becomes more complex, the concept of computer software as a "good" under the ACL is likely to be further tested.

What intellectual property issues may arise regarding ownership?

AI and big data raise new challenges under intellectual property law, particularly regarding ownership and in the areas of copyright. Two key issues are ascertaining who is the rightful owner of an algorithm, and who owns the AI output. Copyright subsists in Australia in an original work which has originated from the independent intellectual effort of a human author. Therefore, copyright becomes particularly challenging when the nature of big data and AI demands that manual "human" involvement be abandoned in favour of automated and computerised processes.

The application of this existing principle is exemplified in the case of *Telstra Corporation Limited v Phone Directories Pty Ltd*,[22] where it was found that copyright did not subsist in a computerised process that had been applied to create the White Pages and Yellow Pages directories, with substantial parts being automated with minimal or no human author.[23] New Zealand, on the other hand, has amended its copyright legislation to keep up with the changing landscape of AI, where the author for computer-generated works is considered to be the person "*by whom the arrangements necessary for the creation of the work are undertaken*".[24]

In addition to ownership, automation has generated significant issues surrounding access to data and records held by someone else. In the consumer world, there have been calls by individuals for rights to access their information, and legislated rights are being introduced. In November 2017, the Australian Federal Government announced the implementation of a "consumer data right". The consumer data right is intended to provide Australian consumers with greater control of their data, and will be initially rolled out within the banking sector in 2020, with the energy and telecommunications industries to follow shortly. The Australian Competition and Consumer Commission (**ACCC**) is leading the implementation of the consumer data right, in conjunction with the OAIC and CSIRO's Data61.

How are companies protecting their technology and data?

Companies are increasingly implementing measures to protect their technology and data. In an era where the law is consistently outrun by the pace of technological change, organisations cannot afford to be complacent about the potential cyber risks relating to their technology and data.[25] It is therefore incumbent on organisations to develop their own resilience framework and baseline governance.

To demonstrate their commitment to technology and data protection, organisations include cyber security measures as an ongoing cost of doing business, factoring it into their operations and resourcing it appropriately, having regard to the assessed risks. As cyber criminals (whether individuals, organised crime syndicates, terrorist groups or nation states) are becoming more sophisticated in their attacks, organisations are developing and practising cyber security arrangements, supported by appropriately skilled staff.[26] Key leaders in organisations are beginning to recognise that, ultimately, the approach to privacy governance, data protection, ethics, consumer-centricity and cyber resilience is established within the culture of an organisation.[27]

In line with demonstrating commitment to the protection of an organisation's technology and data, it is essential for organisations to develop their own baseline rules and frameworks to meet community, consumer, market and regulatory expectations. A thorough understanding of the privacy and security impact of these new technologies will be an increasingly important aspect of understanding an organisation's cyber risk profile. Organisations that are adopting AI and big data solutions should consider developing their own governance and ethical framework to guide decision making in relation to the use of this technology.

What are the applicable laws with respect to data ownership, security and information privacy?

The key laws in relation to data ownership, security and privacy in Australia include the Privacy Act, the Notifiable Data Breach Scheme and general data protection regulations.

The principle data protection legislation in Australia is the Privacy Act, which includes the APPs. The Privacy Act regulates how entities handle personal information, particularly "sensitive information" under the Privacy Act.[28] The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. There is a general requirement under APP 11 to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Any entity that holds personal information is responsible for ensuring the security of the information. The Australian Government has committed to reviewing and amending the Privacy Act, particularly in light of the increased usage of and power held by digital platforms such as Facebook and Google, including increasing maximum civil penalties to align with the penalties under the ACL;[29] "*amending the definition of 'personal information'…to capture technical data and other online identifiers; strengthening existing notice and consent requirements…; and introducing a direct right of action for individuals to bring actions in court to seek compensation for an interference with their privacy under the Privacy Act*".[30] The Australian Government in its periodic review of the Privacy Act[31] is also seeking to develop a binding privacy code applicable to online platforms that trade in personal information.[32]

All entities with existing personal information security obligations under the Privacy Act must also comply with the Notifiable Data Breach Scheme. The scheme requires organisations to notify the OAIC and affected individuals when an "eligible data breach" occurs. Eligible data breaches are those that may result in serious harm to the affected individuals. Due to the extraterritorial reach of the European Union's General Data Protection Regulation (**GDPR**), Australian entities may be required to comply with requirements under both Australian and EU privacy laws.

Antitrust/competition laws

What happens when machines collude?

The uptake of AI and machine learning technologies has seen increased adoption by

businesses of automated systems and AI-based algorithms designed to monitor and adjust prices. These systems may make it easier for competitors to achieve a form of collusion without formal agreement or human interaction.

With no human instruction, a price-setting AI algorithm could teach itself to coordinate with competitors, referred to as "*tacit algorithmic collusion*".[33] Given that tacit algorithmic collusion does not involve any element of human agency and is often conducted by systems that do not have explicable decision-making processes, it is difficult to regulate such anti-competitive behaviour.

In late 2017, significant reforms (referred to as the Harper reforms) were made to the *Competition and Consumer Act 2010* (Cth). The reforms included a new prohibition on "concerted practices" in section 45[34] and a revised misuse of market provision under section 46.[35] The new concerted practices provision is designed to prohibit "*any form of cooperation between two or more firms (or people) or conduct that would be likely to establish such cooperation, where this conduct substitutes, or would be likely to substitute, cooperation in place of the uncertainty of competition*".[36] The ACCC Chairman explained that this new prohibition addressed algorithmic collusion by moving away from having to establish a "*meeting of the minds*" to determine whether there has been anti-competitive collusion between competing businesses.[37] The revised misuse of market power provisions introduced a new "effects" test so that "*[a] corporation that has a substantial degree of power in a market must not engage in conduct that has the purpose, or has or is likely to have the effect, of substantially lessening competition…*".[38] This is a broader test and replaces the previous requirement to prove that corporations had taken advantage of their market power for one of three specific purposes.[39] The ACCC discussed the effect of this revised clause on the use of anti-competitive algorithms, stating that: "*[i]t may be difficult to establish that a firm with substantial market power had a proscribed anti-competitive purpose when deploying that algorithm. By focusing on the effect or likely effect of conduct, however, the new misuse of market power provision is fit-for-purpose to prohibit this conduct.*"[40]

While the ACCC has recently announced that it was developing its ability to analyse algorithms used for anti-competitive behaviour, including the establishment of a Data Analytics Unit,[41] as AI develops and is entrusted with greater decision-making ability, the challenges for regulators will likely become greater. However, the ACCC Chairman has delivered a strong message to those who use algorithm collusion, stating that "*you cannot avoid liability by saying 'my robot did it'*".[42]

What antitrust concerns arise from big data?

There is growing concern led by Australian and European antitrust authorities that monolithic technology companies, such as Facebook, Google and Amazon, have an unparalleled ability to access and harness big data to their own competitive advantage.

In July 2019, the ACCC released its final report on the *Digital Platforms Inquiry* which concluded that Google and Facebook possess substantial market power in their respective areas,[43] and have the "*ability and incentive to favour a business with which they have an existing relationship*".[44] Additionally, despite submissions from Google, that it does not favour its own ad inventory, and similarly from Facebook, that it is not vertically integrated, the ACCC is of the view that "*digital platforms with substantial market power, and which are present in related markets, have the ability and incentive to engage in…self-preferencing behaviour*".[45]

In response to the *Digital Platforms Inquiry* the Australian Government has introduced an implementation roadmap for a series of competition and consumer reforms, including asking the ACCC to assist in the development and implementation of a voluntary code of conduct to address concerns about bargaining imbalances between digital platforms and news media

businesses,[46] and the commitment of $27 million worth of funding for the establishment of a Digital Platforms Branch within the ACCC to monitor and report on, take necessary enforcement action against and conduct inquiries into digital platforms.[47]

Access to strategic information by vertically integrated companies, such as Google and Amazon can distort competition where market participants also operating as online retailers obtain access to information about competitors selling on the marketplace and their consumer behaviour. Vertically integrated operators may restrict the information received by downstream competitors regarding relevant transactions, or adjust their products and pricing more efficiently than non-vertically integrated competitors.

In 2018, the European Commissioner for Competition expressed concern that large companies could use access to mass data sets of consumers to hurt potential competitors. The Commissioner emphasised the value of big data but warned that "*[big data] can foreclose the market – [it] can give the parties that have [it] immense business opportunities that are not available to others*".[48] The Commissioner has continued this sentiment, stating in March this year that digital platforms have the potential to become "*so dominant that they're effectively private regulators, with the power to set the rules for markets that depend on those platforms*".[49]

In June 2017, the European Commission fined Google $2.8 billion for abusing its market power by systematically favouring its own comparison shopping service over competitors' in its search result pages. The European Commission found that this tactic stifled innovation and led to users not viewing the most relevant search results.

Board of directors/governance

Why is governance important for companies using AI and big data?

Good governance is imperative for companies to benefit from AI and big data. Issues arise when the rate at which the AI and big data technology progresses outstrips the pace of regulation. Where gaps in regulation exist, ensuring there is good governance of AI and big data will assist in ensuring that emerging technologies are used for fit and proper purposes. Improving the company's technological expertise, including on boards, to have sufficient understanding of the technology will also likewise strengthen the framework to help identify and address risks.

Since AI and big data technologies are underpinned by the collection and processing of information, companies need to protect against mishandling personal information which may lead to breaches of the Privacy Act and reputational damage. Governance is important to ensure adequate security and confidentiality protections are in place, key to guaranteeing compliance with existing obligations around security and privacy as required under the APPs.[50] Companies should also have clear and transparent policies to establish and maintain internal systems around the use of AI and big data. Where big data is de-identified, with the intention of reducing a company's risk of breaching the Privacy Act in its use of this information, there is the danger that the collection of various and large amounts of anonymous information about an individual can be combined down the track to transform it into personal data, and therefore may result in a breach of the APPs. Companies need to ensure strong de-identification processes are in place to counteract this risk.

How does AI and big data affect a board of director's duties?

As the law struggles to keep up with advances in AI and big data, directors must think and act proactively to ensure that they are complying with their directors' duties under

the *Corporations Act 2001* (Cth). Directors have various duties in their role of governing companies for the benefit of shareholders, members and other stakeholders. These include a duty to act with care and diligence,[51] and a fiduciary duty to act in good faith in the best interests of the company and for a proper purpose.[52]

The governance of a company must address the effects of big data and AI. For example, a director's duty to act with care and diligence may be breached by entering into high-risk transactions without the prospect of substantially benefiting the company. This may occur in a big data project, possibly yielding uncertain results and the time and cost-intensive process of coding the AI program. Despite the risks, boards are realising the need to invest in new technologies such as AI to remain competitive while acting in the best interests of the corporation.[53] As the development of these new technologies often exceeds general knowledge, a board of directors must also increase their technological expertise and ensure that they have reviewed all of the appropriate technical advice in order to satisfy the requirements of being fully informed, and be able to make an honest judgment about whether the uptake of this technology is in the best interest of the company. This includes a board's duty to implement robust security and confidentiality protections.

In addition, for certain regulated industries, such as banking, building societies, insurance companies and superannuation funds, the Australian Prudential Regulation Authority (**APRA**) imposes further requirements on directors of these regulated entities of meeting fit and proper standards (including having the necessary skills, knowledge, experience, diligence and soundness of judgment to undertake their duties).

Additionally, APRA imposed obligations on boards of APRA-regulated entities by way of prudential standard CPS 234, effective from 1 July 2019. The new standard explicitly requires that information security be the responsibility of board members. The board must endeavour to educate themselves as to information security risks and take initiative in both preventing and remedying data breaches. People who have been unwilling to comply with legal obligations, breached fiduciary duties or been negligent or deceitful are deemed to not be fit and proper. The capability of AI to make links between information collected as de-identified data may lead to an output of personal information which falls within the ambit of the APPs.

How does AI and big data affect the board of director's day-to-day activities?

Given the role of the board to monitor management and performance, AI and big data affect a board's agenda in that security, privacy and confidentiality must be constantly monitored and updated. The APRA standard CPS 234 (as outlined above) is a prime example of how developments in the technology sphere are creating additional requirements and obligations on entities and their boards. CPS 234 is relatively broad in its drafting, requiring the board to ensure a level of data protection "commensurate with the size and extent of the threats to its information assets". Ensuring such a level of protection will obviously require ongoing and adaptive efforts to help ensure data security in a rapidly evolving threat environment.

While the board of directors may rely on the APP guidelines to assist in relation to how the OAIC will interpret the APPs, there is currently minimal case law regarding how the courts will interpret the Australian privacy laws. Boards should take note of recent case law from 2019 which discusses the interpretation of the Privacy Act and the APPs.

In *Jeremy Lee v Superior Wood Pty Ltd*,[54] the Fair Work Commission held that the exemption in relation to employee records under the Privacy Act[55] only applied to the use and disclosure of employee records which are held by an organisation and does not apply to the creation of future records or records which are "*not yet in the possession or control of the organisation*".[56]

Boards should therefore be cautious when collecting new employee data and be aware that the employee record exemption may continue to be interpreted narrowly by superior courts. Additionally, boards should be wary of the case of *Shahin Enterprises Pty Ltd v BP Australia* which discussed the interpretation and application of APP 6 and APP 7,[57] dealing with the use and disclosure of personal information for the purpose of direct marketing. The Supreme Court of South Australia made a number of conclusions about APP 6 and APP 7, including that APP 7.2 authorises the use or disclosure of personal information for the purpose of direct marketing by that organisation which collected the data and does not allow for the disclosure of that data to a second organisation,[58] and that while APP 6 permits an organisation to use personal information for more than one purpose, the primary purpose should nevertheless be construed narrowly.[59] Boards should also therefore be cautious when considering the collection of personal information for the purpose of direct marketing.

As case law in this area develops, rather than taking the approach of "set and forget", boards must be aware of changes in privacy and security laws and update their internal policies regularly to ensure compliance.

This extends to response plans for data breaches and unethical use of AI. Boards of directors must have in place a response plan for these events that is continually reviewed and updated. Reputational damage caused by information security breaches has a real potential to impact profitability.

Further, under APP 1, APP entities are required to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs. As such, the APPs prescribe a "privacy by design" approach whereby privacy compliance is included in the design of projects from the outset, rather than added at a later stage of development. A board of directors, when guiding the company and making strategic decisions on AI and big data projects, must adopt this "privacy by design" framework.

How does AI and big data affect the due diligence process?

In a context where boards of directors are considering the strategic decision of acquiring further assets or conducting takeovers, the due diligence process is central in evaluating whether the decision is in the best interests of the company. AI can streamline due diligence processes by reviewing large amounts of information for standard considerations and risks. As with any technology, the use of AI has certain risks which boards should be aware of. Companies using AI and big data must invest not only in the AI, but also in the human resources required to train and develop the AI. While AI may reliably perform frequent, high-volume and repetitive tasks, without breaking down, the data inputted by human resources to code the AI is key to realising the benefit from this technology. The necessity for investment in the skill set of human resources to train and develop the AI is particularly important in the Australian context where AI-specific legislation does not yet exist. For example, for an AI system conducting a bulk review of contracts, human enquiry is essential to frame the scope of review and ask the right questions, such as problematic clauses to pick up on. Otherwise the assessment of the relevant risks may be incorrect.

There is also the risk of performance limitations of AI. Off-the-shelf AI software may be sufficient to review simple contracts. However, in the case of bespoke agreements, the lack of further human enquiry and input into the AI may mean that anomalies are not detected. In the context of deep learning AI, massive data sets are required for the AI model to become proficient at classification tasks and perform at the level of humans. Boards must therefore be aware of the need to invest resources into checking the final output produced by the AI, rather than relying on the assumption that it is correct.

Regulations/government intervention

Does your jurisdiction have specific laws relating to AI, big data or machine learning?

Federal and State governments have previously favoured an industry self-regulation model for AI, big data and machine learning. As such there are few laws specific to these areas in Australia. Nevertheless, the Privacy Act, the Notifiable Data Breach Scheme and general data protection regulations will generally apply to AI, big data and machine learning. Recently there has also been an increasing government focus and developing policy discourse in this area reflected by a number of initiatives relating to AI and machine learning, many of which we discussed above in considering the government's view on the adoption of AI.

Informed by the experiences of the European Union[60] in AI and machine learning, the government has, as we have outlined, commissioned various "road-maps" and "frameworks" intended to see legislative developments keep pace with evolving technology, whilst deriving further support via the promotion of industry best practice development via the AI Ethics Principles. Aside from this, there have been a number of instances of law reform in response to burgeoning technology, such as AI and big data (see next subheading).

Given the uncertainty of the form and pace of legislative change, to date many Federal Government initiatives have centred on creating a robust and adaptive framework to help identify opportunities in AI to assist in developing the technology. However, as the technology continues to mature and be implemented, it is likely that the government will address the legal concerns.

Are any law reform authorities considering specific laws relating to AI, big data or machine learning?

Various Australian Federal Government authorities and non-government bodies are driving law reform, shaping policy and advocating for the development of legislation governing AI and big data. Key to the development of laws has been ensuring that technological development occurs within the confines of existing Australian laws and regulations, such as privacy laws and data protection regulations. In addition to the various "roadmaps" and "frameworks" canvassed and *Artificial Intelligence: Australia's Ethics Framework* of CSIRO's Data61, the Australia Human Rights Commission has since 2019 engaged in an extensive consultation process to develop proposals for robust regulatory protections to address the impact of emerging technologies on human rights. In December 2019, it released an interim Discussion Paper on Human Rights and Technology outlining 29 proposals for establishing and enhancing Australia's human rights protection framework as it relates to emerging technologies with a key focus on AI and its use and implementation in decision-making procedures.[61]

What are governments considering and what should governments do to prevent adverse outcomes (e.g., the "AI robots take over" problem)?

Currently Australia is not a leading nation in the implementation of automation and AI, lagging behind global leaders across the G20 in adopting automation: 50 per cent fewer Australian firms are actively investing in automation compared to firms in comparable economies.[62] To remedy this and to prevent adverse outcomes, the government and private sector would need to work together to build a more dynamic innovation ecosystem, specifically in regard to developing and implementing automation technologies. Accelerating the deployment of AI across Australia would require organisations of all sizes – including a rising proportion of the small and medium-sized enterprises that contribute more than half of the country's GDP – to explore new data-driven processes and business models that would benefit from machine learning.

Despite Australia's slow adoption of AI, the Australian Federal Government is developing Australia's AI Ethics Framework to ensure AI is developed and applied responsibly in

Australia. AI has enormous potential to improve society and the government is carefully managing the risks that accompany the benefits of adopting AI. To date, the government has developed core principles of AI to ensure that the benefits of AI are still embraced in the context of regulatory and legal compliance, fairness, transparency and privacy protection.[63]

Further reform considerations may also be prompted upon the submission of the Australian Human Rights Commission's final report – set to be developed following the public consultations following the release of its discussion paper in April 2020. Many discussion paper proposals are heavily influenced by the EU's GDPR but purport to extend regulatory restrictions over a wider range of technologies in certain areas. For instance, many of the proposals address "AI-Informed Decision Making", which is also addressed by the GDPR; decisions which are wholly made by AI and have "a legal or similarly significant effect"[64] are subject to strict regulation. This includes decisions affecting financial circumstances (eligibility to credit), access to health services (triage systems), access to employment (recruiting tools), and access to education (university admissions). The discussion paper adopts a similar definition, however it expands the ambit to decisions that are only "materially" influenced by AI rather than wholly determined by it.[65]

Other notable regulatory proposals considered in the discussion paper include: requiring a right of (technical and non-technical) explainability for individuals subject to AI-Informed Decision Making;[66] the creation of a rebuttable presumption that the legal person deploying an AI-informed Decision Making system be legally liable for its use;[67] and the introduction of a moratorium on facial recognition technology for legal or similarly significant decision making, pending the development of further regulation.[68]

How does this relate further to discrimination and bias considerations?

Such proposals reflect concern among some stakeholders about the growing social impacts of AI and big data, especially on vulnerable communities. Many of these are spurred by worrying developments from some of the world's market leading companies experienced in developing and implementing AI decision-making systems. High-profile examples of this include Amazon's in-house built hiring tool, which was held back from deployment once it was revealed it unintentionally discriminated against hiring women for STEM jobs if they attended an all-women's college.[69]

In Australia, further concerns have been raised in respect of government deployments of AI in this space.[70] Notable examples include an algorithmic risk assessment tool used by NSW Police, which has been suggested to disproportionately impact Indigenous Australians by labelling them as possessing a higher risk of offending.[71] Further, in November 2019, the Federal Minister for Government Services announced the cessation of wholly automated debt discrepancy notices,[72] following criticism that use of an algorithm to identify discrepancies between welfare recipients' declared income (as reported separately to tax and welfare authorities) and actual income, in order to automatically generate a notice of debt to the individual concerned once a discrepancy was identified, had exacerbated the disadvantage of vulnerable persons.[73]

Thus, while reform in the use of AI and big data is likely to occur in the near term, nevertheless Australia has various anti-discrimination protections in place through dedicated legislation of various forms.[74] Furthermore, additional protections for "sensitive information" under the Privacy Act[75] will likely provide added protections in the interim for at least some forms of personal data including facial recognition data (and other biometric data).[76]

Acknowledgment

The authors would like to thank Anthony Small, a graduate in the Technology & Data practice at MinterEllison, for his contribution to the preparation of this chapter. Anthony is passionate about emerging technologies. Prior to joining the Technology & Data practice, he gained experience in MinterEllison's innovation team, and has worked with start-ups on drafting, negotiating and implementing SaaS and PaaS agreements.

Tel: +61 2 9921 8878 / Email: Anthony.Small@minterellison.com

* * *

Endnotes

1. 'Big Data', *Gartner* (Web Page) <https://www.gartner.com/it-glossary/big-data/>.
2. D Dawson *et al.*, 'Artificial Intelligence: Australia's Ethics Framework' (Discussion Paper, Data61 CSIRO, 2019).
3. *Ibid.*
4. See, e.g., Office of the Australian Information Commissioners, 'Developing Standards For Artificial Intelligence: Hearing Australia's Voice – Submission to Standards Australia' (Submission, 26 August 2019) <https://www.oaic.gov.au/engage-with-us/submissions/developing-standards-for-artificial-intelligence-hearing-australias-voice-submission-to-standards-australia/#footnotes>.
5. Sam Levin and Julia Carrie Wong, 'Self-Driving Uber Kills Arizona Woman in First Fatal Crash Involving Pedestrian', *The Guardian* (online, 20 March 2018) <https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe>.
6. See, e.g., National Transport Commission, 'Automated Vehicle Program' (October 2019), <https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Automated%20Vehicle%20Reform%20Program%20Approach%20%28October%202019%29%20-%20Public%20version.pdf>.
7. Commonwealth, *Budget Strategy and Outlook* (Budget Paper No. 1 2018–19, 8 May 2018) 1–23.
8. *Ibid.*
9. Toby Walsh, *et al.*, *The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve our Wellbeing*, (Report, July 2019) <https://acola.org/hs4-artificial-intelligence-australia/>.
10. Standards Australia, *An Artificial Intelligence Roadmap: Making Australia's Voice Heard* (Final Report, March 2020).
11. D Dawson *et al.*, 'Artificial Intelligence: Australia's Ethics Framework' (Discussion Paper, Data61 CSIRO, 2019).
12. 'AI Ethics Principles', *Department of Industry, Science, Energy and Resources* (Web Page, November 2019) <https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles>.
13. See Department of Industry, Science, Energy and Resources, 'Techtonic: Shaping Australia's Future' (Media Release, 27 November 2019) <https://www.industry.gov.au/news-media/techtonic-shaping-australias-ai-future>.
14. SA Hajkowicz *et al.*, Data61 CSIRO, *Artificial Intelligence: Solving Problems, Growing the Economy and Improving our Quality of Life* (Report, November 2019).
15. 'NSW Government AI Summit', *NSW Government – digital.nsw* (Forum Post, 2 December 2019) <https://www.digital.nsw.gov.au/article/nsw-government-ai-summit>.

16. *Commissioner of Patents v RPL Central Pty Ltd* (2015) FCAFC 177.
17. World Intellectual Property Organisation, *Technology Trends 2019: Artificial Intelligence* (Report, 2019) 15 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf>.
18. *Competition and Consumer Act 2010* (Cth) sch 2 ss 138–141.
19. *Ibid.* sch 2 s 54.
20. *Ibid.* sch 2 s 55.
21. *Ibid.* sch 2 s 2 (definition of 'goods').
22. *Telstra Corporation Limited v Phone Directories Co Pty Ltd* (2010) 264 ALR 617.
23. *Ibid.* at 335.
24. *Copyright Act 1994* (NZ) s(5)(2)(a); See also *Copyright, Designs and Patents Act 1988* (UK) c 1, s 9(3).
25. MinterEllison, *Perspectives on Cyber Risk 2019* (Report, March 2019) 4 <https://www.minterellison.com/articles/2019-perspectives-on-cyber-risk>.
26. *Ibid.* 28.
27. *Ibid.*
28. Section 6 provides that Sensitive Information includes biometric information used for the purposes of biometric verification or identification, or biometric templates.
29. Commonwealth, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Government Response, 12 December 2019) 8 <https://treasury.gov.au/publication/p2019-41708>.
30. *Ibid.*
31. *Ibid.*
32. *Ibid.*
33. Ariel Ezrachi and Maurice E Stucke, 'Algorithmic Collusion: Problems and Counter-Measures' (Paper No DAF/COMP/WD(2017)25, OECD Directorate for Financial and Enterprise Affairs Competition Committee, 21–23 June 2017).
34. *Competition and Consumer Amendment (Competition Policy Review) Act 2017* (Cth).
35. *Competition and Consumer Amendment (Misuse of Market Power) Act 2017* (Cth).
36. Explanatory Memorandum, Competition and Consumer Amendment (Competition Policy Review) Bill 2017 (Cth) 28 [3.19].
37. Rod Sims R, 'The ACCC's Approach to Colluding Robots' (Speech, Conference – Can Robots Collude? 16 November 2017 <https://www.accc.gov.au/speech/the-accc%E2%80%99s-approach-to-colluding-robots>.
38. *Competition and Consumer Act 2010* (Cth) s 46.
39. Revised Explanatory Memorandum, Competition and Consumer Amendment (Misuse of Market Power) Bill 2016 (Cth) 9 [1.21].
40. Rod Sims R, 'The ACCC's Approach to Colluding Robots' (Speech, Conference – Can Robots Collude? 16 November 2017 <https://www.accc.gov.au/speech/the-accc%E2%80%99s-approach-to-colluding-robots>.
41. *Ibid.*
42. *Ibid.*
43. Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, 26 July 2019) 8–9, 58 <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>.
44. *Ibid.* 12.
45. *Ibid.* 136.
46. Commonwealth, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Government Response, 12 December 2019) 8 <https://treasury.gov.au/publication/p2019-41708>.

47. *Ibid.*
48. Natalia Drozdiak, 'EU Asks: Does Control of 'Big Data' Kill Competition' (2 January 2018) *The Wall Street Journal* <https://www.wsj.com/articles/eu-competition-chief-trackshow-companies-use-big-data-1514889000>.
49. Margrethe Vestager, 'Keeping the EU Competitive in a Green and Digital World' (Speech, College of Europe, Bruges, 2 March 2020) <https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/keeping-eu-competitive-green-and-digital-world_en>.
50. *Privacy Act 1988* (Cth).
51. *Corporations Act 2001* (Cth) s 180.
52. *Ibid.* s 181.
53. *Ibid.* s 181(1).
54. *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 (1 May 2019).
55. *Privacy Act 1988* (Cth) s7B(3).
56. *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 (1 May 2019) [55-56].
57. *Shahin Enterprises Pty Ltd v CP Australia Pty Ltd* [2019] SASC 12.
58. *Ibid.* [202].
59. *Ibid.* [186].
60. Andrew Carrington, 'Artificial Intelligence and government regulation' (11 October 2017) *GovernmentNews.com.au* <https://www.governmentnews.com.au/artificial-intelligence-government-regulation/>.
61. Sophie Farthing *et al.*, 'Human Rights and Technology' (Discussion Paper, Australian Human Rights Commission, December 2019).
62. D Dawson *et al.*, 'Artificial Intelligence: Australia's Ethics Framework' (Discussion Paper, Data61 CSIRO, 2019).
63. *Ibid.*
64. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), Article 22.
65. Sophie Farthing *et al.*, 'Human Rights and Technology' (Discussion Paper, Australian Human Rights Commission, December 2019) 190. See Proposal 5.
66. *Ibid.* See Proposal 7/8.
67. *Ibid.* See Proposal 10.
68. *Ibid.* See Proposal 11.
69. Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women', (10 October 2018) *Reuters* <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.
70. See discussions of these and other cases in Sophie Farthing *et al.*, 'Human Rights and Technology' (Discussion Paper, Australian Human Rights Commission, December 2019).
71. Michael McGowan, 'More than 50% of those on Secretive NSW Police Blacklist are Aboriginal', *The Guardian* (online, 11 November 2017) <https://www.theguardian.com/australia-news/2017/nov/11/more-than-50-of-those-on-secretive-nsw-police-blacklist-are-aboriginal>.
72. Paul Farrell, 'Government Halting Key part of Robodebt Scheme, will Freeze Debts for some Welfare Recipients', (20 November 2019) *ABC News* <https://www.abc.net.au/news/2019-11-19/robodebt-scheme-human-services-department-halts-existing-debts/11717188>.

73. Richard Glenn, Commonwealth Ombudsman, *Centrelink's Automated Debt Raising and Recovery System: A Report about the Department of Human Services' Online Compliance Intervention System for Debt Raising and Recovery* (Report No. 02/2017, April 2017) 4 <https://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf>; Senate Community Affairs References Committee, *Design, Scope, Cost Benefit Analysis, Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative* (Report, 21 June 2017) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/SocialWelfareSystem/Report>.
74. See *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Australian Human Rights Commission Act 1986* (Cth); *Disability Discrimination Act 1992* (Cth); *Age Discrimination Act 2004* (Cth); and *Fair Work Act 2009* (Cth).
75. Section 6 provides that Sensitive Information includes biometric information used for the purposes of biometric verification or identification, or biometric templates.
76. See, e.g., Australian Privacy Principles 3,6 and 7.

Anthony Borgese
Tel: +61 2 9921 4250 / Email: Anthony.Borgese@minterellison.com

Anthony Borgese has extensive experience assisting clients in their IT, telecommunications and complex outsourcing arrangements. His practice includes data and privacy advice, domestic and cross-border outsourcing, reviewing and negotiating long-term supply and outsourcing arrangements, vendor management, cloud computing, technology disputes and cyber security. Anthony leads the outsourcing team with over 20 years' experience of delivering strategic, commercially focused solutions within the ICT arena for client organisations. He has a solid understanding of the commercial drivers of a wide range of both public and private sector organisations and service providers.

Anthony is recognised for his expertise in leading independent guides such as *Best Lawyers* in the areas of commercial law, information technology law, outsourcing law and telecommunications law, and is listed as a Leading Individual in *Chambers Asia Pacific* (TMT: IT category).

Jonathan Thompson
Tel: +61 2 9921 4827 / Email: Jonathan.Thompson@minterellison.com

Jonathan Thompson is a lawyer in the Technology & Data practice at MinterEllison.

Jonathan advises private and public sector clients on a range of technology-related matters, including outsourcing and IT supply agreements, IT transitional service arrangements and data protection. Jonathan also works closely with clients as they navigate the complex economy-wide regulatory reforms impacting Australia's technology and telecommunications industries, including the Consumer Data Right. Jonathan has also fostered a keen interest in emerging disruptive technologies as they intersect with the law.

Alice Scamps-Goodman
Tel: +61 2 9921 4395 / Email: Alice.ScampsGoodman@minterellison.com

Alice Scamps-Goodman is a lawyer in the Technology & Data practice at MinterEllison.

Alice has experience working with private and public sector clients on a range of commercial matters including drafting ICT procurement agreements, conducting due diligence as part of private M&A acquisitions and advising on general commercial contractual matters.

MinterEllison

Level 40 Governor Macquarie Tower, One Farrer Place, Sydney NSW 2000, Australia
Tel: +61 2 9921 8888 / URL: www.minterellison.com

Austria

Günther Leissler & Thomas Kulnigg
Schönherr Rechtsanwälte GmbH

Trends

Artificial Intelligence (AI), Machine Learning and Big Data are still trending topics in Austria's tech and start-up scene.

AI and Machine Learning

The Austrian Council on Robotics and Artificial Intelligence (ACRAI) has summarised details, facts and figures on the status of AI and Machine Learning in Austria in a comprehensive study published in May 2019.[1] Here are the main takeaways of the study:

- The study identified more than 600 companies in Austria that are active in the area of AI, which is still only a fraction of all Austrian companies.
- Most AI-related companies are software developers, who offer data processing solutions, often in combination with consulting services.
- Approximately a quarter of all identified companies are active in the area of consulting services (business or market consulting), developing their own software solutions to analyse company information, stock prices, etc. Production companies (such as mechanical engineering, plant construction, electrical equipment, pharmaceutical products, sensors, etc.) represented 28% of the identified companies.
- There are further several institutions active in AI, including specific institutions (such as the the Austrian Research Institute for Artificial Intelligence of the Austrian Society for Cybernetic Studies[2]) and larger institutions, such as universities.
- Public subsidies, including Horizon 2020 projects, reached EUR 350 million.[3]
- R&D in AI is generally widely spread throughout Austria (with focus on Vienna, Graz, Linz/Hagenberg and Klagenfurt).
- Start-ups further play an important factor in the AI industry in Austria; they are generally considered as technology leader and competence centres, with AI-as-Service as a potential new business model for start-ups and other players.
- Lack of personnel, for instance neuronal network and software engineers, are one of the major constraints for AI, as well as the cost for obtaining/creating the relevant know-how and the implementation of innovation. Also, the current AI hype may create wrong expectations (and could trigger disappointments). General restraints and lack of data (in the required quality and quantity) are further hurdles and challenges to AI in Austria.

Further, from our perspective as market participants, we see more and more AI/Machine Learning activities by MedTech start-ups, aiming to create artificial doctors, such as radiologists, or automising the interpretation of medicinal test results or images (e.g. retina scans). This area of AI application has become significant recently, with telemedicine generally being on the rise (especially in the current Corona situation). Also, the combination

between the distributed ledger technology (a.k.a. the "Blockchain") and AI is a trending topic in Austria (and overall) due to the importance of having tamper-proof databases and logs for the purposes of verifying decisions taken by AI algorithms, in particular when used by authorities or corporations.

By way of an outlook, in its 2020–2024 governmental programme,[4] the Austrian Federal Government promised to foster an eco-system for innovation through connecting start-ups, R&D institutions and public/private media houses to support, *inter alia*, AI technology, with the goal of strengthening the international competitiveness of Austria. It remains to be seen if the promises of the Austrian Federal Government will be kept.

Big Data

It comes with no surprise that in light of the world's data-based attempts to fight the Coronavirus that Austria has also reverted to Big Data and data exploitation mechanisms. As with many other states, Austria attempts to combat the spread of the virus by collecting and evaluating mass data. This approach is inspired by other countries such as, for example:

- Israel: Launch of a cellphone surveillance system. This system allows identifying whether someone has been in contact with a Coronavirus-infected person and to messages that person ("*You were near someone sick with the Coronavirus. You must immediately isolate at home [14 days] to protect your relatives and the public […]*").[5]
- South Korea: Contact tracing. South Korea goes beyond mass alerts in regions of suspected Corona infection. It believes in the efficiency of retracing the latest movements of individuals that have been positively tested for the Coronavirus and to isolate anyone who, according to his/her identified motion pattern, has been in contact with those infected individuals. Such contact tracing includes not only an analysis of the individual's cellphone location data, but also of his/her credit card records, CCTV footage and other available data sources.[6]
- China: China relies on a similar approach. Apps will alert individuals if they had been in contact with infected persons and ask them to stay at home and to contact the local health agency.[7]

Such concepts have proven their effectiveness. Most recent data has shown that the infection rate in South Korea has flattened and China has even announced a zero notice of new infections. The flip side of the coin, however, is a loss of people's privacy.

Austria has taken the middle ground by balancing the effectiveness of such preventive measures against data protection limitations. The outcome has been an amendment to the Austrian Telecommunications Act which entitles the government to request telecommunications providers to send nationwide or regional SMS mass alerts to their users if a public emergency (such as an outbreak of an infectious disease) occurs in that region.[8]

With this, Austria allows compulsory mass alerts but refrains from governmental tracking systems as they are in place in countries like South Korea or China. Instead, comparable systems are made available on a voluntary and non-governmental basis. For example, the Austrian Red Cross (an Austrian rescue service provider) has developed an app which provides several features, including "electronic handshake logs". Such log data shall allow alerts to contact persons of the app user as soon as the app user himself gets positively Coronavirus-tested. However, besides this app being a non-governmental app, it operates on a voluntary basis. In contrast to this, the tracing systems used in China or South Korea are operated on a governmental level and without allowing people to choose whether they want to participate. Also, under the Austrian model, contact persons will only be added to the user's handshake logs if they have agreed to being added. This means the system does

not allow the tracing of each and every contact person; rather, only those contact persons who have given consent. In essence, compared to the Asian systems, the Austrian concept accepts lower system efficiency to the benefit of maintaining higher privacy standards.

Also, one of the country's largest telecommunications providers has, on its own initiative, provided the government with large-scale location data of its users in order to allow the government to verify people's acceptance of quarantine orders. However, in order to safeguard users' privacy, the data was anonymised before it had been provided to the government. This was done by creating movement clusters of at least 20 users so that no individual profiles of movement could be extracted from that data.

Ownership/protection

Computer programs may enjoy copyright protection under specific provisions on the protection of computer programs (Section 40a of the Austrian Copyright Act; UrhG). In accordance with the EU Software Directive (Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs), protection applies to the expression in any form of a computer program. However, ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright.

Under current legislation, only natural or legal persons can hold rights; a machine itself may not be the owner of a right. Thus, every intellectual property right must be allocated to a person. In respect to copyright and patent, only natural persons may be the creator or inventor. This can lead to interesting questions in the context of work products created by AI/Machine Learning systems. According to legal theory, either the owner of the algorithm or the person that applied the algorithm becomes the owner of its work products (or both). Alternatively, none of them becomes the owner if their contribution to the AI/Machine Learning system does not qualify as an "intellectual" or "spiritual" creation, and the creation was truly autonomously developed by the system.

Antitrust/competition laws

Current antitrust rules are flexible enough to deal with most competition law problems created by the use of AI/Machine Learning algorithms. There is uncertainty, however, as to whether future developments in digitalisation will necessitate broadening the extent of the cartel prohibition. This notwithstanding, competition authorities need to stay on top of technological developments and keep improving their expertise on algorithms.

Board of directors/governance

There is little discussion going on in Austria regarding whether management decisions of an Austrian company may be taken by AI. This is mainly because under Austrian corporate law, directors remain responsible for their decisions even if the decision is influenced, supported or even taken by an AI application. From a management liability's perspective, it remains to be seen to what extent managers can exculpate themselves on the argument that a decision was based on the results of an AI application. Managers are well advised to double check (at least for plausibility) whether the basis of their decision is adequate in the given circumstances, to avoid any personal liability caused by their decision. This will be particularly difficult in respect to AI algorithms due to the complexity of the underlying technology (e.g. the manager will have to ensure that the results of the application are not influenced by hidden or unwanted factors) and also because AI applications typically use large amounts of data

(and it is quite difficulty to verify the quality of the underlying data). It also will need to be ensured that the results of the algorithm can be verified and reproduced, to be able to later audit the decision of the manager. As outlined above, a combination of AI and distributed ledger technologies could provide the basis for such criteria.

Regulations/government intervention

AI and Machine Learning

On 8 April 2019, the High-Level Expert Group on Artificial Intelligence – a supportive body to the European Commission – launched their "Ethics Guidelines for Trustworthy AI". According to the guidelines, Trustworthy AI has three components, which should be met throughout every AI system's lifecycle: AI systems should be (i) lawful, (ii) ethical, and (iii) robust. Thus, legal compliance ("lawfulness") alone shall not be sufficient anymore. Based on this theory, the guidelines aim to offer guidance on ethical and robust AI. These requirements will go through a piloting process expected to conclude with the presentation of a revised document in early 2020; to our understanding, the process is still pending. In Austria, no specific AI regulation has been implemented yet. However, this does not exclude applicability of other frameworks of relevance. Often, AI systems are typically based on the exploitation and the use of data. If such data counts as personal data, the limitations and requirements of the GDPR will apply. Thus, a key AI component is a valid anonymisation of the AI-related database.

Big Data

Features like the "electronic handshake log" (described above), or equivalent, are partly based on the processing of personal data in terms of the GDPR. This is because Art 4 Para 1 GDPR qualifies not only information as personal data that relates to identified persons but also where such data relates to persons that are identifiable. In its decision in the *Breyer* case, the CJEU took a very broad view on the question of whether an individual shall be deemed identifiable. In essence, the court took the view that data shall be deemed "personal" as long as it is not practically impossible or prohibited by law to identify the person the data relates to.[9] Features like the "electronic handshake tool" doubtlessly involve personal data processing. This is the case when the user gets positively Corona-tested and provides through this system this information to the Austrian Red Cross. Such information is not only personal data. In the context of the described system, it describes the health status of the app user and, as such, forms a special category of data in terms of Art 9 GDPR. Since the use of the app is voluntary its data processing requires consent as enshrined in Art 9 Para 2 lit a GDPR. Such consent needs to be freely given and in full knowledge of all the details of the data processing. This seems doable *vis-à-vis* the user of the app. So the Austrian Red Cross has provided comprehensive data protection information which shall form the basis for the app user's consent.[10]

However, things get trickier when it comes to people who get in touch with the app user. In other words, those "contact people" who provide their "electronic handshake" to the app user. Such contact people are identified by the system as soon as the app user discloses that he is infected by the Coronavirus because if the app user has been infected by the Coronavirus his contact people could potentially be infected as well. Therefore, they will receive alerts telling them to isolate themselves. From a data protection perspective, as soon as they become identified by the "relevant" handshakes, their personal contact data gets processed in context with their health status. This is because an indication of a potential COVID-19 infection is arguably information about an individual's health status. This leads to the consequence that

such contact persons must declare their consent to their data being processed as personal health data (in case the app user turns out to be infected). The responsibility for obtaining such consent is with the app user, since he is the controller for the "electronic handshake".[11] However, it might be doubtful that the average app user indeed provides such comprehensive information to his/her contact person while performing the "electronic handshake" and that the contact person arguably understands all of the consequences arising from his/her allowance to get captured in the app user's "electronic handshake logs" – with the effect that such consent might potentially be insufficient.

The above shows the pitfalls of a voluntary tracking system. On the one hand, it is by its nature less effective because it does not apply throughout the entire population. On the other hand, for the above reasons, it is not legally sound in all its nuances. An alternative could be the establishment of such systems on a compulsory basis through statutory enactment. This approach has obviously been chosen by countries like China and Israel. Art 9 GDPR does not *per se* prevent states from doing so. In particular, Art 9 Para 2 lit i GDPR allows the processing of special data categories on the grounds of public health interests. However, such processing is only legitimate on the basis of national laws that provide suitable privacy safeguards. So here it is up to the legislator to balance the benefit of compulsory health data processing against the population's privacy interests.

For Austria, the outcome has been that the legislator (at least for now) has not taken any steps further than obliging telecommunications providers to send out SMS alerts to their users upon governmental orders (see above). So, obviously the legislator did not deem the threat of Coronavirus to be severe enough to deprive people of their privacy in such an intrusive manner as it would be the case with compulsory contact tracing. This, however, is merely a snapshot in time and the legislator's evaluation might change if the currently taken measures turn out to be not efficient enough in order to effectively combat the Coronavirus.

Criminal issues

Besides the government's ambitions to reduce the spread of the Coronavirus, there remains a strong element of self-responsibility with each individual. Not complying with quarantine orders or circumventing regional access restrictions might, depending on the case, trigger administrative fines. An even more serious consequence, however, is enshrined in Sections 178 and 179 of the Austrian Criminal Code whereby negligently or deliberately exposing the public to infectious diseases shall be sanctioned by up to one year (in case of negligence) and up to three years (in case of deliberate action) of imprisonment. This adds another consideration to the scenario: Does someone who denies or withdraws consent to the processing of his/her health data arguably impede the efforts to eradicate the Coronavirus and be deemed to be acting negligently within the meaning of the Criminal Code? On an overall view, it should be far off from any criminal liability if an individual refrains from contributing to a data mining process, as it would be the case with an individual denying consent to his participation in a voluntary tracing system. However, there might be scenarios where such liability comes closer than it initially seems. One might imagine a scenario under the discussed Red Cross app where a contact person first agrees to the electronic handshake, but immediately after his handshake was added to the app user's log data he realises that the app user is coughing or sneezing. If that contact person then withdraws his consent in fear of his upcoming isolation, this might come close to what is prohibited under the Austrian Criminal Code. Notwithstanding, of course, the burden of proof aspect since it would be with the state prosecutor to provide evidence for the discussed negligence.

Data anonymisation

The above considerations show that each type of tracing related to personal data processing has its limits. Voluntary tracing meets consent restraints, compulsory tracing means severe loss in privacy. A feasible compromise might be data anonymisation. Data is deemed anonymous if the data does not contain information about individuals. If data is anonymous it can be processed without the limitations of the GDPR, as it has arguably been the case with Austrian telecommunications providers when providing mass user data to the government to allow verification of people's quarantine acceptance. As stated, whether or not data shall be deemed personal depends on whether it relates to an identified or identifiable individual. The Austrian Data Protection Regulator has taken a somehow liberal view on that point. The authority was asked whether data anonymisation can be deemed valid data deletion under the GDPR and has accepted deletion through anonymisation. It is of particular relevance for the present context that in its decision the regulator has explicitly accepted that anonymised data might become identifiable again through future, more enhanced technical means.[12] At least for Austria it seems deducible from those considerations that data can validly be claimed to be anonymous if, for the time being, the data-related individual cannot be identified anymore although that individual's re-identification might become possible in the future. Under this perspective, data mining and data exploitation activities can arguably be carved out of the GDPR's applicability if it is sufficiently ensured that at the time of the processing the individuals' identities can arguably not be determined. This might be the case if data pools, or equivalent anonymisation tools, prevent individualised evaluations. By following the regulator's arguments, it seems not immediately harmful if such anonymisation does not ultimately prevent future de-anonymisation as long as the anonymisation is diligently done at its origin.

* * *

Endnotes

1. https://www.bmvit.gv.at/dam/jcr:abf0cdc3-bd4c-4335-aef9-8e5b0a33c119/ai_potenzial_oesterreich.pdf.
2. http://www.ofai.at/index.html.
3. Between 2012 and 2017.
4. https://www.bundeskanzleramt.gv.at/bundeskanzleramt/die-bundesregierung/regierungsdokumente.html.
5. https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus?t=1585132364406.
6. https://www.nytimes.com/2020/03/23/world/asia/coronavirus-south-korea-flatten-curve.html.
7. https://abcnews.go.com/Business/china-launches-app-combat-coronavirus-spread/story?id=68907706.
8. Section 98a Telecommunications Act, as amended through the Second-Covid-19-Act: https://www.parlament.gv.at/PAKT/VHG/XXVII/A/A_00397/index.shtml.
9. CJEU 19 October 2019, C-582/14.
10. https://www.roteskreuz.at/fileadmin/user_upload/Stopp_Corona_App_DatenschutzInformation__OeRK_24.03.2020_V1.1.pdf.
11. This is supported by the Austrian Red Cross' data protection information which allocates the said controller responsibility to the user.
12. DPA's decision DSB-D123.270/0009-DSB/2018, dated 5 December 2018.

Günther Leissler
Tel: +43 1534 375 0276 / Email: g.leissler@schoenherr.eu
Günther Leissler is a partner with Schoenherr, where he specialises in data protection, telecommunications and life science regulation. Günther heads the Data Protection Group of Schoenherr.

Thomas Kulnigg
Tel: +43 1534 375 0757 / Email: t.kulnigg@schoenherr.eu
Thomas Kulnigg is a partner with Schoenherr, where he specialises in technology M&A and venture capital transactions, start-ups and digitalisation matters. Thomas heads the Technology & Digitalization Group of Schoenherr.

Schönherr Rechtsanwälte GmbH

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 37 0 / URL: www.schoenherr.eu

Belgium

Steven De Schrijver
Astrea

Trends

Readers of Belgian newspapers saw the following headline in October 2019: "Belgian artificial intelligence manages to predict heart attacks", relating to technology created by a Brussels start-up and the French-speaking Free University of Brussels (ULB) that is able to predict atrial fibrillation 30 seconds before it appears, with a precision rate of 80%. This could be a medical breakthrough for Artificial Intelligence (AI).[1]

Such news certainly contributes to the findings of a recent poll by the Belgian Federal Ministry of Economy, wherein 72% of Belgians said they feel that AI is a positive development for society. While 72% of Belgians feel AI would create new jobs, 20% fear their function would disappear with the appearance of AI.[2] Based on a further recent poll by Ipsos, 54% of Belgians are confronted with AI at work, which is more than in France (44%), Germany (45%) and the UK (47%). In addition, 24% of the employees use AI-based applications at work, which is also more than in France (16%), Germany (15%) and the UK (20%).[3]

2019 was a breakthrough year for governmental action in Belgium with the adoption of a Federal, Flemish and Walloon plan for the development of AI (as much of the economic policy of the country is in hands of the local regions). The Federal government created "AI 4 Belgium", a platform that should enable Belgian citizens and organisations to capture the opportunities of AI while facilitating the ongoing transition responsibly, so that Belgium becomes the main European research centre for AI.[4]

Wallonia will invest €900,000 in AI next year, and Brussels an additional €4m in the next few years.[5] In April 2019, Microsoft and the coding school BeCode opened an educational course on AI together with five other tech companies. They have the ambition to create nine AI schools in Belgium, so that each year 350 to 500 AI specialists can be trained.

Apart from that, the Flemish government has created the "Flemish Action Plan Artificial Intelligence" which will each year invest €32m in AI, including in research (€12m) and the development of AI at companies and their digitalisation (€15m). €5m of funding will go to education about AI and the creation of a Knowledge Centre of Ethics which will discuss the ethical aspects of AI. The goal is to give 100,000 Flemish people within three years basic knowledge about AI.[6] This plan also contributed to the faster creation of an AI Experience Centre with the Dutch-speaking Free University of Brussels (VUB) which creates a platform for 200 AI researchers to show companies and organisations how to use AI.

This chapter intends to touch upon a number of legal subjects concerning AI, Machine Learning and Big Data, focusing primarily on the Belgian point of view thereof. As Belgium is a member of the European Union and adopts European laws, many fields of law (such as competition law or intellectual property rights law) are of course heavily influenced by

European law. Hence, some legal solutions that are or will be introduced in Belgium will closely follow the law of the European Union.

In that sense, it is expected that the European Commission's long-awaited White Paper on Artificial Intelligence, which was published on 19 February 2020, will invite legal scholars and governments in Europe to debate even more on the way how AI must be regulated, taking into account both the many benefits it may bring as well as its risks. Interestingly, the European Commission has stated in its White Paper that a solid European regulatory framework for trustworthy AI should be expected as it will protect European citizens and help create a frictionless internal market for the further development and uptake of AI as well as strengthening Europe's industrial basis for AI. The White Paper foresees a risk-based approach to regulating AI, based on whether the relevant sector and intended use involve significant risks, especially with regard to the protection of safety, consumer rights and fundamental rights. This would lead to a targeted regulatory framework which provides legal certainty.

Ownership/protection

Copyright law

Copyright law is dealing with two main questions regarding AI:

(i) How can the works that are created by AI be protected?

(ii) Who can be held liable if a copyright relating to a certain work is violated by an AI system?

Under Belgian law, copyright protection is enjoyed by the physical author that effectively creates the work. Such work must be in a concrete form (*e.g.* ideas cannot be protected, but texts or websites can) and it must constitute an original creation (which is understood as a human creation that is sufficiently original, whereby the author included his personality and intellectual work in the creation).

Hence, the (human) author of a work that is created with the use of AI will enjoy copyright protection if a direct connection is established between his input (the efforts to create a concrete and original work), and the output (the work itself). The AI system itself, created by a human, will enjoy copyright protection too.

In principle, the copyrights on works created by employees in fulfilment of their employee obligations are held by the employee himself and not by his employer. Consequently, the employer cannot use or transfer these creations without the consent of his employee. To avoid this, the employer can include the transfer of copyrights in the respective employment agreement of the employee. This must be done expressly and in writing. Such a transfer can also be included in the work rules of the company, whereby it must be proven for the transfer to be valid that the employee gained effective knowledge of the transfer under the work rules. All these agreements must be drafted in clear terms, as, in case of doubt, they will be interpreted in the benefit of the employee. Moral rights, however, cannot be transferred.

However, the regime applying to copyrights on computer programs (software) and certain databases is different, as for these type of works, unless agreed otherwise, the employer will be presumed automatically to hold the copyrights (at least the patrimonial rights in relation thereto) and not the employee. This exception is thus important with respect to companies that develop AI and other related systems.

By contrast, a work that is created by a self-learning AI system may not be protected by copyrights in favour of the creator. After all: (i) it will not be created by a human author;

and (ii) it will not show an element of creativity in the form of an inclusion of the author's personality in the work.

In order to avoid that developers of AI systems will not benefit from special protection for the work they have invested in, it should be considered whether a right *sui generis* for the copyright protection of AI and other related systems should be created, which could be comparable to the *sui generis* right given in Europe to protect the producers of databases.

If an AI-driven system violates the copyrights attached to a certain work itself, the liability for such breach must also be established. If the AI is merely used as a tool by a human, it may be argued that the person (or the legal entity behind the person), being in control of the system, should be held liable for the breach as he or she instructed the system to create, for instance, unlawful reproductions of the protected work.

If AI breaches copyrights itself based on its self-learning capabilities, it may be more difficult to establish its liability. For more on the issues related to this, we refer to the section on civil liability below.

Patent law

Under Belgian (and European) law, an invention can be protected by a patent if it: (i) is novel (so that it is not part of the current state of the technique); (ii) is inventive (shows inventive activity); (iii) has industrial applicability; and (iv) is lawful. Such invention must have a technical character, which means that it provides a technical solution to a technical problem.

Scientific theories, mathematical methods (such as algorithms) or software do not enjoy the protection of patent law. However, software that has further technical effects may qualify for patent protection as a computer-implemented invention if it serves the solution of a specific technical problem (*e.g.* steering an autonomous car). Hence, only under certain conditions AI may be patentable. Otherwise, intellectual property right protection should rather be sought under copyright law.

The same questions as reviewed under copyright law will arise with respect to patent law. Where a human creates inventions using AI, he will be reasonably found to be the inventor. If AI would create a patentable invention itself, it is yet undetermined whether it could have rights to a patent itself or whether its creator could enjoy a *sui generis* right that protects the invention.

Interestingly, the European Patent Office (EPO) has recently refused to grant patents to two inventions that, according to the applicants, were created by AI without any human intervention. The EPO stated that the inventor designated in the application has to be a natural person and not a machine based on the interpretation of the legal framework of the European patent system and internationally applicable standards. The EPO added that it is mandatory for an inventor to be a natural person as the designation as inventor bears a series of legal consequences, notably to ensure that the designated inventor is the legitimate one and that he or she can benefit from rights linked to this status. To exercise these rights, the inventor must have a legal personality that AI or machines in general do not have.

Belgian law does not regulate whether the employer or the employee may patent the invention created by the employee during the performance of an employee's obligations. This must be further determined contractually between the parties in the employment agreement. Courts also do not always present a clear answer to this question. If an invention is made as a result of the performance of the normal tasks of an employee (*e.g.* who works in a R&D centre), the rights to the invention will be held by the employer. The same goes for inventions which are clearly linked to the activities of the company, as the employee can then only create

an invention by using the equipment and know-how of the company (with or without the company's consent). However, even if an employee is granted the rights to a patent, he will not always be able to exercise these rights as he may breach his confidentiality obligations under his employment agreement by doing so.

Trade secrets

Pursuant to Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, a trade secret: (i) is a secret that is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (ii) has commercial value because it is secret; and (iii) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret (*e.g.* contractual confidentiality obligations, security measures).

If an AI system or similar technologies are kept secret and are not generally known by other persons dealing with AI technology, the provisions of this Directive and the transposed provisions of Belgian law may apply. More specifically, the company that holds the AI technology may act against unlawful acts such as unauthorised access to the documents or electronic files concerning the AI system, the copy thereof, or the breach of a confidentiality agreement. The owner of the technology can also act against third-party recipients of the trade secrets, provided that such a third party, at the moment of receipt, uses or discloses a trade secret which was unlawfully obtained and where the third party had knowledge of or should have had knowledge of the unlawful character of the trade secret.

The legitimate owner of the trade secret may, amongst others, obtain a cease-and-desist order against the unlawful user of the trade secret and/or claim damages for all losses caused by the unlawful obtaining, use or disclosure of the trade secrets.

Antitrust/competition laws

The Belgian rules regarding anti-competitive behaviour largely correspond with the European law on anti-competitive agreements and the abuse of a dominant position (Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU)), supplemented by the Court of Justice's case law.

As almost any field of law, competition law will also need to find new tools against breaches of competition rules by or with the use of AI-driven tools and other similar technologies. There are various potential issues. In online retail, it is already known that certain algorithms determine prices based on the patterns of client behaviour, as a consequence of which certain products may be more expensive in one neighbourhood than in another, solely because it is inhabited, for instance, by richer persons. An automated system may also show a different product price for a customer of whom it is known that he or she particularly likes the category to which the respective product belongs. To appreciate such and other risks, the Belgian Competition Authority is therefore already planning to set up a knowledge centre to supervise algorithms, AI and big data that may jeopardise the market.

The use of algorithm to automate pricing could also lead to the conclusion of unlawful agreements between competitors that limit competition as such algorithm may facilitate monitoring the pricing of competitors and coordinate this pricing with them in an automated manner. Competitors could agree to automatically keep the same prices for products they sell on sales platforms by automatic monitoring and repricing. This may constitute a breach of Article 101 TFEU which prohibits all agreements, decisions by associations and concerted practices between undertakings which may affect the trade between Member States and

which have as their object the prevention, restriction or distortion of competition within the internal market. In particular, this provision prohibits, *i.a.*, the direct or indirect fixing of selling prices, as may be the case with algorithmic pricing.

The question rises, though, whether in case of algorithm collusion there is an intention to prevent, restrict or distort competition in the internal market or not. If an algorithm makes autonomous decisions it will be difficult to prove such intent. Future competition law may have to create new legal grounds to, *e.g.*, hold the creator or user of algorithms liable based on the design of the algorithm (*e.g.* its purpose to monitor and align pricing to that of competitors). But even then, certain technologies such as deep learning, where human intervention is unnecessary, may impede efforts to hold the creator or user of the respective algorithm liable, unless a system of strict liability would be applied whereby no finding of fault is required.

The use of algorithms itself may also constitute an abuse of a dominant position. The *Google Search (Shopping)* competition case has already shown that a dominant firm may include criteria in its algorithms which give priority to its own products or services to the detriment of competitors' products or services.

It is not only the possibly unlawful use of AI, Machine Learning and Big Data which may constitute an issue under competition law. It is likely that the company which is the first to have achieved certain milestones in these technologies will be reluctant to share this technology with its competitors given the enormous investments that are required to develop such technologies. This is where the doctrine of "essential facilities" may come into play.

In competition law, the doctrine of "essential facilities" may apply to a dominant player who unreasonably denies access to its infrastructure or technology to a player who does not have such facilities. Such a refusal of access may prove to be abusive under Article 102 TFEU if: (1) the refusal of access is likely to prevent any competition in the market; (2) access is essential or indispensable for the applicant to carry out his activities; and (3) access is refused without any objective justification (*e.g.* in an arbitrary or discriminatory manner). Thus, if a company that develops AI technology proves to be dominant, it will need to refrain from an unjustified access to this superior technology in order to avoid antitrust sanctions, such as the requirement to grant access.

The current competition law may also need to be modernised to cope with the challenges of the digital age. A first insight into possible changes has been provided by the European Commission in its *Competition Policy for the Digital Area* report in 2019 which, amongst others, analyses the role of competition law with respect to data in the digital age (including the use of algorithms).

Board of directors/governance

Without doubt, AI, Machine Learning and Big Data analysis will be introduced in the daily functioning of many companies in the future even more than it is now. Consequently, the management of such AI-driven businesses will have to obtain at least a basic understanding of both the opportunities and risks of the use of such technologies, as well as its duties in relation hereto, so that it can operate with diligence and appropriate technical knowledge.

When for instance implementing AI in the organisation, the board must conduct the necessary impact assessments and appreciate the potential (privacy and other) risks and benefits of this technology. Prior to the effective use hereof, the board should make sure that sufficient tests have been held to verify whether the system accurately interprets the data it receives.

The board itself may also be assisted by these technologies, especially when complex and big data volumes must be processed and reviewed in order to let the board take informed decisions.

Even though AI may gather information, analyse it and make certain decisions based on its analysis, the board of directors will at all times remain responsible for the overall supervision and management of the company, including the use of AI. Hence, it could be argued that a board member may still be held liable by the company in case of mistakes committed by AI functions, due to, *e.g.*, a lack of oversight or, more in general, if a reasonable board member acting in the same circumstances would have verified whether the decision made by AI was justifiable, accurate or based on objective information. After all, even though a decision is proposed or even made by AI, the board should still be in a position to verify this on its own.

By contrast, if the board would decide to delegate certain decision-making powers to AI, whereby AI would be allowed to take decisions based on pre-defined criteria and procedures (a fully-automated system) or, a step further, based on self-learning (an autonomous system), it may become more difficult for the board to exercise its monitoring function, especially since the reasoning for decisions taken by AI will not always be clear.

Privacy and data protection

Without data there is no AI, Machine Learning or Big Data. Hence, the importance of the General Data Protection Regulation (GDPR) and other data protection legislation will only increase in the future as it will try to regulate the use of the large amounts of data to be generated for the functioning of these technologies.

It is clear that these entail many new risks for citizens and entities. Citizens may, for instance, be made subject to actions and decisions taken by or with the assistance of AI systems which may often prove difficult to understand or challenge due to the lack of clear reasoning. After all, AI can analyse large amounts of data and identify links between them to retrace and even de-anonymise data about persons. Humans will not always be capable of understanding the pattern that AI used. This lack of clear reasoning may also by consequence create a loss of privacy by facilitating mass surveillance or even lead to discrimination when it would be capable of, for instance, deciding who should be employed in a company.

Hence, Article 22 GDPR must be kept in mind which gives data subjects the right not to be subject to a decision based solely on automated processing if such processing will lead to a decision which produces legal effects or has a significant impact on the data subject. Data subjects have the right to request the decision be reviewed by a human. Additionally, under Belgian law, the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data prohibits a person from being made subject to legal consequences of a decision that was taken based on automatic processing of personal data which evaluates certain aspects of a person's personality.

Even though the reasoning of AI may be difficult to follow for human beings, it should nevertheless be transparent to meet the principle of transparency under Articles 13 to 15 GDPR. The data subject should know that automated decision-making (including profiling) exists in the processing of its data and, in such case, must receive meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. Evidently, the AI systems themselves should also be designed in a way that secures processing of data and which only allows processing that is necessary for their goals.

This lack of transparency shows itself clearly in the "Black Box" problem that AI has: the inner functioning and reasoning is inaccessible to humans, as they are not capable of understanding the algorithm that was used between the input and output. A solution that is presented by some for this issue is "Explainable AI", whereby visibility is provided into how an AI system makes decisions and predictions and executes its actions. Thus, by explaining

the decision-making process and presenting the strengths and weaknesses of the process a level of transparency could be achieved that may be legally sufficient.

As mentioned in the introduction, one of the most important topics regarding AI is its ethical aspect, which is highly debated. Indeed, as AI (but also Machine Learning and Big Data) make use of personal data, which often may be sensitive (such as health records) the necessary oversight must be put in place to ensure that the system's process and outcomes are not only in compliance with the law, but also with ethical guidelines which without doubt will be further specified in the future. As set out earlier, this task of supervision should also be performed by the board of directors, if a company processes personal data using AI. Hereto, any entity introducing AI and similar technologies will have to conduct a data protection impact assessment (in accordance with Article 35 GDPR), given that the processing of personal data by AI systems is likely to result in a high risk to the rights and freedoms of natural persons.

The GDPR is seen by some as impeding AI itself. One of its main principles is that of "purpose limitation" (under Article 5 (1) (b) GDPR), which means that the processing of personal data will only take place for the purposes whereof the data subject was informed (and to which it consequently may have consented). In an AI context, it will often be difficult to determine the exact goals of the processing as the focus will rather lay on the collection of large amounts of data which can then later be analysed by AI systems. Unless express use could be made of the exception on the principle of "purpose limitation", namely processing for scientific purposes (which is undefined under the GDPR), this provision may prove to be an impediment to AI development. The same goes for Article 5 (1) (c) GDPR, which describes the principle of "data minimisation", whereby only the personal data that is necessary for the processing may be used. Again, at an early stage of engineering an autonomous system it may be impossible to clearly understand which data will be essential for the operation of the system. Hence, some have even called for the GDPR to be revised on these points to foster the development of AI. In any case, a balance between the freedoms and rights of data subjects and the need of AI to process data to function and create business opportunities will always have to be made.

Civil liability

When the use of AI, Machine Learning or Big Data causes losses with third parties, then the civil (extra-contractual) liability regime must be applied to the new technology. AI could, for instance, create a flaw in the object recognition technology of an autonomous car which could let it wrongly identify an object and cause an accident involving injuries and material damage. Such issue can be caused by flaws in the design of the AI technology, but can also be related to problems with the availability and quality of data or other problems stemming from machine learning. The current civil liability regime may prove insufficient.

For instance, going further on the example of an accident involving and caused by an autonomous car, it may prove difficult to hold the "driver" of the autonomous car liable, as he or she was not in control of the car and thus did not commit an error for which he or she could be held liable (*i.e.* a lack of the subjective element of fault which determines that the person that commits a fault does so out of free will).

By contrast, if the "driver" may have had the opportunity to intervene before the accident and take control over the autonomous car, reasonable grounds would exist to hold him or her (at least partially) liable as it may be argued that a reasonable and cautious "driver", when placed in the same circumstances, would have intervened to avoid the accident. But even then it will have to be determined when a reasonable driver placed in the same circumstances would

have intervened, taking into account the knowledge of the algorithms and technology in an autonomous car that an average person using such car possesses and the fact that algorithms make decisions in a matter of seconds whereby little time is left for humans to analyse the situation and intervene.

Hence, the *classis trias* of the civil liability regime under Belgian law (fault – mistake – causality) may prove insufficient to hold someone liable for the losses caused by an autonomous car or, more in general, AI-driven technology.

Alternatively, the liability *qualitate qua* could be used. Here, a person is not held liable for a fault that he or she commits, but based on the capacity of that person (*e.g.* parents that are liable for the faults committed by their children or owners that are liable for the damages caused by their dogs or cats). A person could be held liable in this sense for the damages caused by a defect in the object that he or she keeps. Such defect could be understood as an accident caused by an autonomous car while such car is supposed to provide security to traffic users by its intelligent behaviour.

Liability of AI could also be established based on the rules of product liability. If AI that is incorporated in an object (*e.g.* the autonomous car that wrongly identified an object on the road and caused an accident involving injuries and material losses), the manufacturer of the product or its developer may be held liable.

Under the current Product Liability Directive (Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products), it is not yet clear if software constitutes a product and is therefore covered by the Directive. This is a first issue that should be resolved in further guidance by the European Commission or in a possible update of the Directive. Under Belgian law, however, software that is part of a product and is incorporated in such a way that it is essential to keep the product functioning entirely or partially so that it cannot be considered to be a separate element anymore, falls under the rules on product liability. Only when it is stand-alone software (*e.g.* online) these rules will not apply in such case.

According to the Directive, a product is defective when it does not provide the safety which a person is entitled to expect from the product, taking into account all circumstances such as the intended use. Hence, it may be argued that an AI system that takes decisions that are clearly disproportionate with regard to the intended purpose or causes significant harm is not as safe as expected, which makes the product defective.

However, a producer cannot be held liable if the defect which caused the damage did not exist at the time when the product was put into circulation by the producer or if the defect came into being afterwards. Based on a strict interpretation of the law, a manufacturer of a system that learns itself to take certain decisions may argue that he cannot be held liable for the defective results of such self-learning as these came into being after the putting into circulation of the product.

If a European-wide solution would be preferred to resolve the liability issues of AI, such solution should be pursued under the Product Liability Directive, as it will prove very difficult to reach consensus between the Member States of the European Union to pursue solutions in general civil liability law. Not only does this vary between the Member States, but Member States are often wary of allowing European legislation into their civil law.

The future of AI regulation

No specific legislation has been adopted as regards AI, Machine Learning and Big Data in Belgium yet. It seems that the main focus is on researching the ethical questions with respect to the use of such technologies, whose impact on society is yet difficult to fully grasp.

Lawyers and other legal professionals will, however, be confronted in the future with many questions regarding the use of AI. While the current legal framework will, as this chapter shows with respect to certain aspects of Belgian (and, indirectly, European) law, sometimes provide an answer to these legal challenges analogously, many matters will nonetheless arise which cannot be assessed under current law.

Perhaps regulating these new technologies should not be a priority. Rather, investing in the ethical side thereof may prove wise to do first as AI and other technologies will probably for the first time in history match and possibly even surpass the intelligence of the *homo sapiens* which created the world we live in. Only when the necessary answers have been found in the field of ethics, a legal framework governing AI can be introduced. Even then the question remains whether it is necessary to create a general law on AI, or whether government intervention should not be limited to specific issues that arise. Or perhaps even co-regulation and self-regulation will prove more appropriate to resolve these novel issues that we will face?

* * *

Endnotes

1. https://www.hln.be/wetenschap-planeet/medisch/belgische-artificiele-intelligentie-slaagt-erin-om-hartaanvallen-te-voorspellen~aaa0aefe/.
2. https://economie.fgov.be/nl/publicaties/perceptie-van-artificiele.
3. https://www.hrsquare.be/nl/nieuws/belgische-werknemers-koploper-in-gebruik-van-artificiele-intelligentie-op-de-werkvloer.
4. https://www.ai4belgium.be/.
5. https://ondernemingen.bnpparibasfortis.be/nl/artikel?n=waarom-brussel-investeert-in-artificiele-intelligentie; https://www.lecho.be/economie-politique/belgique/wallonie/la-wallonie-fait-enfin-de-l-intelligence-artificielle-une-priorite/10185999.html.
6. https://www.ewi-vlaanderen.be/nieuws/vlaams-actieplan-artificiele-intelligentie-gelanceerd.

Steven De Schrijver
Tel: +32 2 215 9758 / Email: sds@astrealaw.be

Areas of practice

Tech M&A; private equity and venture capital; data protection and cybersecurity; e-commerce; software licensing; technology transfer; IT projects and outsourcing; cloud computing; artificial intelligence; drones and robot law; ILO Client Choice Award 2012 in the General Corporate Category for Belgium; and Who's Who Legal Global Data Lawyer of the Year in 2012, 2014, 2017, 2018 and 2019.

Experience

- 27 years' experience in advising Belgian and foreign companies on mergers and acquisitions, with a strong focus and unique experience in technology-related and life sciences transactions.
- Serves a principally international clientele with an outstanding price proposition and the added value of a personalised service and round-the-clock availability.
- Provides his clients with pragmatic solutions that enable them to achieve their strategic business goals.

Astrea

Posthofbrug 6, 2600 Antwerp, Belgium / Louizalaan 235, 1050 Brussels, Belgium
Tel: +32 3 287 1111 / URL: www.astrealaw.be/en

Brazil

Eduardo Ribeiro Augusto & Pedro Rangel Lourenço da Fonseca
Siqueira Castro Advogados

Trends

What artificial intelligence (AI)/big data/machine learning trends are you seeing in your jurisdiction?

Undoubtedly, one of the major concerns of anyone who is a party in a lawsuit or in legal administrative proceedings is the length of it. The Federal Constitution of Brazil determines, in article 5, item LXXVIII that a reasonable length of proceedings is a fundamental right. Therefore, given the amount of processes and the lack of public officers in Courts, using new technologies of artificial intelligence to ensure faster proceedings would be natural and desirable. So, it can be said that it is already a trend in Brazilian Courts today.

The use of artificial intelligence in Justice gained weight a year ago, when the National Council of Justice (CNJ), the body that gives guidelines to the work of judges, published an ordinance listing the adoption of this model as one of the priorities to unburden Courts.

The main technological device tested now in Brazil is an artificial intelligence system called "robot". Robots can help in decision making in order to reduce the amount of lawsuits. Today, there are several Courts in Brazil, including the Superior Court of Justice, which use robots to perform tasks like indication of sentences, especially in repetitive cases, and jurisprudence. It is important to say that all robots' standard decisions must confirmed or rejected by a public officer.

This is the case of "Leia", a robot that reads millions of pages in seconds to identify cases with jurisprudence in the Supreme Court. In September last year, "Leia" scanned 1.9 million cases in forums in five states: Acre; Alagoas; Amazonas; Ceará; and Mato Grosso do Sul. The analysis identified jurisprudence in 8% of cases.

The State Court of Rio Grande do Norte is testing three different robots, each one with a specific function. The first one, called "Poti", promotes the online blocking of money in debtors' bank accounts. "Jerimun" classifies and label lawsuits and "Clara" reads documents, suggests tasks and recommends standard decisions, which will be obviously confirmed or rejected by an officer.

In the State of Minas Gerais, a robot called "Radar" can read lawsuits, identify repetitive claims in the Court and show the article of law to be used as fundament for a specific case. This robot suggests standardised decisions to be applied to repetitive cases, which will be also reviewed by an officer.

The State Court of Pernambuco is using a robot called "Elis" in tax enforcement proceedings. The results are very good, since the analysis process has become faster. Before "Elis", it took an average of 18 months to complete the analysis of 70,000 lawsuits, whereas now, with Elis, it takes only 15 days to analyse 80,000 lawsuits.

The State of Rondônia also uses a robot called "Sinapse" to assist judges in elaboration of decisions.

Even the Brazilian Superior Court of Justice developed a robot called "Victor", which analyses records and identifies themes to be considered of general repercussion.

With the automatic distribution of cases, sentences dropped from 860 to 119 days since the beginning of the decade, without any increase of expenses. The procedural speed has increased, in order to guarantee to citizens the fundamental right of reasonable length of process.

What is the state of the technology and competitive landscape?

Naturally, firms which invest in artificial intelligence technologies are able to optimise processes and, thus, provide services more quickly. Thus, investing in artificial intelligence increases competitive advantages.

For this reason, firms are increasing their budgets for the adoption of robots that help in the execution of their tasks, as well as in interaction with consumers.

How are companies maximising their use of data for machine learning and other applications?

One of the main concerns of companies nowadays is the use of data, because they receive a large amount of data all the time. So, the use of technology of artificial intelligence to analyse and process data is fundamental. Therefore, companies are investing in putting their big data in cloud computing structures in order to maximise their use of big data for robots.

What are the key legal issues that are arising out of adoption of AI/big data/machine learning?

There are two main legal issues.

First, the protection of data in itself, especially personal data. The adoption of artificial intelligence devices, like robots, to process personal data must ensure the protection of such data. In Brazil, a General Data Protection Law (Law No. 13,709) has already been signed by the President and should come into force in August 2020. The new law establishes legal parameters for the use of personal data. This regulation was mirrored in the General Data Protection Regulation (GDPR) established by the European Commission, and places Brazil on the list of safe countries for the use of data.

The law provides some sanctions if companies are not in compliance, so, from now on, companies will have to increase their budgets in order to create departments with data protection specialists to ensure compliance with the new law and avoid punishment. The specialists will have to show total control over any new artificial intelligence device to avoid system failures and security breaches.

The second legal issue has to do with transparency. One clear advantage of using robots is the automated process of decision making. However, that sort of decision making can be biased. It is known that some artificial intelligence systems have provided discriminatory decisions, such as different responses depending on physical or ethnical conditions. In this case, such decisions can represent serious offences to fundamental rights.

One of the key discussions concerning this issue is the right to access the criteria of automated decisions and the possibility to have it reassessed by a real person. Citizens should have the right to know the decision criteria and to challenge the automated decision by the machine.

Therefore, since artificial intelligence mechanisms are used in a recurring manner in Brazil for public decision-making, as well as for decisions within the Judiciary, it will be important to establish a minimum level of transparency regarding the machine source code. In other words, it must be possible for citizens to understand "how the machine thinks", being aware of the way automated decisions are made though the computer software algorithms.

Based on this context, the General Data Protection Law (LGPD) provides in its article 20 the right to review decisions taken solely on the basis of automated treatment. However,

the President of the Republic decided to interpose the device that contained the forecast for review by a human person.

The presidential decision of denying reassessments of automated decisions by a human person does not seem compatible with the fundamental rights listed in the Federal Constitution and will probably be discussed by higher Courts.

Moreover, another legal challenge regarding the use of artificial intelligence concerns civil liability. Our Federal Constitution ensures as its main principle the dignity of the human person. So, it is very important to have specific regulations on the use of artificial intelligence in order to define responsibility in cases of systemic failures. The lack of regulation about artificial intelligence, especially in the public sector, can lead to legal insecurity.

The Code of Consumer Protection and Defense provides that the service supplier will be responsible, regardless of the existence of guilt, in case of damages. In other words, if it is a consumer relationship, it seems obvious that any damage caused by a failure in any artificial intelligence device will be liable to indemnity.

What is the government view with respect to the adoption of AI?

Alongside the Courts, Federal agencies of the Brazilian administration are using artificial intelligence in different procedures and it seems that the government has the intention to foster the adoption of such devices by Brazilian companies.

The Ministry of Science, Technology, Innovations and Communications is preparing a Brazilian Strategy for artificial intelligence with the objective of solving concrete problems in the country, identifying priority areas in the development and use of artificial intelligence-related technologies in which there is greater potential for obtaining benefits. According to the Ministry, it is envisaged that artificial intelligence can bring gains in promoting competitiveness and increasing Brazilian productivity, in providing public services, in improving people's quality of life and in reducing social inequalities, among others. In this context, the Ministry made a public consultation with the objective of collecting subsidies for the construction of a National Artificial Intelligence Strategy.

Moreover, there are already Public Administration bodies that use AI to make decisions, as well as to monitor government actions. For instance, the control of public expenses of the members of the Parliament.

Another interesting example of using of artificial intelligence in order to monitor public expenses is the system known as "Alice". The device is used by Ministry of Transparency and Comptroller General of the Union (CGU) in order to find evidence of deviations in the performance of public officers, to supervise contracts and suppliers and to identify irregularities in bids and electronic auctions from the Federal administration.

What industries/sectors do you see being leaders in the development and adoption of AI?

The banking, healthcare, insurance and retail sectors are likely to be the leaders in the development and adoption of AI. Law firms are also aware of the importance of such technology and many firms, like Siqueira Castro Advogados, are adopting artificial intelligence tools in its activities.

Ownership/protection

When a company creates an AI algorithm, who is the owner?

According to article 4 of Law No. 9,609/1998 (Brazilian Software Law), the rights relating to the computer program, developed and prepared during the term of the contract, shall belong exclusively to the employer, service contractor or public agency.

If the developing of the software is not related to the work contract, then the developer will be the owner of the software.

What intellectual property issues may arise regarding ownership? What issues exist regarding ownership issues?

The question of ownership of works created by machines is inevitable. Under Law No. 9,610 (Copyright Law), article 11, the individual who created the work is the author. Thus, it can be said, by plan, that the current national legislation does not allow copyright to be attributed to a machine.

Apparently, Brazilian law seems to confer, in this case, ownership to the creator of the work through the software, but the law should be adapted in order to guarantee the protection of works designed by artificial intelligence, which can be done through modification of the current Copyright Law.

How are companies protecting their technology and data?

Companies often outsource the protection and data processing service. However, with the entry into force of the General Data Protection Law in August 2020, companies will have to be especially careful when outsourcing this kind of service, as they will need to rely on high-level professionals. The operator of data, that will be hired by companies, must be absolutely reliable concerning observation of the new Law, avoiding security breaches, sanctions and, consequently, loss of reputation.

The Brazilian Data Protection Law requires that companies adopt several security measures to protect personal data. According to article 6, item VII of the new Law, companies that process personal data must use technical and administrative measures capable of protecting personal data from unauthorised access and from accidental or purposeful situations of destruction, loss, alteration, communication or dissemination.

What are the applicable laws with respect to data ownership, security and information privacy?

The Software Law (Law No. 9,609/1998) regulates rights over software; the Data Protection General Law (LGPD) regulates personal data protection in Brazil and the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*) – Law No. 12,965/2014 – establishes principles, guarantees, rights and duties for the use of the Internet in Brazil.

What antitrust concerns arise from big data?

The question that arises regarding the use of big data by big companies has to do with competitiveness problems in the market. The expectation is that the more a company uses big data, the more unequal the competition, because the tendency is for companies to further refine their technologies to the point of becoming monopolies, enabling anticompetitive practices.

What governance issues do companies need to be aware of, specific to AI and big data?

Artificial intelligence can be useful among company directors to take decisions and predict risks in the business based on the analysis of the processed data. Yet, there will be specific concern about the quality of the data that feeds these programs. Using data through artificial intelligence devices cannot contribute negatively to the performance of the company. Moreover, it is also necessary that the company has an information security structure in order to avoid possible data leaks.

How does AI and big data affect the due diligence process for boards of directors?

Particularly in relation to M&A processes, companies must now focus on verification of other companies' compliance with the data protection rules arising from LGPD, since it will be

from now on a very important competitive advantage. A company that does not observe the dictates of the new law can have its market value reduced.

Does your jurisdiction have specific laws relating to AI, big data or machine learning?

There are no laws yet specifically on artificial intelligence, big data or machine learning, but there is a law that regulates the protection of personal data (the Brazilian Data Protection Law).

Are any laws or law reform authorities considering specific laws relating to AI, big data or machine learning?

There are no specific laws concerning these issues, however there are efforts in this direction.

The Law Project No. 21/2020, presented in February 2020 in the Chamber of Deputies by deputy Eduardo Bismarck (PDT-CE), creates the legal framework for the development of artificial intelligence in Brazil. The idea is to adapt the country to the "ethical principles" of the new technology set out in a document released in 2019 by the Organization for Economic Cooperation and Development (OECD), an entity that includes the richest countries. One is the protection of users' data.

The National Congress is promoting public hearings to discuss the matter. For instance, Requirement No. 9/2019 was presented by deputy Alex Santana (PDT-BA) for "the realization of a Public Hearing to discuss the use of technological trends in Artificial Intelligence, Machine Learning and Deep Learning, and impacts in the social context". There was also the request of Public Hearing No. 3/2019, by deputy Bibo Nunes (PSL-RS), to "discuss the issue of facial recognition technologies for public safety in Brazil", as well as Requirement No. 288/2018, by Deputy Goulart (PSD-SP), for "a Public Hearing to examine the legal implications of adopting artificial intelligence resources in the productive sector".

What are the liability considerations when using AI technology?

What happens if a particular artificial intelligence technology causes harm to a person? That is the main question. What kind of civil liability would be applicable? Artificial intelligence devices are autonomous and work through machine learning algorithms, which imply automated decisions concerning real people.

If we let our imagination flow in the direction of the dystopian future predicted by cinema and science fiction literature, we can think about machines becoming able to make decisions autonomously, develop new skills independently, and act in a way not foreseen even by its developer. It is not feasible, at least for now, to imagine some kind of robot responsibility. And we hope that such a gloomy future does not arrive and that the limits of technology are kept framed by the limits of ethics. If an automated decision of an artificial device causes harm to a person, it does not make sense that a device could be responsible for its actions – it must be the person who implemented the technology and accepted the risks of system failures.

Where does the liability fall when AI fails (e.g., contractual issues, etc.)?

Artificial intelligence devices are products of complex programming of algorithms. So, it has no will, ethical discernment or social sensitivity, which are human features. Thus, their liability would be impossible and senseless. It would be up to the programmer or entrepreneur who sells or manufactures the product to pay for the damages resulting from the acts of intelligent robots.

In this sense, it is possible to understand the civil liability of artificial intelligence from a consumerist perspective, considering that the relation between supplier and consumer involving products endowed with artificial intelligence would be a consumer relation.

The Code of Consumer Defense and Protection establishes the objective civil liability of the supplier/company or programmer. Objective civil liability makes sense, since the relationship between the parties is unequal: the supplier has, as a rule, more economic power and means of defence than the consumer.

In the case of damage caused by automatic decisions by artificial intelligence mechanisms, it must be taken into account, in terms of liability, that the machines can behave in a way not predicted by the developer?

We must apply to the case the theory of the risk of development, defined by Brazilian Superior Court of Justice Minister Herman Benjamin as that risk that cannot be scientifically known when the product was launched on the market, only to be discovered after a certain period and use.

Concerning artificial intelligence devices, there can be instances where, later, some defect appears that generates damage to the consumers. Those risks are only discovered after a certain period of use of the product.

The doctrine discusses the possibility of excluding the supplier's liability in such cases. The issue becomes controversial when trying to reconcile the need for development with the well-being of the consumer.

Some argue that the supplier's liability should be excluded as a means of guaranteeing technological development. At the heart of this point of view is the idea that the damage does not occur because the supplier failed in his duties of safety and diligence, but because it was impossible to know the defect of the product before the state of the art at the time.

However, others argue that excluding the liability, in this case, would let the consumer without any kind of protection or compensation for damages. The question is: every type of technological improvement has risks already calculated or still unknown. Who should bear the damage if there are unforeseen failures? The supplier or the consumer? The debate continues in Brazilian doctrine and Courts.

What impact does AI have on negligence and malpractice (e.g., medical malpractice)?

The use of artificial intelligence devices which take automatic decisions in medical practice is especially delicate. Of course, the use of such tools can be extremely important from a therapeutic point of view.

However, who will be liable for any damages suffered by a patient, when these damages are caused by failures in systems that use artificial intelligence?

It is not possible to exclude the physician's liability in such cases, as a general rule. So, especially in medical procedures, artificial intelligence devices must be tested until the risk is proven to be practically non-existent.

Considering that every therapy has an inherent risk, it will always be up to the doctor to assess, given the patient's condition, if it should be used or not. A line of defence may be possible for the doctor – to prove that a particular procedure, which may be an artificial intelligence mechanism or not, despite the risks, was the only possible therapeutic form.

Eduardo Ribeiro Augusto
Tel: +55 11 3704 9840 / Email: eaugusto@siqueiracastro.com.br
Over 15 years of work in the intellectual property area, with focus on trademark registration, anti-piracy measures and border measures. He is member of the Brazilian Intellectual Property Association (ABPI) and Vice-president of the Association for Defense of Intellectual Property in Portuguese-Speaking Countries (APILOP).

Pedro Rangel Lourenço da Fonseca
Tel: +55 21 2223 8818 / Email: prangel@siqueiracastro.com.br
Pedro Rangel Lourenço da Fonseca graduated from Rio de Janeiro's Federal University (UFRJ) in 2014. He is an attorney at law at Siqueira Castro and his practice is focused on intellectual property and digital law.

Siqueira Castro Advogados

Praça Pio X, 15 – 3º andar. 20040-020 Rio de Janeiro – RJ, Brazil
Tel: +55 21 2223 8818 / URL: www.siqueiracastro.com.br

Bulgaria

Grozdan Dobrev & Lyuben Todev
DOBREV & LYUTSKANOV Law Firm

Trends

When talking about the legal aspects of AI and big data in Bulgaria, a few words must be said concerning the specific structure of the legislation and the market it creates.

On one hand, Bulgarian law, while compliant with the standards of WIPO and the international treaties on protection of IP rights, has a long way to go in terms of regulating the use of software, databases, etc. Currently, the regulation remains focused on literary works – and software is being treated as such, while databases are getting similar treatment to periodical literature issues, anthology works and other compilations of works. This raises particular problems with the licensing, use, updates and maintenance of software systems (AI included), as well as with the use and protection of databases which will be discussed below. As a result, there are not many trends in the national legislation concerning innovation, and this leaves attorneys to find a way to protect their clients' interests on a case-by-case basis.

On the other hand, Bulgaria is a Member State of the EU, which in turn means that some of the EU legislative acts – namely regulations – apply directly on Bulgarian territory. Furthermore, EU directives set guidelines for the national legislation of all Member States, which must be achieved with appropriate national measures. These directives though indicate how the national measures should be interpreted – and if the said measures are inadequate or are delayed after the term set for their implementation, the directives can apply directly.

It should be considered also that Brussels is not the only direction rules are coming from in the EU – the Court of Justice in Luxembourg has the authority to interpret EU legislation, and in certain cases it can formulate concrete rules from rather more abstract principles of EU law. Examples in that regard are the data protection rights that were derived from the principles of protection of consumers – and were consolidated with the General Data Protection Regulation. The Court of Justice of the EU has a major role and upholds the rules of protecting competition and the freedoms of movement, even when Member States try to limit or circumvent them.

Within this legislative framework, the Bulgarian IT industry is flourishing – mainly because of the low set-up expenses for businesses and the specific economic situation, which allows IT specialists to maintain a high standard with relatively lower wages. This creates a highly competitive environment, focused on innovation – but practice shows that, especially when it comes to start-ups, all of the attention is reserved for the product under development. Matters of internal relations between partners, ownership over software, etc. are often overlooked – until they become problematic, or, in other words, too late. More complex questions – concerning ownership, predictability, interoperability, liability – are mostly overlooked in both the national legislation and by businesses.

In terms of trends which will definitely affect the development of this market, in February 2020 the European Commission published a White Paper on AI (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf) and a European Data Strategy (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf). While these documents have mainly political aims, they contain the outlines of what should be expected of the EU legislation in this field of technology: the EU does not accept that AI can be a black box, which will take decisions on the basis of output data without control. So, the White Paper clearly states that AI must be trustworthy – and not be allowed to take opaque or biased decisions. The Data Strategy is based around the understanding – expressed also in the White Paper on AI – that big data will mean more and more for businesses in the future, and that it is expected that larger and larger amounts of data will be gathered from enterprises, whereas to this point most of the data concerned consumers. The Data Strategy emphasises the free access to data – but also states that companies gathering data with regard to other services might create an unbalanced data market. Therefore, an additional focus falls on guaranteeing the protection of competition, educating everyone on the market about their data-related rights and encouraging small- and medium-sized enterprises to create, use and operate on the data market.

These documents might contain a lot of political statements – and even be considered as wishful thinking. But they first confirm that both AI and big data will be regulated further and in more detail in the near future. The regulation will be focused on consumers' rights and the protection of competition – two main pillars of European commercial policy – as well as the free flow of data between Member States, including from and to the public sector. Some measures have already been taken in that regard – such as the Free Flow of Data Regulation (Regulation EU/2018/1807 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807)) and the Open Data Directive (Directive EU/2019/1024 (https://eur-lex.europa.eu/eli/dir/2019/1024/oj)) – and another legislative act has been discussed for quite a while now: the E-Privacy Regulation, which extends the standards introduced by the General Data Protection Regulation also to every type of electronic data, as well as introduces rules on updates of software and requirements for the use of the terminal devices by software manufacturers.

As a result, the market shows the signs of an upcoming disaster – an old national legislation together with businesses left without any form of supervision whatsoever, which are about to be hit by the next wave of EU legislative measures, which are intended to have a wider and deeper impact than GDPR.

Ownership/protection

As mentioned above, in Bulgaria, AI and software in general are considered literary works – which is in line with the understanding of most pieces of national legislation. The copyright over AI will arise for the author – meaning the natural person or persons who have written it – though art. 14 of the Bulgarian Act on Copyright and Related Rights Act explicitly states that the rights arise for the employer, unless the employment contract states otherwise. This is a special rule that applies only for software; however, it does not cover a case that is becoming more common in Bulgaria – software created by freelancers, who do not work under the terms of employment contracts. For such cases, the freelancer shall be the owner of the software he/she has written, unless the contract for creating the software stipulates otherwise.

As a result, for companies it is extremely important to regulate the relations with programmers very carefully, to avoid a situation where the AI is owned together by a number of freelancers,

or even employees, due to the fact that the HR department has overlooked a seemingly harmless clause in the employment contracts.

The duration of the protection is 70 years after the moment of publishing – so any AI will be protected long after it is incompatible with any hardware on the market. Issues start to arise when applying the protection of literary works towards the use of software – Bulgarian law is adapted to the standard relationship between author and publisher, so use can be licensed only for a term of 10 years, as a measure granting the author some independence, in accordance with art. 37, para. 2 of the Copyright and Related Rights Act. However, this rule applies also to end-users of every type of software – which creates problems when the end-user has the intention of using the said software for a longer period of time. Of course, the matter can be resolved at a later point by extending the licence – but practice shows that this creates uncertainty, especially when the end-user expects to have an asset for a longer period of time. For literary works, this matter is resolved easily – the rights of the author end at the moment of the sale of a hard-copy of the book, which is a solution that can be applied with some prejudice to CDs, DVDs, etc., but not to digital copies.

But when dealing with AI, issues arise without an analogue to literary works. The Bulgarian legislation contains some specific provisions concerning software, especially the rights of end-users. However, these provisions deal only with the most basic issues – such as the specific right to activate the program or even decompile it and change it for the purposes of compatibility.

These provisions do not reflect the way software companies currently work. AI as any other software must be updated, upgraded and might have to be maintained periodically – and it must be compatible with the hardware and software it works with. Updates, upgrades and maintenance can of course be done by the company which is holding the copyright. Also, the end-user might have the right to change the AI – unless the licence agreement explicitly forbids it (outside the mentioned changes for purpose of compatibility – which cannot be limited under a contract as per art. 71 of the Copyright and Related Rights Act). However, involving a third party should be considered a violation of the copyright – because the end-user cannot share the algorithms, unless explicitly authorised to issue a licence to the third party. Such matters must be resolved at the beginning of any long-term partnership – and the set-up of an AI should be exactly that in every case, but in practice this is not the case – they are left unregulated until they turn into a problem. And if the company providing the AI has not settled the copyright – because the relations with a freelancer have remained unregulated – the matter might become nigh on impossible to resolve. Such cases might have seemed exotic recently – but are slowly making their way to the Bulgarian courts and will become more common as more and more specialists in the area learn how and to what extent they can defend their rights.

Things get complicated further when the algorithms created by an employee bring huge profits to the employer – which is the goal of any business. In such cases, the employee – who of course has received the respective salary – has the right to claim an additional remuneration, to make it proportional to the employer's profit in accordance with art. 41, para. 2 and 3 of the Copyright and Related Rights Act. This right is still rarely claimed – and would be difficult to utilise when the AI is created by a larger team. But it leaves a potential conflict between employer and employee and further complicates the already difficult HR aspect of the IT business.

And the actual problems AI brings to the software market are not even close to any form of regulation. Concerning ownership, two such problems arise from the very nature of AI.

First of all, an AI can grow more complex while operated by the end-user – so who would be holding the rights over the developed AI? And who would hold the rights over any other algorithms (or any other intellectual property, for that matter) created by or with the help of the AI? European law currently cannot accept the idea that the AI might be the owner of anything, and rights can be held only by persons, as already the EUIPO answered to an application for a patent to the name of an AI. Given the current legal framework, we might guess that the rights should be for the person holding the copyright over the AI – but with the same effect an argument can be made that the end-user has facilitated the AI's work and should benefit from its work.

An AI can get additional protection by the law, if it is patented – which under Bulgarian law would be possible only if the AI is a part of a larger invention meeting the requirements for patent protection – or if it is considered a trade secret due to the way it is kept confidential. These two options would provide additional options of protection – but are incompatible, since a patent is made public, and a trade secret is protected only as long as it remains a secret. The patent would be the better option – granting better rights and not requiring the holder to keep the invention secret – but it is more difficult to obtain, given the requirements for originality and inventive step (being non-obvious). The protection of a trade secret is easier to get, because it depends entirely on the holder to take measures, including adequate non-disclosure clauses in the respective contract, to keep the information confidential. In both cases, protection will not be granted only against copying/modifying the algorithms, but also against using their underlying principles.

It should be noted, however, that this additional protection – via a patent or the rules on trade secrets – has an impact on the relations between the company owning the AI and its employees. If the invention is created under an employment contract – or with resources of a company – then that company shall be the holder of the right to patent the invention. However, in case a patent is issued, the inventor – who is always a natural person – will have a right of an additional remuneration, similar to the right of the author. However, unlike the author, the inventor enjoys more clarity as to the amount of this remuneration – it will be a percentage of all profit from the invention, the value of the latter, but also considering the resources provided by the employer, both material and non-material (equipment, personnel, experience that the inventor has gathered while working for the employer, know-how, etc.). Such rules do not exist for trade secrets – so protecting information in that fashion, while less effective, is also less expensive in certain cases.

The regulation of databases is a little more up to date – whereas the ownership over the database is always for the company which has invested in gathering the data. The database is protected for 15 years – and the timer is reset every time the database is updated significantly. The owner can sell the database – and the current wording of the legislation implies that this would not be equal to transferring the copyright over it (i.e. the database can be re-sold to several clients). A problem arises when the database has been published illegally – because every person who has gained access without committing an illegal act (e.g. by downloading it from a content-sharing service) can use it. So, databases must be kept secret, similarly to know-how, in order to be protected under the law. As above, marking them as confidential might provide some additional protection of the database – but the rules on non-disclosure should always be expressly negotiated with any party getting access to the database.

Antitrust/competition laws

AI can be assigned to take decisions with effect in almost every possible aspect related to the commercial activity of company – acquiring goods, trade at the stock market, pricing,

labelling, etc. Bulgarian and EU completion law though do not focus on the way the decisions are being taken – but rather on their effect. So, the possibility of an AI taking decisions which clash with the rules on fair competition would be a problem for the involved companies, rather than for the AI. Therefore, it is in the company's interest to have sufficient safeguards against the risk of an AI colluding with representatives or AIs of other companies or other anti-competition measures.

The more acute problem – which was already identified in EU policy documents – is that AI- and big data-related service providers gather data about every business they work with. This data can allow them on one hand to gain a market advantage if they work in the same field as their clients. And if the service provider works on another market, the gathered data can still have use in vertically connected markets – or when providing services to companies competing at the same market. The EU has already indicated the measures being considered in that regard – the proposed E-Privacy Regulation draft introduces the standards of personal data protection to commercial relations: for any type of electronic data accessed by a service provider, the latter shall have to provide information on how the data shall be used, who will have access to it, etc. This means that the gathering of data and its use shall not be limited as such – but the persons whom the data concerns shall have more information on how the data is used, and in turn have some control over who receives it. Based on the experience with personal data protection, the result will be that some companies shall have to adapt their data gathering policy and perhaps provide incentives for the free sharing of data. As mentioned, the E-Privacy Regulation has become a point of contention, but it can be expected that such rules will be introduced one way or the other – and this is confirmed by the European Data Strategy introduced in 2020, which identifies exactly the problem the proposed regulation addresses.

Board of directors/governance

Big data is a great opportunity for businesses to improve their decision-making – detailed information on processes both inside and outside the company can give even smaller players a commercial edge. And big data goes hand in hand with AI as the best tool for data processing, especially with the growing volumes of information. The issue is that these volumes of information grow to become impossible to manage by company management and decisions respectively become more and more reliant on AI to analyse and identify the important bits of data. Specific regulation here does not exist yet in Bulgaria – though rules on the decision-making process and information for shareholders in public companies affect the possible use of AI for such purposes.

It should be noted that Bulgarian law considers that decisions are always taken by natural persons – and those decisions should be regulated. So, whatever the process includes, in the end a board member shall be considered liable for the decision. Therefore, it would be in the interest of board members to introduce fail-safes and measures to ensure that the decisions they are liable for are reliable and correspond to company policy.

Regulations/government intervention

There are no specific national regulations, applicable to AI or big data. Several legislative regimes concern separate aspects of the operation of AI – namely GDPR, and by extension the Bulgarian Personal Data Protection Act. These acts contain provisions that deal with the use of any personal information and would apply to big data as well. There is also a requirement that data subjects are to be informed when their data is processed automatically

– and granted the right to object to such processing. It should be noted that automated processing does not mean the storing of data electronically – but the taking of any decision on basis of the data without human supervision, which of course includes the work of an AI. A further concern arises from the rules on allocation of company resources – such as computing power, hardware, etc. – which again can affect the use of both AI and the big data gathered by the company.

With regard to data collection and flow, the EU has issued Directive EU/2019/1024 from 20.06.2019 on open data and the re-use of public sector information, which focuses on the access and re-use of data created in the public sector and research data – and repeals Directive 2003/98/EC, which had a similar scope, but was less effect. The Bulgarian legislation is still harmonised with this older directive – the new one must be transposed with according measures by all Member States by 2021 – and guarantees the possibilities for access to data created in the public sector. However, the new directive means that the national law will be changed for sure in the next two years – and currently it cannot be speculated in which way.

Another legislative measure that is already in effect is Regulation EU/2018/1807 from 14.11.2018 on a framework for the free flow of non-personal data in the European Union, which guarantees at least a part of the measures to ensure that the borders of Member States do not stop the traffic of data. The regulation guarantees that data localisation requirements within the EU can be enforced only as exclusion, and that sufficient rules exist allowing portability of user data, transfers between service providers, access of authorities, etc.

As mentioned above, one of the expected legislative acts is the proposed draft of an E-Privacy Regulation by the European Commission, which will extend the application of some of the rules of GDPR to the data created in the commercial sector. Maybe the rule that will have the most impact – if it remains unchanged – is that any company that gathers data from its clients will have to notify them on how this data is being used. So, for instance, data concerning use and stress/damage to provided equipment will be used only for the purposes for which it is gathered (servicing the said equipment), but not for models of the business growth of the company. The E-Privacy Regulation has met fierce resistance – one reason is because of the problems it will cause with software updates and maintenance, but the White Paper on AI and the Data Strategy confirms that commercial, non-personal data shall be protected one way or another, to guarantee the level playing field EU competition rules try to create. So it can be expected that even if the E-Privacy Regulation gets delayed further, the Court of Justice of the EU might refer to the principles of EU law and formulate the rights related to data in the commercial sector piecemeal – and the last few years have proven that the court will enforce the requirements for protection on ICT giants, even where single Member States do not see a market, much less a threat to competition.

In terms of government intervention, the main issues being addressed are still limited to the protection of data and competition. Contingencies for scenarios where the economy or administration becomes over-dependent on AI and big data, or where too much power is delegated to AI, are still not being considered. And given the state of the Bulgarian administration, which is still focused on paper-based services, such contingencies shall not be needed soon.

Civil liability

The concept of civil liability in relation to AI leaves a lot of open questions – and it is our expectation that exactly these questions will drive the creation of new legislation concerning the civil liability of AI-related damages.

The first problem concerns the AI creator – because no matter how expensive the AI is, it will be used to manage more expensive processes. So, an AI failure might easily cost much more than the AI creator has received as remuneration. This would turn AI services into an increasingly dangerous business, though it is a problem which can be limited to some extent with contractual provisions. Under Bulgarian law, it is possible to limit liability for damages due to common negligence, and compensations are always for actual damages suffered or proven missed gains, but only the ones which could have been predicted at the conclusion of the contract. So, the AI manufacturer has the tools to negotiate the right price for the risks being taken. And, additionally, those are risks that can be insured – though the insurance market in Bulgaria has yet to start thinking about insuring the civil liability arising from the use of any type of software.

The relations between manufacturer and user are quite malleable in the end – even considering the pretty rigid Bulgarian contract law – the manufacturer can stipulate what guarantees are provided, that the AI will provide certain results and be held liable for failing to achieve them. The problem with liability towards third persons, especially in cases of torts is more complicated.

As a first question that needs an answer at a fundamental legal level, we can ask whether AI activity is currently regulated under law. Because the law regulates the behaviour of natural persons – even when an obligation concerns a company or even a state, it is always to be performed by a specific human being. Without resolving this matter, all actions of an AI, regardless of their effect, will remain beyond the scope of the law. Currently, an attempt to attribute AI actions to the author might be made, but given the very nature of AI this will not be possible. Because liability is tied to the concept that actions can be controlled – and only guilty actions lead to an obligation to compensate the damages done. Only an exclusion liability can arise without an action or without guilt – and only on grounds of an explicit provision of the law.

The second question is how a future law on AI liability should be formulated to adequately provide protection for all stakeholders. A concept that is being discussed is that AI can be made a person, similar to a company, and be liable for its own actions. However, this would require the AI to have a property of its own. Alternatively, the user can be liable for the AI's actions – because the user is supervising the operation, determining its scope and means, and reaping the benefits. On the other hand, the AI was created by another company, and this company has reaped benefits of its own.

And once the more general rules are defined, it should also be considered whether the standard options for the limitations of liability and exculpations shall apply. Because the concept of negligence seems difficult when it comes to the actions of an AI – it is either programmed to make a respective check to avoid causing damage, or not.

Currently, there are no applicable standards in Bulgaria for the use of AI and big data, including when considering specific regulated activities – such as practising medicine or law – and, respectively, there are no specific rules on malpractice. Given the concept of personal liability for decisions, it is not to be expected that this specific approach will change in the near future. For now, AI and big data are rather additional instruments, which do not change the requirements for care and performing obligations, both for specialised activities and for everyday company management.

Criminal issues

The concept of a crime in Bulgarian law is closely related to the delict as grounds for the arising of civil liability. As a result, a lot of the problems mentioned in cases of civil liability

are relevant to criminal issues as well. However, the concept that only the behaviour of a human being can be regulated via criminal law is much more deeply rooted. In the national law of European countries, the concept that companies can commit a crime seems almost impossible, including because of the understanding of how crime can be prevented and respectively sanctioned.

The problem is that the lack of regulation does not mean a lack of opportunities for criminal issues to arise. An AI can conduct illegal acts both by design and by accident. And if adequate measures are not taken, then the cases where the illegal acts are a result of design will increase both as a percentage and as a total number. This is the reason that criminal law can endure a vacuum in regulation for a shorter period of time – even if AI civil liability is more justifiable as a legal construct. For now, the most possible solution seems to be to impose obligations on AI developers to make AI adhere to the law.

The questions asked when criminal issues are involved will be similar to the ones asked when talking about civil liability – but with a greater emphasis on establishing the chain of cause and effect. However, time would play a much more significant role as a factor – because civil liability can boil down to the obligation to repair any damage done, but criminal liability is always for committing an act that has been strictly prohibited as a crime by the law. A natural question arises – what if an AI is programmed to act in accordance with the law at the moment it has been developed, but commits a crime either because it has evolved or because the law has changed at a later point? Any attempt to answer this question can currently only be speculation, but for now asking the right questions will be more than enough – because any criminal issue will quickly reflect on the relations between the AI manufacturer and user. Matters related to criminal activity must be discussed between the parties in time, to protect their interests – and give them a chance to prepare for the possible risks.

Discrimination and bias

In terms of protection against discrimination, some of the concerns for anti-competition measures shall apply – Bulgarian law shall currently deem any action by an AI to be taken on behalf of a person and that person shall be held liable if the action has resulted in discrimination. So, companies using AI have the responsibility to check any decisions to make sure they do not involve a judgment on the basis of discrimination.

It should be noted that there are two very important rights of data subjects when it comes to protection against discrimination and biased decisions, granted under art. 21 of GDPR – to be informed when data is being processed automatically, and to object to such processing. GDPR states some cases where such an objection is impossible – but then the data subject has the right to require human intervention, to express a point of view on the matter and contest the decision. The only exclusion where these rights do not apply is when EU or national law authorises the use of automated decisions and requires suitable measures to guarantee the rights of the data subjects.

In accordance with GDPR, the Bulgarian Personal Data Protection Act explicitly requires that automated data processing – including via AI – should always be conducted only after an impact assessment. As a result, starting such an operation shall require a very careful analysis of the safeguards, guaranteeing data security on one hand, and the rights of the data subjects on the other.

Grozdan Dobrev
Tel: +359 889 299 492 / Email: dobrev@legaldl.com

Grozdan Dobrev is co-founder of DOBREV & LYUTSKANOV Law Firm and Managing Partner since 1989. He is a member of the Sofia Bar and the scholarly board of the Bulgarian Supreme Bar Council. Mr. Dobrev is a founding member of the Bulgarian Commission of Jurists, and a member and national representative (until 2018) of the International Association of Lawyers.

Mr. Dobrev graduated from Sofia University St. Kliment Ohridski, Faculty of Law. He specialised in International Economic Relations and International Economic Activities at the University of National and World Economy in 1989.

His work is focused on providing complex services to domestic and international clients. He heads the following departments: Corporate and M&A; Energy; Capital Markets; Taxation; Intellectual Property; and Technology, Media and Telecommunications. He is also registered as a professional representative for industrial property.

Lyuben Todev
Tel: +359 889 299 492 / Email: todev@legaldl.com

Lyuben Todev joined DOBREV & LYUTSKANOV Law Firm in 2013 and is currently a Senior Associate. He is a member of the Sofia Bar Association.

Mr. Todev has graduated from Sofia University St. Kliment Ohridski (LL.M. 2012), with a specialisation in Public Administration. Currently, he is pursuing a Ph.D. in General Theory of Law at Sofia University.

From the beginning of his work at the law firm, Mr. Todev has focused on the matters arising from the ever-increasing role of technology in modern industry and everyday life. Currently, he works within the following departments at the law firm: Intellectual Property; Technology, Media and Telecommunications; Transport and Maritime Law; and Migration.

DOBREV & LYUTSKANOV Law Firm

25 Khan Kroum Str., Sofia, PC 1000, Bulgaria
Tel: +359 2 980 38 76 / URL: www.legaldl.com/en

Canada

Simon Hodgett, Ted Liu & André Perey
Osler, Hoskin & Harcourt, LLP

Introduction

In the past few years, we have seen artificial intelligence (AI) move from the periphery and become more and more mainstream, as real, practical use cases, such as chatbots, image and facial recognition, and robotic process automation, are deployed across industries. Across the globe, AI advocates are predicting that AI will fundamentally reshape the ways in which we live and transform the consumer and business experience.

As global competition to lead the AI race increases, Canada, propelled by a stellar research community 30 years in the making, and an innovative and dynamic ecosystem, is set to become a global leader in AI.

Canadian trends

Research and development

Canada has been at the forefront of AI advancements for decades and has gained notoriety for being a global AI hub. The research of Geoffrey Hinton, Yoshua Bengio and Richard Sutton, the so-called Canadian "founding fathers" of AI, underlie many of today's prolific AI advancements.

The Canadian research community continues to uphold this legacy. By some estimates, Canada boasts the third-largest concentration of AI experts in the world.[1] The students of the founding fathers are at the forefront. Ilya Sutskever, who studied under Geoffrey Hinton, is now a co-founder and research director at OpenAI, an AI-focused non-profit co-founded by Elon Musk. The city of Montreal, where Yoshua Bengio was educated, has the highest concentration of researchers and students of deep learning in the world, with almost 9,000 students in AI and related programmes. Researchers from the University of Alberta, including Richard Sutton, rank #2 in Artificial Intelligence/Machine Learning combined, according to worldwide university rankings.[2]

Canada is already home to a dynamic technology ecosystem with more than 4,000 active startups, making it one of the world's largest innovation hubs.[3] The Toronto-Waterloo region, Canada's technology and innovation capital, is second only to Silicon Valley in the number of technology workers and companies.[4] AI is no exception; Toronto has the highest concentration of AI startups in the world, with it being noted in 2019, that there were more than 650 active AI startups in Canada.[5] In 2017–2018, there was a 28% increase in the number of active AI-related startups. Meanwhile, Canadian job opportunities in AI have grown more than 500% since June 2015.[6]

Key actors and significant developments

The Canadian AI industry is quickly accelerating, supported by research labs, government

funding, and global investors. The Vector Institute, founded in Toronto and committed to attracting, developing and retaining top Canadian AI talent, is where some of the world's top minds in machine learning and deep learning come together to collaborate on research, data and real-world problems.[7] It has received more than CAN$100 million in combined provincial and federal funding, and CAN$80 million from more than 30 private partners, including Air Canada, Shopify, Telus, Google, Uber, and Thomson Reuters.[8] These institutes, among others, have attracted Canadian and worldwide talent such as Geoffrey Hinton, Vector Institute, Raquel Urtasun, Uber ATG, Sven Dickinson, Samsung AI Centre and Sanja Fidler, Nvidia AI Research Facility. Other regions of Canada are also emerging as AI hubs. Montreal is home to the Montreal Institute for Learning Algorithms (Mila), one of the world's largest public deep learning labs with sponsors like IBM, Facebook and Google.[9] The Waterloo Artificial Intelligence Institute has partnered with more than a dozen research labs to create products and services actively used by many AI firms, such as MioVision (traffic data collection), Clearpath Robotics (autonomous mobile robots), and Kik Interactive (chat application).[10] In Edmonton, the Alberta Machine Intelligence Institute (Amii) is considered a global leader in machine intelligence research,[11] and the city of Ottawa has opened a 16km test track for self-driving cars, which will be the first of its kind in North America.[12]

Businesses are already implementing innovative AI solutions developed by Canadian startups. When Corus Entertainment, a Canadian broadcaster, worked with Integrate.ai to win back viewers from giants such as Netflix and Amazon, their partnership was 50% more effective than past efforts in generating viewership for certain shows.[13] Acerta Analytics Solutions of Kitchener, Ontario, developed an AI-enabled quality control solution for the manufacturing industry and is already being used by major international car manufacturers, such as Daimler (Mercedes Benz) and Volkswagen. Finn.ai, which won the Best of Show at the Finovate conference in New York in 2017, supplies the Bank of Montreal with a personal chatbot to directly engage with customers.[14]

Finance and investment

The strength of the Canadian AI ecosystem has spurred a growing level of finance and investment from private and public actors. Funding to Canadian AI companies in 2017 surpassed 2016 totals by a wide margin, as US$252 million was invested across 31 deals.[15] This number increased by 51% in 2018, when Canadian AI companies raised US$418 million.[16] In 2019, funding to Canadian AI companies increased yet again, by 49% to US$658 million across 57 deals. The record high of 57 deals in 2019 was driven by larger deal sizes.[17] Acquisitions have been driven by strategic buyers in recent years. Microsoft acquired Maluuba, a Montreal and Waterloo-based startup specialising in natural language understanding.[18] As of early 2016, Maluuba's natural language understanding technologies were being used in more than 50 million devices around the world.[19] Layer 6 is another successful AI company based in Canada. It developed AI that can transform financial banking data into more personalised services for consumers. TD Bank acquired Layer 6 in 2018, after which it integrated Layer 6's capabilities into the bank's operations in the hopes of providing more directed services for customers. As mentioned above, 2019 was a particularly successful year for Canadian AI companies in relation to venture funding. Deep Genomics, a Toronto-based AI therapeutics startup, raised $40 million in its Series B funding. Toronto-based Xanadu raised a CAN$32 million Series A funding for its quantum cloud computing platform. Canada also observed an increase in 2019 in larger deals involving Canadian AI companies, such as Element AI's CAN$200 million Series B funding. Following its launch in 2016, Element AI has since become one of the world's biggest AI startups and this round of funding brought the total amount raised to an estimated CAN$340 million. The largest

venture funding round in Canadian history took place in June 2019 involving Verafin, a financial crime management company based in Newfoundland and its CAN$515 million equity and debt recapitalisation.

The Government of Canada is also committed to ensuring the country succeeds in this space. Announced as part of its federal budget released in March of 2017,[20] Canada was the first country in the world to adopt a national AI strategy.[21] The "Pan-Canadian Artificial Intelligence Strategy", a CAN$125 million commitment over five years, is led by CIFAR (Canadian Institute for Advanced Research) and is intended to build on Canada's long pioneering history in the field by attracting, developing and retaining top talent in Canada, advancing research and fostering collaboration across the country, and providing thought leadership on the impacts of AI. CIFAR is working with researchers and partners in Canada, France (CNRS) and the UK (UKRI) to explore economic, legal, ethical and social perspectives on AI as part of its AI & Society programme, and CIFAR and its partners have also been running the AI Futures Policy Labs, which is a series of workshops to promote discussions across Canada about the future of AI, its impact on society, and potential public policy repercussions.[22] In 2018, the Government of Canada also announced it would be investing more than CAN$950 million in five "superclusters" of innovative industries – what it calls "made-in-Canada Silicon Valleys" – including two focused on AI and digital technology.[23]

AI-related issues

The Canadian legal and regulatory framework is starting to catch-up to the realities of this new world. Canada's legal and regulatory regimes, which were not created to address unique AI issues, are in the process of being reviewed and revisited. Key examples include the following:

Intellectual property

The ownership of intellectual property in the AI models that incorporate machine learning algorithms (which are themselves often open source) is complex, and not always clear, as the legislation in Canada supporting intellectual property was not written and has not been adapted to deal with AI. For example, in the case where the AI model creates a work product, there is no "author", as this concept is understood in copyright law, and no "inventor", as this concept is understood in patent law. Moreover, it may turn out that the data comprising such work product does not meet the legal threshold necessary for intellectual property protection, as Canada does not have a statutory regime that protects ownership of raw data elements. That being said, there is an increased focus and discussions regarding whether copyright should be granted to works created by or with the help of AI,[24] and whether AI can be the inventor of a patentable invention; unfortunately, these questions remain outstanding in Canada.

Data rights

Businesses in Canada that procure AI-based tools or services typically view their data as a valuable asset and expect AI suppliers to agree that use rights in data and insights derived from or based on the customer's data will be exclusively for the customer's benefit. However, this derived data (which includes both the final output data, as well as the intermediary meta-data that is generated during the course of processing the customer data) also has significant value for a supplier's future customers that are similarly situated. As such, suppliers also have an interest in obtaining the right to use this data. Without clear legislation or judicial guidance from the courts, it is imperative that suppliers and customers clearly allocate data use rights as between supplier and customer in their commercial contracts.

Privacy

Meaningful consent and reasonable purpose restrictions are at the heart of Canada's privacy legislation. Although limited exceptions exist, processing information about an identifiable individual requires meaningful, informed consent (typically separate and apart from a privacy policy). Even with consent, the collection, use of, or disclosure of personal information must satisfy a "reasonable purpose" test.[25] As AI increases in complexity, obtaining meaningful consent and satisfying the reasonable purpose test is becoming increasingly difficult and the importance of recognising alternative authority for processing personal information grows. As such, suppliers are increasingly seeking to limit the application of privacy laws by "anonymising" the data that their AI solutions require, but achieving "anonymisation" of such data, itself or in combination with other data, is not a trivial task; and it is often the case that when suppliers are pushed to describe their anonymisation protocols, true anonymity is not achieved.

Torts

Under Canadian tort law (or extracontractual liability in the province of Québec), a party may be liable to another party for injury due to the first party's negligence with respect to the goods or services they provided. Suppliers of goods and services owe a duty of care to the users or consumers of such goods or services as is reasonable, taking into consideration all of the circumstances. There is little in the way of case law on the application of tort law to AI (including those of creators/inventors of AI); however, the following are examples of areas where tortious liability has historically been applied, and which should be closely watched as having potential application to AI:

- Manufacturing and design defects – Generally, the manufacturer or supplier of defective products can be exposed to tort liability if a defective product or the flaw in the design of the product gives rise to harm or injury that should have been foreseen by the manufacturer or supplier, and if the standard of care has not been met in consideration of all of the circumstances.[26] In the context of AI, the question is whether a higher standard of care will be applied to manufacturing or design defects since (in theory) the use of AI in manufacturing and design should reduce the likelihood of defects or flaws. Note that in Québec, a manufacturer, distributor or supplier is not bound to repair the injury if it proves that, according to the state of knowledge at the time that the product was manufactured, the existence of the defect could not have been known.[27]
- Failure to warn – Tort liability can also arise for a supplier of products or services that fails to warn users or consumers of the potential danger in using or consuming the product or service. In the context of AI, this could require suppliers of AI-related technologies to consider the potential for the technology to cause suffering or harm and to provide sufficient notice or warning to users and consumers accordingly. It remains to be seen whether some of the less understood risks associated with using AI will become the norm and accepted, and therefore alleviate the need for such warnings.

Case law in this area may be slow to develop as Canadians are generally less litigious, particularly in relation to our US neighbour. The challenge facing Canada will be in determining to what extent the creators/inventors or suppliers of an AI-related technology should be held liable under tort law, when the technology has evolved to be able to modify and even create products and services without any human intervention. It will be interesting to note in what respect decisions concerning "autonomous acts of things",[28] which includes, for example, x-ray machines, automatic car washes, and anti-theft systems, will be used in the AI context. Decisions around the duty and standard of care owed in such circumstances will need to address

many policy considerations around responsible use of AI, including weighing the public benefit of advances in AI against necessary frameworks for oversight and accountability, and such decisions will likely be shaped or informed by the numerous AI framework and policy reviews occurring in Canada.

Consumer protection legislation

In addition to tort law, Canadian provinces and territories also have legislation that is applicable to consumer protection, sale of goods, and product warranties that apply to goods and services. The extent to and the manner in which such legislation applies to AI-based products and services remains to be seen, but raises a number of interesting issues. For example, will the designer, the user, or both be liable if an AI-based product is not compliant with such legislation, and how will implied warranties of fitness for purpose and of merchantable quality apply to AI-based products and services? Navigating this regulatory landscape, which is comprised of a patchwork of provincial legislation that, while having similar themes, may have different requirements, may pose real challenges where AI-based goods or services are caught within its framework.

Criminal law

In Canada, criminal offences generally require both an act or failure to act (or *actus reus*) and a mental intent (or *mens rea*), with the standard of proof being beyond a reasonable doubt. Exceptions to the foregoing include strict and absolute liability offences. A material contributor to the uncertainty with respect to the application of criminal law to AI-related products or services is the *mens rea* requirement; and, as such, the following questions should be carefully considered:

- Although it may be possible for AI products or services to commit an act (or fail to act) in a manner that is contrary to Canada's *Criminal Code*, can AI products or services have the requisite *mens rea*?
- Who (or what) should be punished for a criminal offence for which an AI product or service was responsible, and what should that punishment be?

The lack of a legal regime to directly regulate AI currently poses challenges as the various stakeholders determine how to comply with or apply a regulatory framework that was established without considering AI-related issues.

As part of Canada's ongoing development of its legal and regulatory frameworks for AI, the Government of Canada has ongoing AI-related initiatives which include the following:

National data strategy: Canada's Digital Charter

Following a national consultation on digital and data transformation,[29] the Minister of Innovation, Science and Economic Development announced the creation of Canada's Digital Charter.[30] The Charter adopts 10 principles that will guide policy thinking and action for building trust while harnessing the power of digital and data transformation. Many of these principles, including Data and Digital for Good, Control and Consent, and Transparency, Portability and Interoperability are directly relevant to AI.

Copyright review

As part of its review of the Copyright Act,[31] a committee of parliamentarians (the House of Commons' Standing Committee on Industry, Science and Technology) issued a report that made a series of recommendations related to AI.[32] Most noteworthy were recommendations that the Government of Canada amend the Copyright Act to facilitate the use of a work or other subject matter for the purpose of informational analysis and make the list of purposes allowable under the fair dealing exception an illustrative list rather than an exhaustive one.

The Government has not identified a timeline for introducing copyright reform legislation in Parliament, but there is a growing understanding that Canada runs the risk of falling behind other countries, including the US, Japan and the EU, which have copyright regimes that allow for information analysis of works without a separate licence, including for commercialisation purposes.

Privacy

Following a multi-year consultation with stakeholders, including the publication of a detailed report,[33] it is widely expected that the Government of Canada will introduce privacy reform legislation before Parliament. The legislation is expected to clarify the terms under which personal information can be used without consent, including in respect of the responsible use of personal information in connection with machine learning and other AI techniques.[34] The Privacy Commissioner of Canada is undertaking a consultation on proposals for ensuring appropriate regulation of artificial intelligence.[35] A core question underlying the consultation is whether AI should be governed by the same privacy rules as other forms of processing, or whether certain rules should be limited to AI due to its specific risks to privacy and, consequently, to other human rights.

Within industry, the Canadian Anonymization Network (CANON), whose members include large-scale data custodians from across the private, public and health sectors, is working to develop an overarching framework of principles for demonstrating effective anonymisation that is technologically and sectorally neutral and acceptable to Canadian privacy regulators.

In addition, recognising the need for an international approach to and standards for AI, the Privacy Commissioner of Canada and its provincial counterpart in Québec, along with their global counterparts in over a dozen other countries, adopted the Declaration on Ethics and Data Protection in Artificial Intelligence in October 2018.[36] The declaration sets out guiding principles, including those related to fairness, transparency and privacy by design. In furtherance of this adoption, the Office of the Privacy Commissioner of Canada has stated its intention to monitor AI developments in Canada and globally in anticipation of developing guidance.[37]

Algorithmic transparency

The Government of Canada has issued its Directive on Automated Decision-Making.[38] The Directive introduces rules that govern the use within the Government of Canada of any automated decision system developed or procured after April 1, 2020 within the Government of Canada. The Directive includes a risk-based framework that includes providing advance notice of automated decision-making and meaningful explanations after decisions are made.

Open data

The Government of Canada is a vocal proponent of open data – that is, making available structured, government-controlled and funded data that is machine-readable and freely shared, used and built on without restrictions. Canada now ranks at the top of the Open Data Barometer survey.[39] Implementation of *Canada's 2018-2020 National Action Plan on Open Government*[40] is ongoing. In addition to these initiatives, Canada has been actively engaged in the consideration of whether to follow other jurisdictions such as the EU and Australia to mandate a framework for open banking. In September, 2018, Advisory Committee on Open Banking was established in September 2018[41] and issued a consultation paper on the merits of open banking in January, 2019.[42] On January 31, 2020, the Advisory Committee published its report on the outcome of the consultations, entitled "Consumer-directed finance: the future of financial services".[43] The report recommends that the phrase "consumer-directed finance" be used in place of the term "open banking", and concludes that Canada should

move forward with a framework for consumer-directed finance. The Advisory Committee is now exploring the issues that need to be addressed, such as liability, accreditation, and governance, and how to build an ecosystem that is accessible to all participants in greater detail, with a view to publishing a white paper on consumer-directed finance.

Governance and ethics

While the ethical issues raised by the application of artificial intelligence and machine learning are of global interest, Canada is at the forefront in considering the implications. Issues such as bias, safety, transparency, explainability, humanity, accountability and predictability, and their implications for everything from wealth inequality to discrimination to technology addiction, are all being considered by various stakeholders across the country and by Canadian representatives in international forums.

The CIO Strategy Council, with accreditation from the Standards Council of Canada, published a national standard for automated decision systems. The standard, which sets out a framework for the ethical use of AI and automated decision systems, helps set guardrails to drive the development and commercialisation of responsible AI technologies.

The Treasury Board of Canada Secretariat's Directive on Automated Decision-Making is built upon a framework of strong governance and transparency.

- December 2018: the Fonds de Recherche du Québec launched the International Observatory on the Societal Impacts of Artificial Intelligence and Digital Technologies. Its mandate is to collaborate with the Government and public and private sectors, both nationally and internationally, in informing public policy on the development and use of AI and digital technologies.
- December 2018: Montreal hosted the G7 Multistakeholder Conference on Artificial Intelligence[44] to build on the G7 Innovation Ministers' Statement on Artificial Intelligence, wherein a "common vision of human-centric AI" was propounded.[45] As a starting point for discussions at this meeting, Canada and Japan collaborated on an insightful paper about accountability and trust in AI.[46]

Most notably on the non-governmental front, the Université de Montréal, in collaboration with the Fonds de Recherche du Québec, published the *Montreal Declaration for Responsible Development of Artificial Intelligence* on December 4, 2018,[47] which sets out recommendations for informing the digital transition to ethical AI, based on 10 principles that promote fundamental human rights and interests. In addition, on January 31, 2019, the CIO Strategy Council, whose membership champions the transformation of the Canadian information and technology ecosystem, published a draft standard entitled *Automated decision systems using machine learning: Ethics by design and ethical use*, for public comment.[48]

These activities represent only the first steps in what will ultimately be, for Canada, a concerted, multi-year effort to achieve an appropriately balanced regulatory and governance framework that will effectively promote the growth of AI within Canada, while at the same time addressing the novel legal and ethical risks and issues that AI presents. In the meantime, in the absence of AI-specific regulatory or legislative oversight, it is especially important that the allocation of the risks and responsibilities associated with the issues presented by AI are addressed by the parties contractually.

Implications for business

Parties negotiating agreements for the development, deployment or use of AI are faced with a number of challenges, some of which are typical during the nascent phase of any new technology, and others that are unique to the technology. Canada operates within legal

frameworks, both in its common law and civil law provinces and territories, that generally allow considerable freedom of contract, especially for business-to-business commercial arrangements. A number of typical clauses in technology agreements require reconsideration in the context of AI-related projects, including:

Ownership of AI

In Canada, negotiations around the ownership of the underlying AI solution are often multi-faceted, and a meaningful discussion of ownership often needs to involve a case-by-case consideration of the various elements of the solution, which are typically comprised of: (i) the AI model, which is a mathematical representation used to achieve the desired outcome (such as to make a prediction); (ii) the learning algorithms, many of which are open source and widely available; (iii) the ancillary algorithms, such as those used to select an AI model or to support the training of AI models; (iv) the data inputs; (v) the data outputs; and (vi) improvements or modifications to any of the foregoing. For example, the performance of a supplier's AI model will generally improve from processing large and varied data sets from multiple customers, so the supplier may not be interested in restricting or diluting its rights in enhancements and improvements to its AI model, as the supplier's AI model becomes increasingly valuable with each new customer. However, in other cases, the value to the supplier may not lie in the AI model that is unique to a particular customer, but in the ancillary algorithms used to select or train the AI model, which can be broadly leveraged for future customers. In these circumstances, the supplier may be comfortable with the customer owning the AI model so long as it retains ownership of the ancillary algorithms. Ultimately, the typical allocation of ownership in standard technology agreements must be carefully assessed in the context of the specific AI in question, in order to effectively address the commercial intent of the parties. Traditional IP ownership frameworks, which address concepts of pre-existing (or background) IP and newly developed IP, will often not be appropriate in the context of an AI-based solution, and will not accommodate the nuanced treatment that may be needed to address the complexity of the AI world.

Data use rights

In Canada, the default position in a standard technology agreement in favour of the customer would allocate data use rights in the customer's data and any output that is based on that data to the customer, as well as limit the supplier's access to the data to the term of the agreement and for a limited purpose (note that this is often referred to by parties to commercial agreements as "ownership" of the data; however, within the Canadian legal framework, data is not owned, and it is therefore preferable that the parties clearly negotiate their respective use rights in the data). This typical default position with respect to data use rights may not meet the needs of a developer or supplier of AI, whose business model might rely significantly (or entirely) on continued access to and use of the data and any data derivations. Ongoing access to and use of the data could, for instance, permit greater flexibility to the supplier to later modify or optimise the performance of an AI solution, and derivations of the original data can sometimes be reused to develop or enhance AI solutions for similarly situated customers in the future.

As is the case with the AI solution itself, the negotiation of data use rights as between the parties requires a first principles discussion in the context of the particular AI solution, with a detailed understanding of the various data elements and their sources, which may be numerous and complex. Parties must ensure that their rights to the data, whether collected directly by one of the parties, obtained from third parties, or generated by the AI solution, are broad enough to permit the activities contemplated. Many data licences have scopes of use that were drafted

and negotiated well before AI or even advanced data analytics attained widespread use. As a result, the licensee of data that is subject to such a licence may easily find itself in breach of the licence terms, by making the data accessible to an AI supplier or by using the data internally in new and, from the perspective of the licence terms, unanticipated ways.

Allocation of risk

Parsing through the allocation of risk in an AI-related contract can be challenging, and is highly fact-specific. Some algorithms that underpin the ability of a self-learning system to continue to develop and refine its capabilities without human intervention can be, or can quickly become, opaque – even to its creators. For example, this is often the case with deep neural network implementations of AI, where studying the structure of the underlying algorithm will not yield insights into how the implementation operates in practice. It is thus essential to ensure the proper risk allocation so that the right party is responsible for monitoring and promptly acting on issues as they arise.

To add additional complexity, it is often the case that many AI implementations (particularly in the machine learning category) are only as good as the data used to train them, with the result that inherent gaps or biases in data sets may be amplified. Whether damage has been caused by a defect in the underlying algorithm, or by the quality of the data (or some combination of the two), may be difficult or impossible to determine. The fact that the data sets may originate from multiple sources can make this exercise even more difficult.

In addition, a failure to adequately understand the data and how the AI is consuming the data could expose the parties to liability if the end solution fails to meet basic legal and regulatory compliance requirements, such as where the AI operates in a discriminatory manner.

As a result, parties are approaching traditional risk allocation contract terms like warranty, indemnity and limitations of liability cautiously and often with dramatically different expectations. For example, suppliers of AI-related technologies may be willing to warrant their own performance in creating and providing the technology, but they may distinguish this obligation from any responsibility for the customer's reliance on results, which are probability-based and may therefore vary depending on the point in time at which they are relied upon by the customer.

Given that the current legal regime, as it applies to AI, remains untested in Canada, it is of particular importance that the parties set out their expectations with respect to use of data and ownership in AI, so that contract law will protect their intent with respect to each other (if not to third parties). Parties should also be aware that the rationale for allocating risk in these contracts can vary widely depending on the potential risk inherent to the AI being deployed. For instance, the risk allocation rationale for AI used to perform internal analytics will be dramatically different from that of AI used in customer-facing services, or which may injure or otherwise cause users to suffer loss or damage. The industry has yet to settle on anything like a standard or market position on such matters, and the resulting agreements remain highly contextual.

Concluding thoughts

Canada continues to advance the discourse and development of a made-in-Canada approach to AI that becomes the global standard. However, at this stage, the legal and regulatory framework and the uncertainty that it creates threatens to impede Canada's progress. If Canada is able to translate its early lead in developing AI and AI talent into being one of the first countries to develop a thoughtful and well-informed legal and regulatory framework in anticipation of managing the risks and promoting the benefits of AI, this country will be

in a position to reap the rewards for generations to come. Until the legal and regulatory framework catches up to the technology, it is critical that legal advisors have an awareness of the unique legal issues and challenges that AI presents, and that they work to address these issues with their clients from first principles within the context and with a full understanding of the applicable AI technology.

Acknowledgments

The authors would like to acknowledge Wendy Gross, Mike Fekete, and Sam Ip for their contribution to the writing of this chapter.

* * *

Endnotes

1. "Canada's AI Imperative: From Predictions to Prosperity" *Deloitte* 13.
2. "Canada – A Leader In Artificial Intelligence (AI)" *Invest In Canada*. [online] https://www.international.gc.ca/investors-investisseurs/assets/pdfs/download/Niche_Sector-AI.pdf.
3. Zanni, Tim; "The Changing Landscape of Disruptive Technologies". [online] https:// assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/tech-hubs-forging-new-paths.pdf.
4. Pender, Terry; "Communitech's tech savvy is admired around the world" *The Record.com*. [online] (3 June 2017) https://www.therecord.com/news-story/7350485- communitech-s-tech-savvy-is-admired-around-the-world/.
5. "AI Can 2019" *Annual Report of the CIFAR Pan-Canadian AI Strategy* [online]https://www.cifar.ca/docs/default-source/ai-reports/ai_annualreport2019_web.pdf?sfvrsn=244ded44_17.
6. "Canada's AI Imperative: From Predictions to Prosperity" *Deloitte* 13.
7. "About" *Vector Institute for Artificial Intelligence*. [online] (19 February 2019) https://vectorinstitute.ai/about/#team-leadership.
8. "Federal and Ontario governments invest up to $100 million in new artificial intelligence 'Vector Institute'" *Financial Post*. [online] (30 March 2017) https://business.financialpost.com/technology/federal-and-ontario-governments-invest-up-to-100-million-in-new-artificial-intelligence-vector-institute.
9. "Canada – A Leader In Artificial Intelligence (AI)" *Invest In Canada*. [online] https://www.international.gc.ca/investors-investisseurs/assets/pdfs/download/Niche_ Sector-AI.pdf.
10. "The Canadian AI Ecosystem: A 2018 Profile" *Green Technology Asia Pte Ltd*. [online] 7. http://www.greentechasia.com/wp-content/uploads/2018/02/Canada-AI-Ecosystem-2018-Profile-Summary-Report-Greentech-Asia.pdf.
11. "Explore our Impact" *Alberta Machine Intelligence Institute*. [online] https://www. amii.ca/.
12. Pilieci, Vito; "The future is now: It's opening day for Ottawa's self-driving car test-track". *Ottawa Citizen.* [online] (18 May 2019) https://ottawacitizen.com/news/local-news/its-opening-day-for-ottawas-self-driving-car-test-track.
13. "Canada's AI Imperative: From Predictions to Prosperity" *Deloitte* 14.
14. "From Prediction To Reality Ontario's AI opportunity" *The Institute for Competitiveness & Prosperity*. [online] https://www.competeprosper.ca/uploads/2018_From_prediction_to_reality_Ontarios AI_opportunity.pdf.
15. "PwC MoneyTree™ Canada Q3 2018" *PwC*. [online] 37. https://www.pwc.com/ca/ en/industries/technology/money-tree/money-tree-q3-2018.html.

16. "PwC MoneyTree™ Canada Q4 2018" *PwC*. [online] 2. https://www.pwc.com/ca/ en/industries/technology/money-tree/money-tree-q4-2018.html.
17. "PwC MoneyTree™ Canada H2 & FY 2019" PwC. [online] https://www.pwc.com/ca/en/technology/publications/697449-pwc-cb-insights-money-tree-canada-h2-19.pdf.
18. "Canada – A Leader In Artificial Intelligence (AI)" *Invest In Canada*. [online] https:// www.international.gc.ca/investors-investisseurs/assets/pdfs/download/Niche_Sector-AI.pdf.
19. Vrbanac, Bob; "Waterloo-based Maluuba partners with other AI pioneers to develop machine learning" *Toronto.com*. [online] (28 December 2016) https://www. toronto.com/news-story/7039659-waterloo-based-maluuba-partners-with-other-ai- pioneers-to-develop-machine-learning/.
20. "Growing Canada's Advantage in Artificial Intelligence" *Your Tax Dollar: 2013-2014 Fiscal Year*. [online] (30 March 2017) https://www.fin.gc.ca/n17/17-026-eng.asp.
21. "Canada first to adopt strategy for artificial intelligence" *United Nations Educational, Scientific and Cultural Organization*. [online] http://www.unesco.org/new/en/ natural-sciences/science-technology/single-view-scpolicy/news/canada_first_to_ adopt_strategy_for_artificial_intelligence/.
22. "AI Futures Policy Labs" *CIFAR*. [online] https://www.cifar.ca/ai/ai-futures-policy-labs.
23. "Canada's new superclusters" *SME research and statistics*. [online] (18 February 2019) http://www.ic.gc.ca/eic/site/093.nsf/eng/00008.html.
24. https://www.ourcommons.ca/Content/Committee/421/INDU/Reports/RP10537003/indurp16/indurp16-e.pdf.
25. *Personal Information and Electronic Documents Act* (S.C. 2000, c. 5), s. 5(3).
26. *Civil Code of Québec*, see arts 1468, 1469 and 1473, CCQ-1991.
27. *Civil Code of Québec*, CCQ-1991, art. 1473.
28. *Civil Code of Québec*, CCQ-1991, art. 1465.
29. "National Digital and Data Consultations" *SME research and statistics*. [online] (26 September 2018) https://www.ic.gc.ca/eic/site/084.nsf/eng/home.
30. Canada's Digital Charter in Action: A Plan by Canadians, for Canadians; https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf.
31. "Statutory Review of the Copyright Act" *The Parliament Buildings and Grounds – The Physical and Administrative Setting – House of Commons Procedure and Practice* (3rd Ed.). [online] (2017) https://www.ourcommons.ca/Committees/en/INDU/Study Activity?studyActivityId=9897131.
32. https://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/report-16.
33. Strengthening Privacy for the Digital Age, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.
34. "Submissions to consultations" Office of the Privacy Commissioner of Canada. [online] https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_181123/.
35. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/.
36. "Declaration on Ethics and Data Protection in Artificial Intelligence" 40th International Conference of Data Protection and Privacy Commissioners. [online] (23 October 2018) https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.
37. "International Declaration Highlights Privacy Issues Related to Artificial Intelligence" Office of the Privacy Commissioner of Canada. [online] (21 November 2018) https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181121_01/.

38. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.
39 https://opendatabarometer.org/country-detail/?_year=2017&indicator=ODB&detail=CAN.
40. "Canada's 2018-2020 National Action Plan on Open Government" Government of Canada. [online] (31 December 2018) https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government.
41. "Minister Morneau Launches Advisory Committee on Open Banking" Department of Finance Canada. [online] (26 September 2018) https://www.fin.gc.ca/n18/18-085- eng.asp.
42. "A Review into the Merits of Open Banking" Department of Finance Canada. [online] (January 2019) https://www.fin.gc.ca/activty/consult/2019/ob-bo/pdf/obbo-report-rapport-eng.pdf.
43. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html.
44. "G7 Multistakeholder Conference on Artificial Intelligence" Government of Canada. [online] (6 December 2018) http://www.ic.gc.ca/eic/site/133.nsf/eng/home.
45. "Annex B: G7 Innovation Ministers' Statement on Artificial Intelligence" G7 Information Centre. [online] (28 March 2018) http://www.g8.utoronto.ca/ employment/ 2018-labour-annex-b-en.html.
46. Millar, J. Dr.; Barron, B.; Hori, K. Dr.; Finlay, R.; Kotsuki, K.; Kerr, I. Dr. "Theme 3: Accountability in AI Promoting Greater Societal Trust" G7 Multistakeholder Conference on Artificial Intelligence. [online] (6 December 2018) https://www.ic.gc.ca/ eic/site/133.nsf/vwapj/3_Discussion_Paper_-_Accountability_in_AI_EN.pdf/$FILE/ 3_Discussion_Paper_-_Accountability_in_AI_EN.pdf.
47. Montréal Declaration Responsible AI, https://www.montrealdeclaration- responsibleai.com/ (accessed 22 April 2019).
48. "CIOSC 101, Automated Decision Systems Using Machine Learning: Ethics by Design and Ethical Use" CIO Strategy Council. [online] https://ciostrategycouncil.com/standards/draft-standards/.

Simon Hodgett
Tel: +1 416 862 6819 / Email: shodgett@osler.com

Simon's practice concentrates on technology outsourcing. He advises enterprises whose businesses rely on technology and complex services. He also advises technology suppliers ranging from large established software providers to early stage technology companies. Simon has been lead counsel on projects in the banking, pension, investment, healthcare, energy and other sectors. His practice includes FinTech, data agreements, outsourcing arrangements, software licensing, government contracting, e-commerce and payment systems. Simon is a member of the FinTech Working Group for the Ontario Ministry of Finance.

Ted Liu
Tel: +1 416 862 6459 / Email: tliu@osler.com

Ted has a broad technology-related practice and possesses both technology-commercial and technology-M&A expertise. Ted advises clients across a broad range of industries (e.g. investment companies, financial institutions, insurance companies, energy companies, medical device manufacturing companies, security software development companies, and securities dealers), bringing a depth of perspective that others cannot provide.

Ted advises large financial institutions, insurance companies, and energy companies, as well as mid-size technology companies, on complex outsourcing and strategic corporate and commercial matters. Ted's practice also focuses on advising emerging companies on corporate and commercial matters, including acting for such clients on M&A and financing transactions. Ted also routinely advises clients on privacy, intellectual property, and data access- and management-related issues, as well as contract structures for innovative arrangements.

André Perey
Tel: +1 416 862 6775 / Email: aperey@osler.com

André is a corporate partner in Osler's Toronto Office. His practice focuses on M&A, startups and venture capital financing. André advises a broad range of foreign and Canadian clients operating in various industries, including software, digital media, online commerce, financial services, retail, food & beverage and renewable energy. André represents emerging and growth stage businesses, and strategic and financial investors in and acquirers of such businesses. André regularly advises foreign companies investing in or establishing Canadian ventures and helps structure and implement a variety of complex commercial contracts involving the development and acquisition of intellectual property and technology.

Osler, Hoskin & Harcourt, LLP

100 King Street West, 1 First Canadian Place, Suite 6200, P.O. Box 50, Toronto ON M5X 1B8, Canada
Tel: +1 416 362 2111 / Fax: +1 416 862 6666 / URL: www.osler.com

China

Susan Ning & Han Wu
King & Wood Mallesons

Introduction

Artificial intelligence ("**AI**") is trending and rapidly reshaping our society. AI is no longer a mere concept but rather an appreciable technology that supports our daily life in a variety of aspects, such as facial recognition in e-payments and smart home application systems based on virtual assistants. AI industries in China benefit from various market advantages, such as gigantic amounts of data available for machine learning, diverse and huge demand of market application, and strong policy support. The Chinese government also actively embraces AI technologies and recognises it as a key focus of future economic development. As estimated by the China Academy of Information and Communications Technology ("**CAICT**"), the market size of AI in China could reach RMB71 billion by the end of 2020.

Trends

The Chinese Academy of Science recognises eight key AI technologies that have achieved major breakthrough and identified specific areas of application, including computer vision, natural language processing, trans-media analysis and reasoning, intelligent adaptive learning (which provides each student with a personalised education that suits their own character), collective intelligence, automated unmanned systems, intelligent chips, and brain-computer interfaces.[1] Among the industries adopting AI in China, security protection, finance and marketing account for the majority, representing 53.8%, 15.8%, and 11.6% of the total market size of industries adopting AI in 2018, followed by agriculture, client service, retailing, manufacturing, education, and others.[2]

The Chinese government recognises AI as an important component of national strategy and plans to establish an AI regulatory system in the near future. The State Council has included AI in the Report on the Work of the Government from 2017 to 2019 consecutively and also promulgated a number of national strategic policies such as the *New-generation AI Development Plan* and the *Three-year Plan for New-generation AI Industry Development (2018-2020)* to set forth specific goals in technology achievement and the regulatory regime of AI in three eras from 2018 to 2030. China has also set up "national new-generation AI open innovation platforms" in five areas; namely, the Baidu Apollo Open Platform in automated driving, Alibaba Cloud City Brain in intelligent city management, Tencent Miying in medical imaging, iFlytek in intelligent audio, and SenseTime in intelligent vision (particularly in security protection).[3] In addition to the five national AI platforms, other world-leading AI practices in China include but are not limited to DJI's computer vision and intelligent engine in drones, Songshu AI's adaptive learning in education, ByteDance's trans-media analysis in media, and JD's NeuHub AI Open Platform in e-commerce, logistics, finance and retail.[4]

With the astonishing development of AI technologies, the demand of data for machine learning in terms of volume and quality is also rapidly elevating. Due to the sheer amount of data involved, the lawfulness and legitimacy of data sources has become the key legal issue arising out of adoption of AI and machine learning. For example, under the *Cybersecurity Law of the PRC* ("**CSL**"), network operators (such as service providers adopting AI) may only collect and process personal information within the scope of the personal information subject's consent, save for a few exceptions contemplated by laws and regulations. It is notable that the immense demand for data to feed AI's machine learning becomes a motivation for some enterprises to illegally collect and use data on internet platforms, such as through the automated collection of personal information via a web crawler from websites without the information subjects' consent. The public security bureau of China investigated and suspended the operation of a number of social credit information services that illegally collected citizens' credit information without consent and used it to build up marketable profiles of individuals or to feed the machine learning of AI models. On the other hand, it is also a common issue for AI operators that they might unintentionally breach data protection laws and regulations when purchasing data to feed their AI systems as it is hard for them to ensure that the data transfer involved and their subsequent data processing fall within the initial scope of the data subjects' consent.

Ownership/protection

When talking about AI ownership, we mainly focus on the ownership issues for AI algorithm and data.

AI algorithm ownership

At present, companies in China mainly apply for software copyright and/or patent to claim the ownership of an AI algorithm and protect it from unlawful infringement.

According to the *Regulations on the Protection of Computer Software* ("**Regulations**") that directly govern and regulate the copyright protections for computer software in China, "computer software" as used in the *Regulations* refers to computer programs and related files, and "computer program" refers to coded command sequences which computers or other similar devices with information processing ability could execute in order to achieve a required result, or symbolic command sequences or symbolic statement sequences that can be automatically transformed into coded command sequences. Therefore, an AI algorithm, which in essence is a mathematic method that is developed and achieved through the use of computer programming language, is copyrightable and can be registered. Meanwhile, it is worth noting that software copyright will only be afforded to the expression of the source program: target programs within one computer program, together with source programs, are seen as the same work. In addition, with the same logic of new registration for updated computer software, it is reasonably foreseeable that if an AI algorithm is trained and evolved through machine learning, the original software copyright certificate holder shall consider initiating a new registration for the updated version, if it is materially changed in functionality and performance.

Although software copyright registration may serve as a notary to evidence the protection of certain expressions of source code, it cannot protect the programming ideas, which are the core of the software. Therefore, companies may go a step further and apply for a patent for their software inventions to protect the design. According to the *Patent Law*, an applicant for a patent for an invention shall undergo substantive examination, and inventions and utility models which are granted patent rights shall possess the characteristics of novelty,

creativity and practicality. Part II, Chapter 9 of the *Guidelines for Patent Examination* articulates specific examination standards for invention applications relating to computer programs. On December 31, 2019, the State Intellectual Property Office ("**SIPO**") released the *Announcement of the Revisions to the Guidelines for Patent Examination (No. 343)* to clarify the rules for examining patent applications in new business forms and fields such as artificial intelligence, and thereby decided to add Section 6 to Chapter 9 on "Provisions on Examination of Invention Applications Relating to Algorithmic Features or Features of Business Rules or Methods" to present the particular examination characters for such invention applications. The newly added Section 6 came into effect on February 1, 2020 and serves as succinct reference for both patent examiners and applicants. Specifically, the new Section 6 provides a three-step test to examine the patentability of a claim thereunder and the test mainly focuses on requirements under *Patent Law*, including: 1) inclusion of technical features; 2) the technical solution as a whole; and 3) characteristics of novelty and creativity, illustrated by several examples. With the clear examination guidelines, it is expected that SIPO will embrace an increasing number of patent applications for AI algorithm in the near future and more companies will consider patent protection as one available option to protect their AI algorithm.

Data ownership

Currently, China does not have specific laws that clearly define the ownership of data, while society has reached consensus for the recognition of the data asset – which by definition is an economic resource, competition resource or property right in the form of data – and companies are swarming into the field, eager to make the ultimate use of their data resources. Given that different types of data (personal information, important data, etc.) are subject to specific restrictions on collection, processing, storage and sharing, it is difficult to align on the data ownership in practice. For example, as ownership is the fundamental prerequisite of a trade, there is still a call to draw a clear line between the personal information subjects ("**PI subjects**") and the company for the ownership of personal information, to establish and promote a benign societal data governance.

Traditionally, lawmakers structure the legal framework for personal information protection based on the leading legislative stance of an absolute protection of the PI subject's privacy rights and personality rights. As such, with reference to China's *Cybersecurity Law* and its supporting measures, processing of personal information can only be granted upon the PI subject's authorised consent. However, with the expansion of an information society and wide recognition of data value, the absolute consent prerequisite for personal information processing may somehow restrict the development of the digital economy where, to some extent, the free flow of data exchanges may be needed. Therefore, academic experts and lawmakers have commonly accepted the view that personality rights not only have personal interests but also proprietary interests, the latter of which individuals are entitled to transfer under certain circumstances. Therefore, theoretically the PI subjects are entitled to realise their proprietary interests in personal information as long as no infringement of public interests would incur and upon the PI subject's authorised or explicit consent. In view of the PI subjects' right to realise proprietary interests and almost exclusive right to control their personal information (i.e. to determine the way of provision, usage, and processing), academics regard PI subjects as the owner of their personal information.

Meanwhile, besides personal information itself, companies are concerned over the ownership of anonymised personal information that technically has no connection to and cannot trace back to identify the PI subjects upon erasure of such information's identifiability. Article

42 of the *Cybersecurity Law* prescribes, "network operators may not disclose, tamper with or destroy personal information that it has collected, or disclose such information to others without prior consent of the person whose personal information has been collected, unless such information has been processed to prevent specific person from being identified and such information from being restored". Also, with reference to Article 3 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information,* whoever provides any citizen's legally collected personal information to any other person, without the consent of the person whose information is collected, shall fall within the scope of "providing citizens' personal information" as prescribed in Article 253A of the Criminal Law, except when the information has been processed in a manner wherein it is impossible to distinguish a specific person and it cannot be retraced. Therefore, under the current legal structure to protect personal information from illegal provision to third parties and in consideration of the technical effect of anonymisation, as long as anonymised personal information cannot identify the PI subjects, companies may be entitled to some level of ownership to that anonymised personal information to promote data exchanges. However, academic discussion raises that ownership is an almost exclusive right while, from a personal information protection perspective, even though the personal information is anonymised, companies shall still be bound by PI subjects' initial authorised consent to the usage of their personal information.

What's more, with the rapid development of big data and technological progress, especially the upgrades of algorithms and large volumes of dataset storage, the risk exists that anonymised personal information may be retraced to the PI subjects. In this regard, some academics hold the view that companies should only be granted restricted ownership of the anonymised personal information upon balancing the interests of the PI subjects' privacy rights.

As of today, China is in the legislative process of establishing the personal information protection law and it is expected that lawmakers will respond to the outstanding question of data ownership, especially personal information ownership, in the near future.

Antitrust/competition laws

Over the last decade, AI has greatly empowered and reformed the commercial world, especially in online retailing. For example, Walmart dominated the retail industry in the US in early 2003, but was soon surpassed by Amazon in a few years, due to the latter's possession of a massive scale of personal and market data for its AI machine learning and business pattern experiments, and the adoption of AI algorithm harvesting its data to constantly predict and adjust the pricing for its products. Today, Amazon's success has influenced all e-commerce platforms to adopt a pricing algorithm, yet it also gives rise to competition laws risks.

Under the *Anti-Monopoly Law of the PRC* ("**AML**"), competitors are prohibited from reaching monopoly agreements of price-fixing, production or sales restrictions, market division, boycott, or other restraining behaviours. Under the *Interim Provisions on Prohibiting Monopoly Agreements,* a *de facto* concerted action by competitors, absent an explicit agreement or consent, is also prohibited if there are consistent market behaviours by the competitors and a common intention among them. A common view is that pricing algorithms are controlled by the competitor and should not become an exemption of anti-monopoly liability. As such, the anti-monopoly culpability varies by the methods of adopting

pricing algorithms. If competitors explicitly agreed to adopt the same or similar pricing algorithm and result in similar pricing patterns, such action may be considered as a prohibited price-fixing agreement under the AML. If competitors lack explicit consent, but unilaterally and constantly adopt algorithms that predict and align with the pricing of the competitors, there might be a *de facto* connection of will which also constitutes a prohibited concerted action. However, it is worth noting that in China there are currently no laws or regulations directly addressing the collusion by algorithm, nor are there any actual enforcement actions or litigations regarding this issue. Some views even argue that algorithm collusion may not be as harmful as traditional collusions, because the barrier of market entry in e-commerce is very low, which renders it impractical for competitors to maintain a monopolistic pricing by algorithm collusion.

Algorithms also give rise to the AML liability of abusing a dominant market position by discriminative pricing. In 2019, there was a widespread discussion of possible price discrimination by famous internet companies in industries such as ride hailing, travel agencies, shopping, and food delivery.[5] Algorithmic price discrimination refers to pricing the same product differently depending on the individual features of each buyer, especially empowered by AI harvesting consumer big data. Article 19 of the *Interim Provisions on Prohibiting Abuse of Dominant Market Positions* explicitly prohibits business operators with a dominant market position from offering discriminative treatment to counterparties in price, volume, quality, discount and other conditions without justified reasons. However, this prohibition of price discrimination only applies to operators with dominant market positions under the AML. Endeavouring to prevent discriminative pricing by all e-commerce vendors, Article 18 of the *E-Commerce Law of the PRC* articulated that when e-commerce operators provide search results of goods or services to consumers, they shall also provide options not targeting consumers' personal features. The Ministry of Culture and Tourism published the *Interim Provisions on the Management of Online Travel Business Services (Draft for Comments)* in October 2019, which prohibited price discrimination against travellers by big data and other technical measures.

Application of big data also gives rise to concerns of abusing dominant market positions in data by mega internet platforms. In theory, internet platform behemoths may take advantage of the scale of the platform to attract and collect more user and market data, which is subsequently used to further improve the platform's competitive strength; as such, the platform's dominant position is further strengthened via network effect. While the current Chinese laws and regulations do not specifically address that the concentration of data may constitute dominant market positions, some court decisions have recognised the competitive value of data to companies. In *Sina v. Maimai* in 2016, the Court held that Maimai conducted unfair competition behaviour prohibited by the *Anti-Unfair Competition Law of the PRC* by collecting user information in Sina's social media platform Weibo without Sina's consent. The Court reasoned that, in the internet economy, data such as user information had become important corporate assets and the scale of data was a major element of their competitive strength, and thus data shall be afforded legal protection.[6] Article 18 of the AML also articulates that the identification of a market dominant position shall also consider factors of competitive strengths other than market share, such as technological competitiveness. Therefore, it cannot be ruled out that the control of large amounts of valuable data in a particular market may contribute to a leading enterprise being identified as having a dominant market position, and such enterprises shall be particularly cautious in undertaking actions AML recognised as abusing said dominant position, such as refusal to deal, price discrimination, unreasonable trade restrictions, tying, and others.

Board of directors/governance

With the rapid development of AI and big data, companies are welcoming high tech's efficiency and facing challenges brought to internal management at the same time. One key issue in relation to introducing AI to companies' governance is the integrity of automated decision-making. Factors that may influence the integrity of automated decision-making include, but are not limited to, the legality of data collection, quality of data set, accountability of the algorithm, potential bias in AI application, etc.

From a national regulatory perspective, at the current stage, national standards makers are trying to restrict the use of information systems' automated decision-making from a personal information protection perspective, which we understand may impact the automated decision regulations within companies' governance as well. According to Article 7.10 of the *Personal Information Security Specification* ("**PI Specification**"), when decisions are made based on automated decisions by information systems and may significantly influence the PI subject's rights and interests (such as personal credit, loan limits, or interview screening based on user profiling), the PI subject shall be provided with methods to appeal. Within the text of the new *PI Specification*, detailed requirements are afforded to restrict the use of information system automated decision-making mechanisms, including the requirements of conducting personal information security influence assessments during the mechanism design stage or at the first time using, making the assessment a regular mechanism, taking protective measures in accordance with the evaluation results and providing PI subjects with manual review options.

Regarding the scenario of companies' governance, the automated decision-making may more directly and frequently affect shareholders' vested interests and the operation of the business as a whole. Doubts may be raised in determining the board of directors or shareholders' meeting's relevant obligations, in case shareholders' rights may be infringed upon; that is, it needs to be established whether automated decisions are attributed as decisions by the board of directors or shareholders' meeting. In general, as the automated decision-making scheme is introduced to the company mainly by decisions of the board, there is consensus that such decision shall be considered as a decision of the board or the shareholders' meeting. Therefore, if there is any adverse impact on shareholders or the whole business operation, the company's authoritative agency – the board or the shareholders' meeting – shall be responsible. To mitigate relevant risks, from a technical perspective, ensuring the traceability of automated decision-making results would be a top priority that companies should take care of to remediate potential harms immediately. From a managerial perspective, with reference to measures mentioned in *PI Specification* (both the effective version and the new version), companies are advised to assess potential risks in business before implementing the automated decision-making system, limit the applicable scope of such system if material adverse impact would incur and set up a manual review mechanism to check and ensure the accountability of final decisions. What's more, to neutralise potential bias that may be inserted in or evolved through the algorithm, it is also advisable for companies to set up an AI ethics committee to overview the internal use of AI, lead relevant ethical impact assessments, and coordinate different departments in the face of ethical risks.

Regulations

While few laws or regulations systematically address AI in China, there are rules regulating particular AI-related subject matters, such as the following:

- **Big data**: The National Information Security Standardisation Technical Committee ("**TC260**") has issued a series of recommended national standards that articulate the

security measures (especially security in data processing), management guidelines and technical specifications of big data services and systems, including the *Information Security Technology—Big Data Security Management Guide, Information Security Technology—Big Data Security Management Guide*, and others. The National Health Commission of the PRC ("**NHC**") also issued the *Trial Provisions on Managing the Standards, Security and Service of National Healthcare Big Data* in July 2018 to set forth general system security requirements and big data protection measures such as storing data within the PRC.

- **Personal information protection and automated decision-making**: The recommended national standard of *Information Security Technology—Personal Information Security Specification* issued by the TC260 articulates that when personal information controllers adopt automated decision-making systems that may influence PI subjects' interests (such as automated decision of an individual's credit line, empowered AI and big data analysis), they should conduct security assessments of personal information beforehand and periodically, and should ensure the accessibility for PI subjects to complain against such automated decision-making, followed by manual review of the complaints.
- **Consumer protection**: Please refer to the *E-Commerce Law* and *Interim Provisions on the Management of Online Travel Business Services (Draft for Comments)* regarding prohibition against pricing discrimination in Section Antitrust/Competition Law.
- **Information content management**: The *Provisions on Ecological Governance of Network Information Content* issued by the Cybersecurity Administration of China ("**CAC**"), effective since January 2020, articulates requirements for content provision models, manual intervention and user choice mechanisms when network information content providers push information by adopting personalised algorithms. The *Measures for Data Security Management (Draft for Comments)* issued by the CAC in May 2019 also articulate that when automatically synthesising information content via big data, AI and other technical measures, network operators shall explicitly label such information as "synthetic" and shall not conduct such action for profits or to infringe other people's rights.
- **Automated driving**: The MIIT and other ministries jointly issued the *Trial Administrative Provisions on Road Tests of Intelligent Connected Vehicles*, effective since May 2018, to regulate the qualification, application, and procedure requirements of automated driving road tests and liabilities incurred by road test accidents. In addition, more than 20 cities have issued their own administrative measures for automated driving road test qualifications. On the other hand, the recent draft recommended national standard of *Draft Taxonomy of Driving Automation for Vehicles*, published by the MIIT on March 9, 2020 sets forth six classes of automated driving (from L0 to L5) and contemplates respective technical requirements and the roles of the automated systems at each level.
- **Finance**: The People's Bank of China ("**PBOC**") and other financial regulators jointly issued the *Guidance Opinions on Regulating Asset Management Business by Financial Institutions* in April 2018, which articulates qualification requirements and human intervention obligations for financial institutions providing asset management consulting services based on AI technologies. The recommended industry standard of *Personal Financial Information Protection Technical Specification* issued by the PBOC also sets forth requirements for financial institutions to regularly assess the safety of external automated tools (such as algorithm models and SDKs) adopted in the sharing, transferring or entrusting of personal financial information.

China has also formed a specific plan for establishing a comprehensive legal regime of AI. Under the State Council's *New-generation AI Development Plan,* the State government intends

to initially establish a legal, ethical and policy system of AI regulation by 2025. In October 2019, the China National Information Technology Standardisation Committee announced its plan to establish the AI Technology Sub-committee to engage in the promulgation of national standards regarding AI technology, risk management, products, application and others,[7] which further demonstrates the government's determination in AI regulation. In addition, the Big Data Security Standard Special Taskforce of TC260 released the White Paper of AI Security Standardisation in October 2019 to propose an AI security standard system covering topics of foundational standards, data and algorithm models, technology and systems, management and service, assessments, and products and application. The TC260 is also working on a foundational AI national standard called *Information Security Technologies-AI Application Security Guidelines*.[8]

Civil liability

AI medical software

At the beginning of 2020, the National Medical Products Administration ("**NMPA**") approved several registrations of AI medical software built upon deep learning technology, signalling a wider use of AI medical software in medical diagnostics in the near future. According to the *Medical Device Classification Catalogue*, AI medical software mainly fall under class II or class III of medical devices, where class II AI software provides diagnostic suggestions and supports diagnostic activities while class III AI diagnostic software automatically identify the diseased region and provides diagnostic instructions directly.

For AI medical software's failure, the injured party may refer to China's *Tort Law* and/or *Product Quality Law* for recourses.

China's *Tort Law* adopts a fault theory on medical malpractice cases where negligence liabilities exist. As such, according to Article 57 of the *Tort Law*, in the event that medical personnel failed to perform medical treatment obligations corresponding to the prevailing medical standards in clinic activities and caused a patient to suffer damages, the medical institution shall bear compensation liability. Furthermore, Article 58 identifies three circumstances where presumed negligence exists, including: (1) violation of laws, administrative regulations, rules and any other relevant medical norms; (2) concealment of or refusal to provide medical records relating to the dispute; or (3) forgery, tampering or destruction of medical records. With the introduction of AI medical software to diagnostics, it is arguable whether the medical personnel and medical institution shall be considered as being negligent and liable to patient's damages due to AI medical software's malfunctioning. As discussed before, the key issue is to determine the scope of medical personnel's duty of care in the use of AI medical software.

One thing to be noted is that medical institutions are prohibited from using unregistered medical devices with reference to Article 66 of the *Regulations on Supervision and Administration of Medical Devices*. Therefore, if the malfunctioned AI medical software is not registered with NMPA and is in diagnostic use, the medical institution that uses such unregistered AI medical software violates the administrative regulation, constitutes presumed negligence and shall be liable. However, apart from presumed negligence, a balance of interests test may apply to determine medical institutions' duty of care. Specifically, there are some opinions that medical institutions that use registered AI medical software shall be granted some level of reliance on the authority's confirmation of the reliability of the medical software, as NMPA has assessed the risks before approval of registration. But still, from the perspective of the protection of patients, it remains unclear as to the scope

of medical treatment obligations that medical personnel shall perform in the course of AI medical software usage, especially for class III medical diagnostic software that makes automated final decisions.

Another recourse that the injured party could refer to is *Tort Law*'s product liability Chapter or specifically, the *Product Quality Law*, under which they could claim damages against the manufacturer or seller if a product's defect causes physical injury or damages to third-party property. According to Article 46 of the *Product Quality Law*, a "defect" refers to the unreasonable danger in the products where such danger threatens personal safety or the safety of third-party property. Therefore, burden of proof is on the injured party as plaintiff and in a scenario involving the use of AI medical software, the injured party shall first identify the defect in the AI medical software and then prove the causal chain between the defect and their damages. However, it is to be admitted that identification of defects in AI medical software itself is challenging to a normal individual who lacks expertise in the relevant techniques.

Autonomous driving

On March 9, 2020, the Ministry of Industry and Information Technology ("**MIIT**") released the national standard of *Taxonomy of Driving Automation for Vehicles (submit for approval)* which classifies autonomous driving into six levels reflecting the degree to which the driving automation system can perform dynamic driving tasks: this ranges from emergency support, function-specific automation and combined function automation, to limited self-driving automation, high-level automation and full self-driving automation.

Currently, when there is a car accident, the driver or car owner will be liable to damages according to the *Law on Road Traffic Safety* and the *Tort Law*. If the accident is caused by a defect in the vehicle, the manufacturer or seller of the defective vehicle will be liable. Specifically, according to Article 76 of the *Law on Road Traffic Safety*, where a traffic accident occurs between two motor vehicles, the party in fault shall bear the liability and where a traffic accident occurs between a motor vehicle and a non-motor vehicle or a pedestrian, presumed negligence or strict liability will apply.

For fully autonomous vehicles, the role of a person changes from driver to passenger, and there is no need to monitor driving conditions and the environment or operate in an emergency. Therefore, in the event of an accident or damage caused by a fully autonomous vehicle, even if the human user is in the driver's seat, theoretically speaking, there is no recourse in tort to hold the human driver liable. However, in the operation of semi-autonomous cars where they are not completely out of the control of a person, the current traffic accident liability theory can be applied to some extent. As such, the first and the key issue to determine tort liability under circumstances of self-driving accidents is to identify whether and to what extent human factors were involved in the accident so as to determine which party bears the duty of care and to divide the responsibility between the driver, automobile manufacturer, software provider and other parties.

For instance, under level 0 of autonomous driving, where the automated system only provides emergency support and the driver is in sole and complete control of the primary vehicle controls at all times and is solely responsible for monitoring the roadway and safe operation of all vehicle controls, if there is a car accident, the driver shall bear all liabilities. However, under level 1 or 2 of autonomous driving, where the autonomous system provides driving support, like automatic cruise control, and where drivers share control right with the automated system, drivers are still under the duty of care to monitor the roadway and safe operation. If there is a failure of the system, drivers shall take full control of the vehicle and thus may be held jointly liable for a car accident due to failure of the system. When it comes

to level 4 or 5 of high-level or full self-driving automation, the vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. A human user is expected to be the passenger, not the driver, and is expected to be in full reliance of the automated system. Vehicle manufacturers shall have full responsibility for any damages in self-driving accidents, as a result. What's more, as vehicle manufacturers of autonomous driving vehicles involve parties like hardware equipment providers, algorithm and system software providers, and original equipment manufacturers, the internal liability allocation, especially how tort theory would apply, is also a concern and under discussion by lawmakers and regulators.

* * *

Endnotes

1. Key Laboratory of Big Data Mining and Knowledge Management of China Academy of Science, 2019 White Paper of Artificial Intelligence Development.
2. iResearch, 2019 China Artificial Intelligence Industry Research Report.
3. Key Laboratory of Big Data Mining and Knowledge Management of China Academy of Science, *supra* Note 1.
4. *Id.*
5. Beijing Youth Daily, Beijing Consumer Association Announces the Investigation Result of "Taking Advantage of Existing Customers via Big Data", 28 March 2019, Chinese original version available at http://epaper.ynet.com/html/2019-03/28/content_323364.htm?div=-1.
6. *Beijing Weimeng Chunagke Network Technology Co., Ltd. v. Beijing Taoyou Tianxia Technology Co., Ltd.*, (2016) Jing 73 Civil Final No. 588 (30 December 2016).
7. National Standardisation Technical Committee, Notice on the Proposal of Establishing the AI Technical Sub-Committee of the National Information Security Standardisation Technical Committee, 21 October 2019, Chinese original version available at http://org.sacinfo.org.cn:8088/tcrm/recruit-index/notice/2401.do?menuItem=1.
8. Big Data Security Special Taskforce of the National Information Security Standardisation Technical Committee, Artificial Intelligence Standardisation Whitepaper (2019).

Susan Ning
Tel: +86 10 5878 5010 / Email: susan.ning@cn.kwm.com

Susan Ning is a senior partner and the head of the Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her publications include *Big Data: Success Comes Down to Solid Compliance*, and *No "Data", No "Internet of Vehicles"*, etc.

Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. Susan has assisted companies in sectors such as IT, transportation, finance, etc. in dealing with network security and data compliance issues.

Han Wu
Tel: +86 10 5878 5749 / Email: wuhan@cn.kwm.com

Han Wu is a partner of the Commercial and Regulatory Group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad.

In the areas of cybersecurity and data compliance, Han provides legal services including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets, etc.

Han has provided legal services on cybersecurity and data compliance to companies in multi-industries. The projects he participated in encompass industries of financial payment, consumer electronics, internet advertising and personal care, etc. Han is the only lawyer from Chinese law firms featured in *40-under-40 Data Lawyers* by Global Data Review in 2018.

King & Wood Mallesons

18th Floor, East Tower, World Financial Center 1 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020, P. R. China
Tel: +86 10 5878 5588 / URL: www.kwm.com

Denmark

Timo Minssen, Tue Goldschmieding & Søren Sandfeld Jakobsen
Gorrissen Federspiel

1. Trends

1.1 What is the state of the technology and competitive landscape?

As one of the most digitised countries in Europe, the Danish public and business sector already meets many key requirements for succeeding in the digital economy. Although some challenges remain to be addressed and more investment into artificial intelligence (AI) is needed to face global high-tech competition, the Danish environment provides a very competitive platform for developing and utilising AI. Large Danish businesses, such as Novo Nordisk, Maersk, Lundbeck and Carlsberg, have a strong track-record in developing and using digital technologies, and there is a thriving start-up scene that is successfully implementing and competing with new digital technologies on a global level.[1] Multi-sector examples of successful Danish AI implementations include *inter alia* the use of AI to: (1) diagnose cancer and other diseases more quickly in Danish hospitals; (2) analyse large volumes of water-use data to minimise energy consumption on pumping water in Danish cities; (3) optimise baggage handling at Copenhagen Airport; and (4) analyse chemical and sensory data from yeast types to optimise beer production by predicting taste and quality.[2]

Moreover, the Danish public sector, including healthcare, is one of the world's most digitised with a well-developed digital infrastructure, an advanced digital registration system for citizens, sophisticated digital administrative solutions for communications from public authorities, as well as high-quality public-sector data and a population with good IT skills.[3]

The Danish government is also working very proactively to identify and address remaining challenges through several large-scale studies, investments and initiatives (see the following sections). With a total public research budget of DKK 23 billion (EUR 3.1 billion) in 2019, Denmark has also one of the highest public investments in R&D among all OECD countries in relation to GDP.[4] Public-private partnerships and Danish foundations are also investing heavily in research. The resulting Danish research is internationally highly recognised and has a high impact with strong AI-focused research environments in both the public and private sector.[5]

Last but not least, Denmark has a highly educated and tech-savvy population with a high degree of mutual trust and confidence in public and private administration and governance. In combination with a very flexible labour market, this means that employees have the opportunity and motivation to shift quickly between positions in different sectors. This enables Danish companies and public entities to adapt quickly to technological changes driven by AI and digitalisation.[6]

1.2 What are the key legal issues that are arising out of adoption of AI/big data/machine learning?

Probably the most important areas where challenges and legal issues are frequently debated

upon in Denmark concern (1) the ethics of algorithmic decision making, (2) the cybersecurity of AI systems, (3) the transparency and accountability of complex and opaque algorithmic decision making, (4) the protection of privacy particularly with regard to the General Data Protection Regulation (GDPR), (5) questions concerning intellectual property rights and data ownership, (6) inequality, bias and discrimination resulting from AI applications, (7) quality assurance for both data and AI-driven decision making, (8) the usability and interoperability of data, (9) liability, and (10) trust. These core issues are often discussed in combination with calls to modernise legislation, improve public communication on AI matters, enhance the education and competences of the Danish workforce with regard to computational thinking, adjust legal and regulatory procedures, and reorganise crucial sectors such as healthcare.

1.3 What is the government view with respect to the adoption of AI?

In the recently published "National Strategy for AI",[7] the Danish government indicates that it regards the Healthcare, Agriculture, Transport, as well as the Energy and Utilities sectors as priority areas with respect to the adoption of AI. Moreover, the report specifies *four focus areas* for governmental initiatives within the AI area. *First* of all, the importance of a *responsible and sustainable foundation for AI* is highlighted. This includes the development of ethical principles for the use of AI and the establishment of a National Data Ethics Council (see also in section 5). Moreover, the improvement of AI security, legal clarity on development and use of AI, more transparent use of AI, and ethically responsible and sustainable use of data by the business community are mentioned under this category. It is hoped that this would lead to a particularly Danish imprint on the standards for AI resulting in competitive advantages and make AI and data ethics a Danish "trademark". The *second focus area* identified in the report is more and better data. This includes the establishment of a Danish language resource that will "enable businesses, researchers and public authorities to securely and efficiently develop solutions using voice recognition and language understanding in Danish".[8] In addition, the government believes that better access to public-sector data, better storage solutions, more data in the (European science) cloud for AI, and improved access to data outside Denmark will be crucial for Danish businesses and researchers. To harvest the promises of AI, the government also stresses stronger competences and new knowledge as a *third focus area*, encouraging an intensified dialogue with research funding foundations on AI, stronger digital competences in central government, strong Danish participation in the EU Framework Programme for Research and Innovation, and stronger digital competences through adult, continuing and further education. Finally, the government identifies increased investment in AI as a *fourth focus area*, calling for dedicated AI signature projects, more investment in Danish businesses, exploring possibilities of an investment agreement with the EU, increasing knowledge-sharing across public authorities, and strengthening Denmark as an attractive growth environment.

2. Ownership/protection

2.1 When a company creates an AI algorithm, who is the owner? What intellectual property issues may arise regarding ownership?

AI algorithms fall under the same legal framework as that of traditional software, which means that IP protection may be claimed either under patent law pursuant to the Patents Act[9] or as a copyright under the Copyright Act.[10] Protection pursuant to the Trade Secrets Act[11] and the Marketing Practices Act[12] may also be relevant.

2.1.1 Patent Law

With respect to patent law, computer software cannot in principle be patented.[13] However, algorithms can be patent protected as a part of a computer program, if the software is

considered an "invention" and serves a technical purpose and has a technical effect, i.e. complies with the general patent conditions. Hence, even though the so-called 'software patents' (as seen, e.g., in the US), meaning the grant of a patent to a computer program, are *per se* not possible under Danish law, AI algorithms and software may very often be patented as technical inventions like other types of inventions under the Patent Act.

The issue of ownership of the patent will primarily arise between the employee and the employer. If the AI computer program is considered an 'invention' and, thus, subject to protection as a patent under the Danish Patents Act, the Danish Act on Inventions at Public-sector Research Institutions or the Danish Act on Employees' Inventions applies.[14] Pursuant to the two latter acts, the employer/public institution is entitled to have the rights associated with the invention transferred to the employer/public institution, if the invention is made in the course of the employee's work scope. If the right to an invention has been transferred to the employer/public institution, the employee who made the invention is entitled to fair remuneration from the employee/public institution.

2.1.2 Copyright Law

In respect to copyright law, works of software, including AI software and algorithms, are protected under Sect 1, para 3, of the Copyright Act.[15] Protection is subject to the software or algorithm having originality, i.e. expresses the author or authors' own intellectual creation. Accordingly, only human beings, not machines, can obtain copyright. The originality requirement for software is not high under Danish law. Hence, most coding which is not trivial or a copy of other's work will in general be protected. However, the scope of protection is narrow. Only the specific program/code is protected, and there is no protection of the functionality, techniques or underlying ideas as such.[16]

It is a characteristic of AI and machine learning software that it can be "trained", i.e. the more data, calibration and instructions the software receives the more advanced it gets. This raises the question whether the "trained" version of the AI software can be copyright protected, and if so, who the copyright holder is in that situation. The "trained" version is subject to the ordinary copyright requirements, i.e. it can obtain copyright if it is a "work" which is regarded as original, i.e. expresses an intellectual creation of one or more persons. As mentioned, the AI software or machine cannot in itself hold a copyright. If these requirements are met, who is then the owner: is it the original software developer, the licensee of the AI software, the person who trained the software or the person who owns the data which has been entered into the system? Or two or more of these jointly? At present, the answer to this is highly uncertain under Danish law, as no case law exists yet.

Another copyright question is who the author is to AI-generated copyright-relevant output like news articles, product descriptions, paintings, pictures, etc. Again, the requirement is that the output must qualify as a literary or artistic work, and that it reflects a human creative "fingerprint". Who – if anyone – can be regarded as "author" of the AI-generated work is at present unregulated and highly uncertain under Danish law.

Computer programs, including algorithms, are often created in teams of developers, which may give rise to ownership issues between the team members or between the employer and the employee(s). Only members of the developer team who, individually and creatively, have contributed to the creation of the algorithm may claim copyright, in which event the copyright is regarded as a joint authorship. In practice, teams of developers are normally employees of a company, and pursuant to Sect 59 of the Danish Copyright Act, the copyright to a computer program (including an algorithm), which is created by an employee in the execution of his duties or following the instructions given by the employer, shall pass to the employer unless otherwise agreed.

A computer program and the necessary algorithms will most often be made by an independent software developer, however, based on (detailed) ideas, instructions and specifications – and often with much involvement – of the entity placing the order. The general assumption under Danish law is that the creator of the algorithm/computer program, in this case the third party, will hold the copyright to the algorithm. This means that changes in copyright ownership must be dealt with by contract.

AI technology may prove especially advantageous with respect to collecting, handling and analysing large amounts of data. Pursuant to Sect 71 of the Danish Copyright Act, the producer of a catalogue, a database or the like, in which a great deal of information has been compiled, or which is the result of a substantial investment, may claim copyright in the database, etc., and so hold the exclusive right to make copies of it and make it available to the public (the so-called *sui generis* right). The *sui generis* right implies a right to prevent extraction and/or re-utilisation of the whole of or a substantial part of the database. Consequently, although databases may rarely fulfil the requirements for being a copyright protected "work" (there is not sufficient originality in the mere compilation and presentation of data), they may be protected under the *sui generis* right.

As mentioned, it is a feature of AI software that it can be "trained", because it becomes more skilled and advanced the more data is entered into the system. This raises the issue of whether data generated as part of AI system training qualify for database protection. However, that is not very likely. First, it probably does not express the author's own intellectual creation and thus does not constitute a "work". Second, it probably will not fulfil the definition of a "database" ("a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means"). Third, it will probably not fulfil the requirement subject to case law from the Court of Justice of the EU (CJEU) that the "substantial investment" shall relate to the resources used to collect and present the data in the database, not the resources used for the creation as such of the data.[17]

2.1.3 Trade Secret Act

If companies are able to keep their technology secret from the public, for instance by offering products that contain a technology which cannot be 'reverse engineered', and if companies have taken reasonable measures to preserve such secrecy, companies may also claim protection for the technology as a trade secret pursuant to the Danish Act on Trade Secrets.[18]

The underlying Directive[19] defines a 'trade secret' as information which meets all of the following requirements: a) is secret; b) has commercial value because it is secret; and c) has been subject to reasonable steps to keep it secret. The definition covers know-how, business information and technological information, etc., provided it has a commercial value. The definition of a trade secret excludes trivial information and the experience and skills gained by employees in the normal course of employment, as well as information generally known among or readily accessible to persons within the circles that normally deal with such information.

Data generated as part of operating/training an AI system can in principle qualify as trade secrets, provided the three conditions listed above are fulfilled. This will, however, require that necessary measures are taken beforehand with regard to identifying and preserving the secrecy of the information.

2.1.4 The Marketing Practices Act

Pursuant to Sect 3 of the Danish Marketing Practices Act, businesses must act in accordance with "fair marketing practices". It should be noted that this so-called "general clause" is a special Danish construction which has no EU law background. It is very often used in

B2B relations to protect against "copycats", either as a supplement to the exclusive rights in "ordinary" IP law (patents, copyrights, trademarks, etc.), or as a legal basis in itself for protecting a product's market position against disloyal market conduct, e.g. one company's free-riding on another company's products and goodwill. Hence, Sect 3 constitutes an important legal tool for protecting intellectual property, in particular where no exclusive IP rights can be invoked. In this capacity Sect 3 can turn out to be a vital instrument for protecting AI systems and AI-generated output.

Protection pursuant to Sect 3 requires that 1) the product has a distinctive character, 2) the product has a certain position in the market, and 3) the copier is in bad faith, i.e. has aimed at copying or imitating the product. Obviously, these conditions will also have to be complied with in regard to AI.

2.1.5 Contractual protection

In case none of the above-described IP rights apply, or – more realistically – as a supplement to these, protection of an AI system and algorithms can also be obtained contractually, i.e. by agreement between the parties. However, contractual protection has its limitations. First, it is only binding upon the parties to the contract and hence only governs the parties' internal rights and obligations, not third parties' rights. Second, IP rights cannot be "created" by contract, only by law. Thus, even though the parties to the contract shall abide by the obligations set forth in the contract, this does not create any IP rights that can be enforced upon third parties acting in good faith.

2.2 How are companies protecting their technology and data?

Under Danish law, patents must be registered with the Danish Patent and Trademark Office subject to a patent application which complies with a number of requirements set forth in the Patent Act. Denmark is a party to both the European Patent Convention (EPC) and the Patent Coorporation Treaty (PCT). Hence, it is also possible to apply for patents through the European or international patent system.

A copyright (including database rights) neither can nor shall be registered under Danish law. Hence, a copyright if founded and can be enforced from the time of creation, provided that the work complies with the ordinary copyright conditions, *cf.* above.

Trade secrets cannot be registered either. They are founded and exist if the conditions for trade secrets mentioned above are fulfilled. It should be noted that the Trade Secrets Act introduces a six-month time limit for filing a case to the courts for a preliminary or final injunction in case of alleged infringements of trade secrets. However, the time limit does not begin to run until the owner of the trade secrets has acquired such knowledge of the violation that the company has sufficient grounds to initiate a case. This rule is obviously expected to create uncertainty as to when the time limit will actually begin to run. No case law exists yet.

As described, the rights pursuant to Sect 3 of the Danish Marketing Practices Act are not IP rights as such, because Sect 3 does not establish an exclusive right but only serves to protect a company's market position from "copycats". Hence, no formal protection requirements must be observed.

2.3 What issues exist regarding ownership issues?

As described in the context above, ownership issues primarily arise between employees and employers, between a company and a third-party software developer, independent consultant or software vendor, or in situations involving collaborative projects.

The issues that arise with respect to ownership are primarily related to establishing the degree of the employee's, individual developers' or companies' contribution in creating the

computer program. As computer programs in Denmark are primarily protected under the Danish Copyright Act, it is necessary for a person or company to prove that in fact he or she has individually and creatively contributed to the creation of the program.

Another issue that may arise is when an employer has commercially exploited the invention made by an employee and how to calculate a fair remuneration to the employee with regard to patent law and the Danish Act on Inventions at Public-sector Research Institutions and the Danish Act on Employees' Inventions. We refer to the parts above regarding patent and copyright law.

2.4 What are the applicable laws with respect to data ownership, security and information privacy?

There is no statutory regulation in Denmark concerning data ownership. The use of data is subject to the general regulation in the data protection regime, notably the EU GDPR[20] and the Danish Act on Data Protection.[21] The main applicable laws in Denmark with respect to security and information privacy are the Danish Act on Mass Media's Information Databases,[22] the Danish Act on Television Surveillance,[23] various sector-specific regulation implementing the NIS Directive,[24] and the Danish Health Act.[25]

3. Antitrust/competition laws

3.1 What antitrust concerns arise from AI and big data?[26]

Competition law may affect the market for big data and the behaviour of its holders in different ways, and in Denmark this would typically involve the rules of EU competition law. In the following, we will focus on the rule which prevents the misuse of a dominant position (i.e. Article 102 of the Treaty on the Functioning of the European Union (TFEU)), and which may serve to facilitate data sharing if access is restricted because of misuse of a dominant position, and on the provision that regulates the conditions for the sharing of data via licensing agreements (i.e. Article 101).[27]

Article 102 TFEU bans the misuse of a dominant position by one or more undertakings. The Court of Justice of the European Union (CJEU) has ruled that this provision may be applied for the granting of *compulsory licences* (even) to information which is protected by IPR. Article 102 does not ban "misuse" in the abstract. It is only the misuse of "a dominant position" which is covered by the prohibition. A "dominant position" is characterised by the ability of a firm or group of firms to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers.[28]

In order to determine whether or not a company holds a "dominant position", the "relevant market" must first be established. Normally, the assessment involves the expected effects of a "small but significant and non-transitory increase in price" (the SSNIP test) on demand substitution.[29] Having established a "dominant" position, the next hurdle for a third party wanting access to the data and relying on the granting of a compulsory licence under Article 102 is to prove that a "misuse" has taken place. For information that is protected by IPRs, the CJEU developed what is known as the "indispensability" test[30] as the baseline for compulsory licensing.[31] However, applying this test in a case where a third party requires access to data involves a number of complicated assessments, including how to define the "relevant market" and distinguishing between the (legal) *use* of and the (illegal) *misuse* of market power. In particular, it is far from clear whether and how competition authorities would apply the test to "big data" which is not protected by IPR or which involves (parts) which are considered to be trade secrets.[32]

It is further unclear to what extent the protection of personal data would prevent the issue of compulsory licences *per se*. The intersection between competition law and data protection rules has become an ever more important factor in cases related to big data. Data protection rules, such as the EU's GDPR[33] or international data transfer agreements, such as the Privacy Shield agreement[34] between the United States and Europe, often restrict the ability of public and private commercial research to generate, store, use and transfer data. In particular, the GDPR codifies regulatory requirements that will surely have a considerable impact on the Commission's assessment of (anti-)competitive practices. This includes new types of considerations already anticipated by the Commission in the assessment of the case law already mentioned, such as increasingly relevant evaluations of data portability and the prospective future behaviour of merged entities.[35] Arguably, the CJEU decided in *Asnef-Equifax and Administración del Estado*[36] that privacy considerations *as such* should not be the focus of competition law. Yet, the CJEU also held that data protection rules must be carefully considered for the purposes of establishing the relevant counterfactual, to the same extent as any other regulatory requirement would be considered by the Commission.[37]

Additional problems also apply to the competition law assessment of licensing agreements. Normally the licensing of technology is said to promote competition.[38] However, licensing agreements also often limit competition and therefore they are not always accepted by competition law as such. Article 101 TFEU states that all agreements having an adverse effect on competition between Member States are void. Furthermore, Article 101(3) TFEU exempts competition law constraints from the prohibition in Article 101(1) for agreements which, despite containing anti-competitive elements, have overall pro-competitive effects.

In future cases, Danish courts and competition authorities will most likely rely on the basic principles in the EU Technology Transfer Block Exemption Regulation.[39] This exempts a number of important restrictions regarding access to markets and consumers (within the EU) and it is directly applicable to agreements concerning, *inter alia*, patents and know-how. Defining the relevant market is also central for the application of Article 101. However, defining the relevant product and technology markets is inherently complicated in the big data context and there are many reasons for this. This is *inter alia* demonstrated by the difficulties in assessing which technologies (products) may be *substitutes*.

Considering the *volume* of data, for example, simply having more data than anyone else does not necessarily protect a company from competition.[40] Similar complexities occur when assessing the *nature and relevance* of the type of data that is involved: expected anti-competitive outcomes assume often that all data are competitively useful, and that most data are unique and without reasonable substitutes. This disregards the counterfactual reality that in most cases the data are not essential to competing or there exist reasonable substitutes such that the way in which the owner or controller may choose to leverage that data should not raise a significant competition issue.[41]

3.2 What can be expected for the future of competition law?

The aforementioned complications, along with extensive investigations and discussions that have accompanied cases such as *Microsoft* (2004),[42] *Google Shopping* (2017)[43] and *Google Android* (2018),[44] have raised awareness of the need to adjust the analytical tools, methodologies and theories of harm to better fit the new market realities in case-by-case analysis.[45] For these and other reasons, the Danish EU Commissioner Vestager has asked competition experts to explore how competition policy should evolve to continue to promote pro-consumer innovation in the digital age. The results were published by the EU Commission on April 4th, 2019. In essence, the Report finds that the current framework of EU

competition law provides a sound and sufficiently flexible basis for protecting competition in the digital era.

Yet, it also proposes significant, and potentially controversial, adjustments of the traditional tools of analysis and enforcement to adapt to the challenges posed by the digital economy.[46] In particular, the Report proposes that competition law enforcement in digital markets should adopt a more flexible approach with regard to potentially anti-competitive conduct, even where consumer harm cannot be precisely measured, in the absence of clearly documented benefits for consumers. This could potentially result in lower, or even reversed, standards and burden of proof, requiring incumbents to demonstrate the pro-competitiveness of their conduct.[47]

The Report also argues for a duty on dominant firms to ensure data access, and possibly data interoperability, in respect of data requests to serve complementary markets or after markets. On the other hand, the Report also stresses that an assessment of "indispensability" of the data remains the most crucial test under Article 102 TFEU assessments, and that regulation, rather than competition law, may be the most feasible tool to address data access issues in many cases. Concerning so-called "killer acquisitions" of small start-ups by large/dominant companies, the Report recommends to reconsider substantive theories of harm and to evaluate whether the acquisition forms part of a potential strategy against partial user defection from the ecosystem. [48]

Most recently, on February 19th, 2020, the European Commission published three policy papers: a white paper on AI;[49] a communication on a European strategy for data;[50] and a communication on shaping Europe's digital future.[51] In particular, the Data Strategy and Digital Future Communications contain several proposals relating to competition law, such as: *ex ante* regulation of "Big Tech" platforms; potentially updating competition law as it applies to digital markets; how the collection and use of data can be factored into in merger control analyses; and voluntary and compulsory data sharing.[52]

The scope and goals of the papers seem to be highly ambitious[53] in light of increasing global competition and wide regulatory disparities among various nations. While it is still not certain how many of the proposals and ideas will ultimately be adopted throughout specific sectors, it can be expected that these policy papers will also have an impact on the Danish frameworks for digital competition.

4. Board of directors/governance

4.1 What governance issues do companies need to be aware of, specific to AI and big data?

Any commercial use of big data and/or AI must focus on the use of personal data, which most often play an integral part in commercial AI and big data processing. Companies must ensure that they comply with the GDPR and the Danish Data Protection Act[54] if their programs are processing personal data.

It follows from the abovementioned legislation that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.[55] Due to the broad scope of application of the GDPR and the Danish Data Protection Act, as well as very substantial fines for non-compliance, any party handling personal data should pay meticulous attention to this field of regulatory law and ensure they are compliant. When adopting new types of technology, companies need to be cautious, since a new or different way of processing information may conflict with the data protection law, e.g. use of big data and data mining, where processing and compilation of large amounts of non-sensitive data regarding an individual could in fact generate sensitive information about that individual. Particular attention is necessary in the following areas:

4.1.1 Use of training data

The use of AI is based on large amounts of "training data", which the program uses to "learn from". The principle of *data minimisation* – which states that it is not allowed to process more personal data than necessary[56] – implies that companies must assess the necessity of the data, which the program is "fed" with. An alternative to this could be to anonymise the data used as "training data", since anonymised data is not personal data and thus not covered by the GDPR.

4.1.2 Purpose limitation

The GDPR and the Danish Data Protection Act also introduce the principle of 'purpose limitation', *cf.* Article 5, para 1, litra b GDPR. The principle entails that personal data may only be collected and processed for specified, legitimate and explicit purposes. The principle safeguards that data collected for one purpose is not used for other purposes. This may constitute a problem for programs using big data, because at the time of collecting personal data, it might not be certain what the data will be used for later.

This principle can also constitute a restriction to the use of AI. Programs using AI are created to be able to "think" autonomously. This entails an inherent risk, if the program 'evolves' into processing the collected data for purposes that are not compatible with the purposes for which the data initially was collected. Companies should therefore make sure that programs using AI do not 'evolve' in such a way that the program begins using personal data for purposes, which the data subject has not given its informed consent to.[57] In this respect, it should be noted that a 'general consent' from a data subject stating that data is collected for any possible processing, does not meet the requirement of a specified purpose under the data protection regulation.

4.2 How does AI and big data affect the due diligence process for boards of directors?

The board of directors must serve the interests of several stakeholders, including the company's and its shareholders' best interests. The "best interests" may vary from company to company, taking the specific circumstances of that company into account, and usually changes over time as society and the markets evolve. Due to this dynamic, it is difficult to form general principles as to how a board should serve a company's and its shareholders' best interest.

However, due to AIs increasing importance and relevance in modern society, it may generally be said that board members should obtain at least a basic understanding of what AI and big data are and how they might benefit or impose a risk as to a company's business, production, revenue, etc. In addition to this, board members ought to stay informed and updated concerning developments within areas of technology such as AI and big data to the extent they play a part in the company's business model.

When serving the company's best interests, the board's decisions should be made on an informed basis. AI and big data can be used as a helping-tool in this process, since programs using AI and big data can process and analyse large amounts of data and, in this way, serve as an information or monitoring system for the board, which can help the board make decisions on a more informed ground and thereby benefit the company.

4.3 How does AI and big data affect a board's fiduciary duties?

We do not in Denmark see that AI and big data are affecting a board's fiduciary duties.

4.4 How is AI and big data affecting communication plans to shareholders, vendors, etc.?

Although we already see that companies are holding their annual general meeting electronically, we believe that AI may help to deliver information in new and innovative

ways by offering "virtual" conference rooms, by responding to inquiries from shareholders, vendors, etc.

AI could also affect the way companies respond to crises or issues, and AI could ensure that information is delivered faster and more accurately to relevant stakeholders. For example, in the food product sector it is not uncommon that food businesses need to recall food products from the market due to food safety concerns. With AI, communication to relevant distributors and authorities could be made very quickly.

We predict that AI and big data will heavily affect communications in organisations in the future throughout all the different sectors.

5. Regulation/government intervention

5.1 Does your jurisdiction have specific laws relating to AI, big data or machine learning?

To our knowledge, the government has not yet adopted any new key laws *specifically* and *directly* focusing on recent developments in AI and big data. Consequently, existing EU and national laws on liability, IP and trade secrets, as well as general privacy and data protection law, such as the GDPR, etc., apply to the new technologies. However, since AI offers great opportunities to improve and streamline society, the Danish government has developed the aforementioned new national strategy for AI, which aims to make Denmark one of the leading countries in applying AI by 2025.[58]

The strategy applies across public and private sectors and establishes a common direction for ongoing and future initiatives in the AI area. The main goal of the strategy is to ensure that public authorities and Danish companies have the best framework for exploiting the possibilities of AI, as already mentioned in section 1.4 of this chapter. Based on the latest knowledge from Danish and foreign research, the strategy provides guidelines as to how companies and public authorities can improve their implementation of AI, e.g. by clarifying and giving access to data, initiating trial projects and investing in shared infrastructure. The strategy builds on the actions the government has already initiated, to promote education and research in digital technologies. As indicated above national strategy also includes ethical principles for the use of AI in Denmark to ensure that privacy, security, transparency and justice are not being undermined by AI applications.

5.2 Are any laws or law reform authorities considering specific laws or initiatives relating to AI, big data or machine learning?

It remains to be seen to what extent the national AI strategy will result in new parliamentary laws, but it will certainly provide the basis for new considerations, initiative and ultimately legal developments in the area.[59] One of the first and most important areas where substantial investment and concrete initiatives are being launched is cybersecurity.

In accordance with recent EU legislative developments,[60] the Danish government has adopted a new national Danish cyber and information security strategy,[61] which will provide authorities, businesses and citizens with a better protection against digital threats. The strategy encompasses 25 specific initiatives to consolidate the defence of the Danish society against digital threats. The strategy builds further on the 2018–2023 Defence Agreements.[62] In the next few years, the Danish government will invest DKK 1.5 billion in Danish cyber and information security.[63]

In order for Denmark to minimise the digital threats, the government has also established a national Cyber Situation Centre at the Centre for Cyber Security, which will be staffed day and night. This centre will be responsible for the monitoring of vital IT systems and of Denmark's most important digital networks.[64]

Other areas where initiatives and new regulations are emerging or being considered include changed tax provisions to allow for greater deductions for investment in technology and rules that enable new business models, e.g. for driverless transport and within FinTech.[65] Moreover, it can be expected that the aforementioned three policy papers from the EU Commission, i.e. the white paper on AI,[66] the communication on a European strategy for data,[67] and the communication on shaping Europe's digital future,[68] will have a considerable impact on future Danish laws and initiatives in the area.

5.3 What are governments considering and what should governments do to prevent adverse outcomes (e.g., the "AI robots take over" problem)?

To support the work on the national strategy for AI and to prevent adverse outcomes, the Danish government appointed in March 2018 a Danish Expert Group on Data Ethics.[69] The task of this expert group is to specifically facilitate and improve a sustainable Danish framework and high-quality standards for data ethics. The long-term aim and vision is not only to protect fundamental values, but also to create a "trademark" for Denmark as a leader in data ethics and responsibility.[70] It is *inter alia* hoped that this could provide a competitive advantage for Danish companies and data providers.[71] In November 2018, the Danish Expert Group announced the following nine recommendations.[72]

First, the Expert Group recommends the establishment of an independent *Council for Data Ethics*. The purpose of the council will be to support an ongoing focus on data ethics and ensure that a responsible approach to data ethics becomes a competitive advantage. *Second*, the Expert Group proposes that company directors and staff actively address questions and dilemmas around data ethics by taking a *data ethics oath*. *Third*, the Group suggests the creation of a *dynamic toolbox* for data ethics should support the oath and provide tools and aids to help raise awareness and for specific activities in Danish companies. *Fourth*, it is recommended that Denmark should be the first country in the world to demand a *declaration of companies' data ethics policies*, meaning that Denmark's biggest companies incorporate an outline of their data ethics policies in their management reviews as part of their annual financial statement.

The *fifth* recommendation encourages the introduction of a *data ethics seal* signifying that a product meets data ethics requirements. This would make it easier for consumers to navigate digital products, and for companies to identify responsible partners. The *sixth* recommendation proposes a *national knowledge boost* to increase society's understanding of the opportunities and consequences of using data. This should support the *seventh* proposal recommending that Denmark should be visible in and impact European and global development in data ethics by being a *frontrunner on the international scene*. The *eighth* recommendation urges the government to *stimulate innovation and entrepreneurship* with a focus on new data ethics business models through co-financing, earmarking of funds and innovation contests. The *ninth* and final proposal of the Expert Group recommends that the public sector should drive the demand for innovative and data-ethical solutions from companies by *requiring that digital solutions that are procured or developed by the public sector are data-ethical*.[73]

The Danish government has reacted swiftly to these recommendations and has already appointed the new Danish Ethics Council, which was announced in March 2019.[74] In the wake of COVID-19 and the increasing pressure on data sharing and welfare surveillance, as expected, the Council is facing an extremely busy start.[75] At the same time, it is evident that while ethics can certainly provide blueprints and guidelines for a socially responsible and beneficial use of digital technology, it cannot always implement them.[76] In particular, with

regard to responsible solutions that require major investments and regulatory control, it will be crucial that ethical guidelines are accompanied by enforceable laws.[77] Last, but not least, we would like to stress that Denmark will in our view not be able to solely rely on high data quality and the best ethical standards in the harsh global AI competition. It will also need to be on the forefront of technological developments, which requires major investments on both the national and the EU level.[78]

* * *

Endnotes

1. For example, the Danish start-up Hedia is developing an AI-driven diabetes assistant (https://www.hedia.co/).
2. Danish Ministry of Finance and Ministry of Industry, Business and Financial Affairs, National Strategy for Artificial Intelligence, pp. 12 & 13–14, available at: https://eng.em.dk/media/13081/305755-gb-version_4k.pdf (March 2019).
3. *Id.*
4. *Id.* National Strategy for Artificial Intelligence, pp. 12 & 13–14.
5. *Cf. Id.*
6. For similar conclusions *cf. Id.*
7. *Id.*
8. *Id.*
9. Consolidated Act No 90 of 29.01.19 on Patents. Danish patent law reflects the EPC and EPO case law.
10. Consolidated Act No 1144 of 23.10.14 on Copyrights.
11. Act No 309 of 25.04.19 on Trade Secrets.
12. Act No 426 of 03.05.17 on Marketing Practices.
13. Sect 1, para 2, no 3 of the Patent Act.
14. Act No 104 of 24.01.12 and Consolidated Act No 210 of 17.03.09.
15. Consolidated Act No 1144 of 23.10.14.
16. The "look and feel" and user interface can be protected subject to normal conditions, i.e. as works of art, provided they have sufficient originality.
17. *Cf.* C-203/02, *British Horseracing Board*.
18. Act No 309/2018, implementing the Trade Secrets Directive, 2016/943/EU.
19. Directive 2016/943/EU.
20. Regulation 2016/679.
21. Act No 502 of 23.05.2018 on Data Protection.
22. Act No 430 of 01.06.1994 on Mass Medias Information Databases.
23. Consolidated Act No 1190 of 11.10.2007 on CCTV Surveillance.
24. Directive 2016/1148/EU on Network Information Security.
25. Consolidated Act No 903 of 26.08.2019 on Health.
26. Section 3.1 has been extracted from Timo Minssen & Jens Schovsbo, *Big Data in the Health and Life Sciences: What Are the Challenges for European Competition Law and Where Can They Be Found?*, in: X Seuba, C Geiger & J Pénin (eds), Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data. Centre d'études internationales de la propriété intellectuelles (CEIPI), CEIPI / ICTSD Publication Series on Global Perspectives and Challenges for the Intellectual Property System, no. 5, pp. 121–130 (2018).
27. We focus on the central competition law rules in Articles 101 and 102 TFEU. Yet, the special competition rules regarding *mergers* have also to be considered in cases

involving big data. In the merger leading to Thomson Reuters, Case COMP/M.4726, *Thomson Corporation/Reuters Group*, of 19 February 2008, regulators in the EU and the United States had concerns stemming from big data. Both took the position that the need for a company to collect vast amounts of financial data to effectively compete with the merged firm in the market for data terminals created a significant barrier to entry. To address this concern, both authorities approved the merger on the condition that the merged firm would make copies of its database available for purchase by existing and new potential competitors; http://ec.europa.eu/competition/mergers/cases/decisions/m4726_20080219_20600_en.pdf.

28. Commission Notice (EC) on the Definition of Relevant Market for the Purposes of Community Competition Law, [1997] OJ C 372, p. 5, point 10 with reference to Case 85/76, *Hoffmann-La Roche & Co. AG v. Commission* [1979] ECR 1979-461.
29. Commission Notice, point 15.
30. The "indispensability" test is derived from Joined cases C-241/91 P and C-242/91 P, *RTE & ITP v. Commission* [1995] ECLI:EU:C:1995:98 and Case C-418/01, *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG* [2004] ECLI:EU:C:2004:257, para 38. See also Decision COMP/AT.39612 "Perindopril (Servier)" of 9 July 2014. This test, and in particular the "exceptional circumstances" sub-test, was later confirmed by Case 170/13, *Huawei Technologies Co. Ltd v. ZTE Corp. and ZTE Deutschland GmbH* [2015] ECLI:EU:C:2015:477, paras 46–7.
31. For a more detailed explanation of this test see also Minssen & Schovsbo, *supra* no. 12.
32. For further discussion, see *id.*
33. 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 [2016] L119/1 (General Data Protection Regulation/GDPR).
34. See EU Commission on the EU–US Privacy Shield, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en; note that many details of this agreement are still very controversial.
35. M. Kadar and M. Bogdan, "'Big Data' and EU Merger Control: A Case Review", *Journal of European Competition Law and Practice* 8, no. 8 (2017): 479–91, at 486, referring to Article 20 of the GDPR.
36. See Case C-238/05 Asnef-Equifax and Administración del Estado [2006] ECR I-11145, para 63.
37. Kadar & Bogdan, "'Big Data' and EU Merger Control".
38. Based on "Communication from the Commission: Guidelines on the Application of Article 101 of the Treaty on the Functioning of the European Union to Technology Transfer Agreements", OJ C 89, 28 March 2014, 3–50, point 17.
39. Commission Regulation (EU) No. 316/2014 of 21 March 2014 on the Application of Article 101(3) of the Treaty on the Functioning of the European Union to Categories of Technology Transfer Agreements (Text with EEA Relevance), OJ L 93, 28 March 2014, 17–23.
40. For an excellent and very detailed discussion of these issues, see G. Sivinski, A. Okuliar, and L. Kjolbye, "Is Big Data a Big Deal? A Competition Law Approach to Big Data", European Competition Journal 13.2–3 (2017): 119–227.
41. *Id.*
42. Commission decision of 24 March 2004 in Case C-3/37.792 – *Microsoft*.
43. Commission decision of 27 June 2017 in Case AT.39740 – *Google Search (Shopping)*.

44. Commission decision of 18 July 2018 in Case AT.40099 – *Google Android*.
45. Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, *Competition Policy for the digital era*, Final Report for the European Commission (2019), available at: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
46. See also EU report recommends competition policy for the digital era: game changer or too early to tell?, available at: https://www.ashurst.com/en/news-and-insights/legal-updates/eu-report-recommends-competition-policy-for-the-digital-era-game-changer-or-too-early-to-tell/ (2019).
47. *Id.*
48. *Id.*
49. European Commission. White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed March 9th, 2020.
50. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. Accessed March 9th, 2020.
51. European Commission. 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. https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf. Accessed March 9th, 2020.
52. See Kyriakos Fountoukakos, Veronica Roberts, Peter Rowland and Morris Schonberg, European Commission Announces Strategy for Data, Artificial Intelligence and Competition in the Digital Age. https://www.lexology.com/library/detail.aspx?g=8839c6d8-4244-4496-852a-7319378cca42. Accessed March 10th, 2020.
53. *Id.*
54. Act No 502 of 23.05.2018 on Data Protection.
55. See Section 5 of the Danish Act on Data Protection.
56. Art. 5, para 1, litra c GDPR.
57. For example, if a person has consented to processing of that persons financial information in relation to a check of creditworthiness, such information must not be used for other purposes not relevant to the credit check.
58. National Strategy for Artificial Intelligence. See also Danish Ministry of Finance, "Ny national strategi skal gøre Danmark førende inden for kunstig intelligens", 22.10.2018, available at: https://www.fm.dk/nyheder/pressemeddelelser/2018/10/kunstig-intelligens.
59. *Id.*
60. See European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act) (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)) (Ordinary legislative procedure: first reading), at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0151+0+DOC+XML+V0//EN&language=EN.
61. Danish Ministry of Finance, "Danish cyber and information security strategy", 15.05.2018, available at: https://uk.fm.dk/publications/2018/danish-cyber-and-information-security-strategy.

62. Danish Ministry of Finance, "The Danish Government: Denmark reinforces defences against digital threats", available at: https://uk.fm.dk/news/press-releases/2018/05/dk-reinforces-defences-against-digital-threats.
63. *Id.*
64. *Id.*
65. See Library of Congress, Regulation of Artificial Intelligence: Europe and Central Asia, on Denmark, https://www.loc.gov/law/help/artificial-intelligence/europe-asia.php#denmark. Accessed March 20th, 2020.
66. European Commission. White Paper. On Artificial Intelligence – A European approach to excellence and trust. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed March 9th, 2020.
67. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. Accessed March 9th, 2020.
68. European Commission. 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. https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf. Accessed March 9th, 2020.
69. Danish Ministry of Industry, Business and Financial Affairs, "Regeringen nedsætter ekspertgruppe om dataetik", 12.03.2018, available at: https://em.dk/nyhedsarkiv/2018/marts/regeringen-nedsaetter-ekspertgruppe-om-dataetik/.
70. Thomas Breinstrup, Berlingske, "Digital ansvarlighed skal være et dansk varemærke", 03.04.2019, available at: https://www.berlingske.dk/virksomheder/digital-ansvarlighed-skal-vaere-et-dansk-varemaerke.
71. Thomas Breinstrup, Berlingske, "Danmark skal være verdensmester i dataetik", 22.11.2018, available at: https://www.berlingske.dk/virksomheder/danmark-skal-vaere-verdensmester-i-dataetik.
72. Danish Expert group on Data Ethics, "Data for the Benefit of the People", November 2018, available at: https://eng.em.dk/media/12190/dataethics-v2.pdf.
73. Danish Ministry for Industry, Business and Financial Affairs, "Ekspertgruppe klar med anbefalinger om dataetik", 22.11.2018, https://www.regeringen.dk/nyheder/regeringens-ekspertgruppe-klar-med-anbefalinger-om-dataetik/.
74. Digitaliseringsstyrelsen, Dataetiks Råd, available at: https://digst.dk/data/dataetisk-raad/.
75. Regarding welfare surveillance, see also Catrine S. Byrne & Julia Sommer, Is The Scandinavian Digitalisation Breeding Ground For Social Welfare Surveillance? https://dataethics.eu/is-scandinavian-digitalisation-breeding-ground-for-social-welfare-surveillance/. Accessed March 16th, 2020.
76. Daniel Susser, Ethics Alone Can't Fix Big Tech – Ethics can provide blueprints for good tech, but it can't implement them, available at: https://slate.com/technology/2019/04/ethics-board-google-ai.amp. Curse or Blessing? Ethical and Legal Challenges of Artificial Intelligence in Healthcare (commissioned and in preparation). Gerke, Sara; Minssen, Timo; Cohen, Glenn. 'Artificial Intelligence in Healthcare'. Ed. Adam Bohr; Kaveh Memarzadeh. Elsevier (forthcoming in 2020).
77. *Id.*
78. Thomas Breinstrup, Berlingske, "Danmarks digitale førsteplads er truet", 05.03.2019, available at: https://www.berlingske.dk/virksomheder/danmarks-digitale-foersteplads-er-truet.

Timo Minssen
Mobile: +46 708 607 517 / Email: Timo.Minssen@jur.ku.dk

Professor Timo Minssen is the Director of the Center for Advanced Studies in Biomedical Innovation Law (CeBIL) at the University of Copenhagen and Researcher in Quantum Law at Lund University. Specialising in IP, antitrust and regulatory law in medical AI and big data, he leads major research projects with Harvard Law School, Harvard Medical School, and the University of Cambridge. His research publications comprise three books, as well as 120+ articles and book chapters. His work has been featured in *The Economist*, *The Financial Times* & *Times Higher Education*, and in leading journals, such as *Science*, *Nature Biotechnology, Nature Genetics*, *Nature Electronics*, and *PLoS-Computational Biology*, etc. Holding a German Staatsexamen, as well as Swedish law and life science-related LL.M. and LL.D. degrees, he is also a senior consultant at X-Officio.eu, Steering Committee Member of the Danish Association for the Protection of Industrial Property, and Expert Advisor to the WHO Digital Health Committee.

Tue Goldschmieding
Tel: +45 3341 4302 / Mobile: +45 2428 6875
Email: tgg@gorrissenfederspiel.com

Tue Goldschmieding heads up Gorrissen Federspiel's data protection and cyber security practice. Tue Goldschmieding has a background in IT and outsourcing and is experienced in dealing with complex IT and outsourcing transactions, GDPR compliance matters and data transfer schemes.

Tue Goldschmieding assists a number of the largest Danish companies with all aspects of data protection and cyber security, including (i) global implementation of GDPR compliance programs, (ii) complex data-sharing and transfer schemes, (iii) digitalisation projects, BI and big data analysis, (iv) Binding Corporate Rules, (v) risk assessments and Data Protection Impact Assessments, and (vi) governance and procedure implementation and digitalisation.

In addition, Tue Goldschmieding is a member of the board of the Danish IT Lawyer Association.

Søren Sandfeld Jakobsen
Tel: +45 3341 4116 / Mobile: +45 2428 6830
Email: ssja@gorrissenfederspiel.com

Søren Sandfeld Jakobsen assists our clients with IT, telecoms and media law matters, including the legal aspects associated with new technology, digital media and the implementation of large digital changeover projects in corporate enterprises. Søren's experience also encompasses marketing law, IP law, contract law and transactions in the broader sense.

Søren holds a position as professor of the law of property and obligations at CBS, Copenhagen Business School, and he therefore works part-time in our firm. He is the author of a large number of books and articles on subjects related to mainly IT, telecoms, IP and media law.

Gorrissen Federspiel

Axel Towers, Axelborg 2, 1609, Copenhagen, Denmark
Tel: +45 3341 4141 / URL: www.gorrissenfederspiel.com

France

Claudia Weber, Jean-Christophe Ienné & Arthur Poirier
ITLAW Avocats

Trends

Determined to face the challenges initiated by the digital transformation, the European Commission presented its strategy for Data and Artificial Intelligence in a White Paper published on 19 February 2020, which promotes a dual dynamic based both on investment and regulation. More specifically, the European will is to create a "European Data Area and a Single Data Market", by establishing, in time, a new regulatory framework to allow the free movement of data within the Union between companies, and in particular between private companies and public entities. The EU also aims to develop a responsible AI. The key issue is to develop AI in a safe and trustworthy way, combining ethics and competitiveness.

This dynamic has already been adopted by France, which has a strong and proactive understanding of the challenges and prospects offered by AI. A national strategy named "AI for Humanity" was launched in March 2018[1]: the priorities already identified were research, open data and ethical or societal issues. The steps and axes for the deployment of this strategy were developed from an economic angle in July 2019.[2] Numerous public and private initiatives have been started in those directions.

Indeed, two years after the Villani report was published, France became a privileged host territory for AI researchers and entrepreneurs wishing to exploit AI devices from all over the world. By creating the "Hub France AI" Association, major groups operating in various sectors (public transportation with SNCF, banking with La Banque Postale, public television with France Télévision, cosmetics with L'Oréal, etc.) and numerous startups have joined forces in a desire to develop a proper French AI sector. This strategy has proven to be effective, as France was the European country that attracted the most funding for AI in 2019, notably through the diversity and breadth of France's AI competences.[3] France is therefore pursuing its investment in AI and more than ever ought to display its broad support for its national startups. The acquisition of a supercomputer nicknamed "Jean Zay" in early 2020, which will double France's computing power, is a prime example of this desire.

In parallel to pure AI research, many practical applications have emerged. More specifically, France has focused on the development of AI in certain sectors of public interest. A study revealed that the following areas would be the most transformed by the development of AI in France: Energy and Environment; Transport and Logistics; and Health and Industry.[4]

These evolutions are mainly permitted by the implementation of a strengthened policy for both public and private data. Thus, the policy of opening public data, which means that access and exploitation of this data is public and free, is continuous since its initiation in 2016. This policy of developing a data economy has been renewed in July 2019, as part of the national strategy for AI launched in 2018. For example, the data economy policy

has been implemented in the Mobility Act adopted in December 2019, which stipulates that static and dynamic data collected by transport operators, infrastructure managers and transport authorities must be accessible on a dedicated platform.[5] Also, in this respect, the eagerly awaited implementing decree allowing the open data of court decisions should be released soon.

The creation of the Health Data Hub is also a significant example of this French AI optimisation dynamic. Presented as one of the major points of the French AI strategy in 2018, it was completed in December 2019. The purpose of this platform is to enable a core group of researchers implementing selected projects to access large health data sets to train artificial intelligence models. These data will be obtained from the national health data system, which includes all data retrieved by public health agencies. For example, AI could help determine appropriate and effective medical treatment by aggregating observations from multiple sources, detect precancerous conditions, develop virtual clinical trials, or monitor the impact of diagnostic or therapeutic innovations and the cross-effects of drug prescriptions. Thanks to all these perspectives, France hopes to improve the performance of its healthcare system.

Beyond these technological advances, developing an ethical AI is the French government's flagship trend and has been for several years. To this end, a "Digital Ethics Pilot Committee" was created by the National Ethics Committee in December 2019 to address the ethical issues of digital technology and artificial intelligence in a comprehensive manner. Its study, which will be completed in early 2021, will address three central themes: conversational agents; autonomous cars; and medical diagnosis. In parallel, the issue of data quality and confidence in algorithms is becoming increasingly important, as code auditing and algorithm certification are rising concerns for all the AI actors. As early as 2017, in its study entitled "How to allow humans to remain in charge? Report on the Ethical Issues of Algorithms and Artificial Intelligence", the CNIL (French supervisory authority for data protection) had recommended the creation of a national platform for auditing algorithms, as part of several of its operational recommendations.[6] In this logic, in July 2019, the certification of the algorithms was described as "absolutely decisive" by the Minister of Economic Affaires Bruno Le Maire. It is true that some algorithms have been strongly contested in recent years: for example, the algorithm of the national platform "Parcoursup", which aims at enabling high school graduates to join universities, has been criticised for its opacity when it was finally published. Certification could then intervene as a tool for legitimising AI and eliminating bias and could thus constitute a vector of trust for citizens.

This is particularly important as algorithms will be introduced in many areas of public interest, such as justice or national security. One thinks, for example, of the government's will to experiment facial recognition coupled with video surveillance systems, which is highly contested given the consequences on fundamental rights and freedoms, in particular the right to privacy.

Ownership/protection

The protection of an artificial intelligence and of the creations resulting from the use of such a technology raises different sets of questions.

Protection of AI

At present, there is no legal or regulatory framework specifically dedicated to AI, big data or machine learning, either at national, European or international level. Current intellectual property mechanisms of protection must therefore be considered for AI applications. Due to the variety of the potential elements composing artificial intelligence (algorithms, software,

hardware, databases, interfaces, computer programs, component interacting with the AI, etc.), multiple intellectual property rights may be involved in the protection of an AI. Therefore, the protection of AI may lie in a patchwork of rights which necessarily raises multiple issues concerning their ownership and the contractual agreements to be concluded. Besides this patchwork of rights, and under certain circumstances, an AI tool may be protected as a whole, by a patent registration.

Trade secrets

Intellectual property rights offer no protection for algorithms. Those are indeed excluded from patentability and considered as a mere idea in terms of copyright law. Therefore, for algorithms that are not publicly disclosed, trade secret protection is to be considered. Trade secret protection has recently been formalised by European Directive n°2013/0402 and transposed by French law n°2018-670 into the French commercial code. To be protected, the concerned information (i.e. an algorithm or a whole AI system) must be secret, must have a commercial value, and must have been protected by reasonable protecting measures. Such protection mechanism could be particularly adapted to AI as it offers the possibility to sue, under certain conditions, third parties using others' confidential information. It must nevertheless be borne in mind that there is no infringement action as such for trade secrets, under French law.

Copyright

Since European Directive n°91/250 CEE of 14 May 1991 (now consolidated as Directive n°2009/24/EC of 23 April 2009), the protection of computer programs has been harmonised at the European level under copyright law, though its legal regime differs from the common copyright regime, in particular regarding ownership principles and the scope of moral rights. The software part of an AI tool could therefore be protected by copyright law if it is "original", in the sense that it is its author's own intellectual creation. The French copyright protection of software includes notably the computer program itself (source and object codes), but also the program structure and the preparatory material. However, the functionalities of the software as well as the algorithm on which it is based is excluded from this protection, because under French law, it is generally agreed that ideas are for all to use and only a formalised creation can be appropriated. In that view, a French Court of Appeal[7] has recently judged that the algorithm is "excluded from the benefit of copyright protection" "as a succession of operations which only translates a logical statement of functionalities, devoid of all the functional specifications of the product concerned". The same applies for the functionalities of a computer program, as the CJEU underlined that "[accepting that] functionalities of computer program can be protected by copyright would amount to making it possible to monopolise ideas, to the detriment of technological progress and industrial development".[8]

Considering the ownership of the rights, in principle, the person who creates the protected work is the owner of the related rights. Two major exceptions exist to this principle, that are relevant when computer programs are concerned. On the one hand, in the field of software development, in case of an employment contract the rights to the software are automatically transferred to the employer. On the other hand, in case of collective work created at the initiative of a person who publishes and discloses it under his direction and name and in which the personal contributions of the various authors are merged in the overall work, the rights are automatically vested in this person.

Concerning works other than computer programs that constitute an AI device, such as original databases or interfaces, they must be considered individually in order to determine whether it is

protected, and if so, to identify which legal provisions are applicable to their ownership. In these conditions, assignment contracts have a major importance to secure and operate an AI device.

Databases

An important part of an AI device is the set of data on which it feeds. Relations between AI and databases are multiple, and the question of their protection remains complex. Under French law, databases may benefit from the protection of copyright (for its "container", if its structure is original, and/or for each element composing the database considered independently, to the extent that they are also original), or from a *sui generis* right of database producers that applies to its content considered as a whole. Stemming from European Directive n°96/9/CE, the *sui generis* right grants protection to the contents of the database, against non-authorised substantial or repeated extraction and use. It benefits the producer of the database, i.e. the person who takes the initiative and the risk of the investment (financial, material or human) to constitute, verify the database or present the contents of the database.

To initiate a proper deep learning process, the question of the protection and property of these databases is of great importance. Contracts have a key role to play here, as the developer of the AI will rarely be the owner of such databases, while they are often essential to the operation of their system. The same applies to the underlying works or elements used to train the AI (copyright if original works of art are processed, or personality rights if names, faces, etc. are processed).

It is to be noted that the practices in this field will necessarily be impacted by the recent European Directive n°2019/790 which introduces an exception of "data and text mining" to copyright and *sui generis* rights of database producers. Its 4th article allows the "reproductions and extractions of lawfully accessible works […] for the purposes of text and data mining" under the condition that their rightsholders did not expressly reserve the use of works at issue, in particular in their contracts.

Patents

The most notable increases in patenting activity worldwide between 2013 and 2016 feature a machine learning technique, called deep learning.[9] At first sight, these statistics may be surprising considering that in patent law, computer programs, as well as mathematical methods, are expressly excluded from protection. In France, article L 611-10 of the Intellectual Property Code states that those cannot be considered as inventions. The European patent convention imposes similar bans. However, the composition of an AI device is not limited to its software and its algorithm but is made of multiple components that may not be patentable by themselves, but possibly patentable as a combination. Indeed, it is possible to obtain a patent for an inventive process that includes software and algorithms, provided that the invention (i) does not relate solely to the computer program and method, and (ii) is new, involves an inventive step and is susceptible to industrial application. In this case, the patent will be granted for the overall process, i.e. the combination of the technical components, the software and the algorithm which participate to the invention. An artificial intelligence therefore could subsequently be protected by a patent right if it meets these criteria. Regarding AI, the practice of the French Office (INPI) evolved recently, as a result of the extension of its scope of examination to inventive step in 2019. In its last guidelines on patent issuance, published on October 2019, INPI clarifies the conditions of patentability of an AI method or simulation and makes it easier for such invention to be patented.

On the issue of ownership and setting apart the case of invention made within the scope of employment, according to article L 611-6 of the said code, the patent owner remains in principle its inventor, with a presumption of ownership in favour of its applicant.

AI creations

Another issue might lie in the way AI-generated creations may benefit from a protection under the French Intellectual Property Code.

In patent law, the EPO recently refused two European patent applications in which an AI was designated as the inventor, arguing that the inventor must be a human being, not a machine. These decisions address the matters of protection and ownership of the creations made by an AI under patent law and are in line with the French approach.

In French Copyright Law, no legal provision is dedicated to these creations. Therefore, one must rely on the general principles of copyright law.[10] French Copyright Law is based on a personalist conception, according to which the author can only be the natural person who carried out the act of creating the original work. This work is eligible for protection only if it reflects the "imprint" of the personality of its author. As they do not bear the imprint of a personality, it is generally considered that the decisions made by an AI cannot satisfy these criteria, and that these creations cannot be protected under copyright law.

Under current law, only a human intervention in the process of artificial creation, of enough importance to imprint originality, could justify a protection under copyright law, like in computer-aided creation including human control. In this hypothesis, AI would be a mere tool serving the author's creativity, the author being the owner of the rights. For the time being, on the question of ownership, the creator of an AI itself could hardly be *de facto* qualified as the author of the works created autonomously by the AI as underlined by the AIPPI in its 2019 report on artificially generated works; that would imply that elements composing the AI (originality of a software, etc.) are also present in the works generated thereof which is rarely the case.[11]

These issues of protection and ownership are currently discussed by the legal doctrine. For instance, the French High Council of the Literary and Artistic property (CSPLA) considered, in its report of January 2020, potential solutions for the protection of such creations (copyright vested in the creator of the AI or its user, new specific type of copyright or related right, new *sui generis* right, refusing the protection for such creations, etc.). The High Council considered that, beside the creation of a new right, the copyright may be sufficiently flexible to encompass this type of creations. However, the debate remains open in France, as in the European Union.

Antitrust/competition laws

AI is increasingly seen as a new powerful instrument for companies to indulge in anti-competitive practices, both in the area of cartels and abuses of a dominant position.

This matter was dealt with in a report on Algorithms and Competition Law published in November 2019 by the French and German Competition Authorities. It dwells on the assumption that the use of algorithms has opened new possibilities for economic agents to behave in ways that can upset the market equilibrium. The increasing use by companies of algorithms that manage business strategy and, *inter alia*, the strategy for determining market selling prices (particularly in the online retailing of consumer goods) is of concern. The pricing algorithms used for setting price scales are a focus of this study, as they can contribute to undermine the market balance by creating obstacles to the free determination of prices through the interplay of supply and demand.

Of concern for both Authorities are dynamic pricing algorithms that make it possible to automatically adapt the price offer on the basis of customers' purchasing behaviour but also

on the basis of the prices charged by competitors. Self-learning algorithms are also targeted, as they are capable of learning by themselves in order to adapt their decision-making process with a focus on obtaining the optimal price. These mechanisms may therefore permit practices of alignment or coordination between undertakings, which could constitute anti-competitive agreements.

However, current competition law provisions have not been specifically adapted to the new stakes raised by AI, big data and machine learning. More broadly, no specific provision on AI has been introduced into French law, except in article L 111-7 of the French Consumer Code, which states that any operator of an online platform is required to provide consumers with fair, clear and transparent information on the methods of referencing, classification and dereferencing by algorithms. In any case, the French Competition Authority considers that current French and European texts allow for the apprehension of anti-competitive price-fixing practices, even when they are based on the use of algorithms.

Still, in February 2020, the French Competition Authority presented its reflections on competition policy regarding digital issues. It made proposals on the possible ways of adapting the law to the specificities identified in markets dominated by digital giants.[12] For example, regarding the notion of abuse of a dominant position, consideration could be given to redefining the notion of essential facilities, given the inescapable nature of certain databases, user communities or ecosystems. Developing a new standard to qualify these "unavoidable" assets could be useful. As for mergers, the current control thresholds seem unsuitable for digital giants: indeed, emerging players who have not yet monetised their innovations and who do not have a significant turnover can nevertheless represent extremely promising acquisitions. Such acquisitions may therefore be a source of danger for the markets and should be notifiable to the authorities according to more appropriate criteria.

The French Competition Authority is aware of the fact that if algorithms may be a more discreet means of committing anti-competitive infringements than traditional cartels, they may also be a particularly appropriate and effective weapon for suppressing infringements of free competition. In January 2020, the French Competition Authority set up a department specialising in the digital economy, which will develop in-depth expertise on all digital subjects and collaborate in the investigation of anti-competitive practices in the digital economy. The French Competition Authority has therefore expressly made this department "*responsible for developing new digital investigation tools, based in particular on algorithmic technologies, mass data and artificial intelligence*".

Board of directors/governance

Major French companies are now integrating the challenges of artificial intelligence, whether managerial, legal or ethical, into their governance policies. Indeed, the implementation of automated processes (machine learning) to improve the organisation, production and control of social activity represents an interesting resource for each of them.

AI and machine learning can help law firms and companies in the process of due diligence, which is more and more difficult to achieve manually because of the quantity of data that needs to be processed. AI can help identify relevant documents and reduce the cost and duration of this phase of verification. AI and machine learning can also help data controllers on their regulatory concerns, when used as a compliance tool. For example, AI applications can help data controllers to map personal data processing, assist them in the implementation of the data subjects' right (the right of access) or help identify and locate security incidents.

Nonetheless, French companies remain discreet about their internal decisions. But they have become aware of the challenges of AI in recent years and have taken action accordingly.

However, no legal provisions have been adopted regarding AI governance in France and nor is there any legislative project in progress on the matter. The integration of AI into corporate governance remains entirely discretionary.

Regulations/government intervention

If the GDPR is an essential regulatory issue when developing any AI, machine learning and big data projects, the French legislator and authorities have also been reflecting on regulation in order to facilitate the access to data.

Algorithms and the GDPR

Since 25 May 2018, the most obvious issue with the use of AI, big data and machine learning has been their compliance with the GDPR.[13] When these technologies require the use of personal data, the processing is necessarily massive and therefore threatening to the right to privacy. With a €50 million fine imposed on Google by the CNIL (French Data protection Authority: "*Commission Nationale de l'Informatique et des Libertés*") in January 2019, France leads the European countries, along with Spain, in terms of GDPR penalties.

The conciliation of AI technology with the provisions of the GDPR constitutes a challenge for companies both in terms of compliance and financial risk management but also for optimising their IT projects. Such a conciliation is challenged by at least two core principles of the GDPR: purpose limitation; and data minimisation. In practice, the implementation of AI devices inevitably leads to the accumulation of masses of data, and even looking for correlations or calculating results before knowing the exact purpose of the processing. However, one of the fundamental principles of the GPDR is that any processing of personal data must be carried out after having explained the purpose(s) of the processing to data subjects, which must be: determined; legitimate; and specific. This implies that the data controller must choose why the AI technology is deployed before implementing it, which is not always in line with that kind of technology.

As for the principle of data minimisation, it requires that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (article 5 GDPR). It means limiting the quantity of data, minding its relevance and its suitability for the stated purpose(s). But minimising the quantity of data collected is impossible when using AI, big data or machine learning: a different assessment of the minimisation principle shall be required, if one wants these technologies to eventually comply with the GDPR. Data minimisation would have to be understood in a flexible way, allowing AI and big data users to keep on processing big quantities of personal data, but in a more ethical and accurate way. In that regard, the French 2020 Finance Act has authorised, as a three-year experiment, the tax and customs administration to collect freely accessible data on social networks and electronic networking platform, and to exploit it in order to detect tax fraud. In its opinion of 12 September 2019, the CNIL has recalled, however, the principle of data minimisation and the need to process data that is strictly necessary for the detection of tax fraud, and to immediately delete data considered irrelevant.[14] It should be pointed out that the CNIL did not challenge in that case the massification of the data but its relevance.

Also, in light of the data minimisation principle, the project to implement facial recognition on the premises of two French high schools was strongly contested by the CNIL. In its Decision of 17 October 2019, the CNIL considered that the proposed mechanism is contrary to the main principles of proportionality and minimisation of the data provided, arguing that the objectives of security and the fluidity of entries to these high schools can be achieved by means that are much less intrusive in terms of privacy and individual freedoms.[15]

The CNIL has expressed the desire to encourage the search for technical solutions to make France the leader in ethical AI. Several projects have thus seen the light of day, with various objectives: to promote the explanation of the logic of algorithms to regulators, companies and citizens; to develop research infrastructures that respect personal data; or to launch a participative national cause to boost AI research.[16]

Access to data

Since the entry into force of the French Digital Republic Act on 8 October 2016, which transposed Directive n°2003/98/CE,[17] the public sector is subject to an obligation by default to make its data available and must now provide a "public data service". Every public community above 3,500 inhabitants, and every administration employing more than 50 agents must make available online their database and data, (as the case may be, after anonymisation) when it presents an economic, social or sanitary/environmental interest. The Digital Republic Act also allows the online publication of public interest data such as: court decisions; algorithms; land values; energy production; and consumption data, etc.

The open data policy leads to new services and new development axes for public/private partnerships, but above all to more knowledge for French companies. An example of such services is the augmented reality application that reveals all the prices of real estate sales made around the place you are in.[18]

The new adopted French law on mobility guidance (24 December 2019), adapting European Regulation 2017/1926,[19] grants new competence to public communities to organise services such as carsharing, carpool and transport on demand. Opening data on French mobility offers is scheduled for 2021. It encompasses static (stops, schedules, prices, etc.), and real-time data (disturbance, availabilities) of public transportation or on demand as well as road networks and networks of parking areas: the goal is to make available this data to citizens and businesses in one click. In addition, the Mobility Guidance Act authorises the government to take, within a period of 12 months from the promulgation of this law, all measures with the aim of making accessible certain information. For instance, measures will be taken in order to make data collected from connected vehicles' integrated systems available, for certain purposes.

On the ground of this open data policy and on a more dramatic and immediate concern, various datasets have been published on the public data portal data.gouv.fr during the progression of the COVID-19 epidemic. The data has been collected from the National Public Health Agency, including, for example, the number of emergency room visits for suspicion of COVID-19, broken down by age, sex and department. The principal goal of this platform, however, is to allow the emergence of innovative initiatives.

Civil liability

The wide and increasing use of AI raises important questions regarding responsibility: which stakeholder shall be liable in case the use of an AI or an algorithm has caused damages to something or someone?

In France, the preliminary draft on the responsibility reform,[20] issued on 13 March 2017, unfortunately did not tackle the issue. More recently, the report of the Paris Court of Appeal on the French reform of civil responsibility and commercial relationships,[21] published on 25 June 2019, simply excludes any regulation of AI as part of the said reform. The report, however, lists the following possible solutions, weighing their advantages and disadvantages:

- Liability for defective goods, already existing under French Civil Law.
- Liability for the actions of things, already existing under French Civil Law.
- Creating a legal personality for AI tools and robots.

- Fault-based liability, already existing under French Civil Law.

According to the Senate, in its information report on European strategy for artificial intelligence (31 January 2019), "there can be no liability of machines or robots. An artificial intelligence is, above all, a machine, which has developers and manufacturers. They must be liable in case of difficulty".[22] As a matter of fact, "each stakeholder of the chain is "co-perpetrator" of the result that is artificial intelligence: responsibility lies in the gap between what the AI does and what the AI should do".

Both reports favour a solution at the European level.

The major issue resulting from the use of artificial intelligence, machine learning or big data is indeed to determine liability in the event of a malfunction. Given the lack of specific legislation on the matter, one may rely on contract law when applicable. In most cases, the user of the technology (the buyer) shall have signed terms and conditions with the AI/machine learning/big data provider. This negotiation and signing process should be a major focus for both parties. Negotiating and drafting a custom-made contract is today the best way to secure the relationship and allocate responsibilities. Contract law being largely suppletive, it allows significant flexibility for stakeholders willing to secure their commercial relationship. Two key issues ought to be tackled when implementing a project involving the use of AI, machine learning or big data: liability; and unknown events.

The first issue consists in pre-qualifying the damages that can be compensated for. The French Civil Code provides that damages within a contractual liability can only include what is an immediate and direct consequence of the contractual breach, even in case of gross negligence or intentional misconduct.[23] When faced with damages resulting from the use of AI, machine learning or big data, the notion of direct or indirect link between the contractual breach and the damage itself shall prove to be essential. In case of complex chains of responsibilities, prequalifying which damages must be considered direct or indirect will bring legal certainty to the stakeholders, allowing them to determine how they intend to allocate responsibility instead of leaving it to the interpretation of a judge. The parties can thus decide that some damages shall not be considered direct consequences of a breach of contract, for instance: loss of turnover; or loss of data.

French Contractual Law also enables the parties to limit their financial liability, if the limitation does not conflict with one of the essential obligations of the contract and is consistent with the risk distribution.

The second important issue consists in contractually allocating the risks in case of unforeseeable change of circumstances. Under French law, the parties can stipulate which of them shall bear the costs generated by unforeseeable developments and changes within the meaning of article 1195 of the French Civil Code. This article provides that if a change in circumstances that were unforeseeable at the time of the contract conclusion makes performance excessively onerous for a party who had not agreed to assume the risk, that party may request a renegotiation of the contract from its co-contractor or a revision of the contractual provisions by a judge. It is thus possible to set aside this legal provision and allocate in advance to a party the risk of such an event. Similarly, the concept of *force majeure*, which had been developed in France by case law and has been codified in the French Civil Code by the 2016 reform of contract law, releases the debtor from his obligations, when an event qualified as *force majeure* happens. French Law allows the parties to a contract to contractually define what is and what is not an event deemed to constitute *force majeure*. Thus, any client of an AI solution must understand this concept and pay attention to the contractual provisions pertaining to *force majeure*.

Endnotes

1. https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf.
2. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=0B24A9E8-CBA3-4F4C-8379-78D20E88ACF2&filename=1314-%20IA%20DP.pdf.
3. https://www.francedigitale.org/the-road-to-ia-2019/.
4. https://www.cget.gouv.fr/sites/cget.gouv.fr/files/atoms/files/2019-02-intelligence-artificielle-etat-de-l-art-et-perspectives-synthese.pdf.
5. LOI n°2019-1428 du 24 décembre 2019 d'orientation des mobilités.
6. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf#page=59.
7. Cour d'appel de Caen, 18 March 2015, Ministère public / Skype Ltd et Skype Software Sarl.
8. CJUE, 2 May 2012, SAS Institue Inc. / World Programming Ltd.
9. WIPO - Technology Trends 2019 – Artificial Intelligence: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.
10. Report of the French High Council for literary and artistic property on "legal and economic issues of the Artificial Intelligence in the areas of cultural creation" published on 6 February 2020.
11. https://www.aippi.fr/upload/2019%20Londres/DROIT_DAUTEUR_-_Rapport_definitif.pdf.
12. https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.28_contribution_adlc_enjeux_num.pdf.
13. 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 n°95/46/EC (General Data Protection Regulation).
14. https://www.cnil.fr/fr/projet-de-loi-de-finances-2020-publication-de-lavis-de-la-cnil.
15. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.
16. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.
17. Directive on the re-use of public sector information https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:En:HTML.
18. https://www.data.gouv.fr/fr/reuses/explorateur-de-biens-vendus-dvf/.
19. Regulation supplementing Directive n°2010/40/EU with regard to the provision of EU-wide multimodal travel information services https://eur-lex.europa.eu/eli/reg_del/2017/1926/oj.
20. http://www.justice.gouv.fr/publication/Projet_de_reforme_de_la_responsabilite_civile_13032017.pdf.
21. http://www.justice.gouv.fr/art_pix/Rapport_CA_PARIS_reforme_responsabilite_civile.pdf.
22. http://www.senat.fr/rap/r18-279/r18-2791.pdf.
23. Article 1231-4 of the French Civil Code.

Claudia Weber
Tel: +33 6 1324 5844 / Email: claudia.weber@itlaw.fr

Claudia Weber has been working in the fields of information technology, personal data protection and intellectual property since 1994.

Before creating ITLAW Avocats in 2005, Claudia Weber practised for nearly 10 years in French and international law firms specialising in new technologies. She specialises in the information technology, internet, innovations (especially AI, machine learning, IoT, health, big data, etc.), telecoms, data protection, digital marketing, cybersecurity, intellectual property, and licensing sectors.

She practises a wide range of activities, such as negotiation and drafting of complex contracts, supporting compliance with the GDPR, audits of IT projects, websites and contracts, mediation, litigation, etc. in a variety of sectors such as retail, insurance, health, real estate, construction, press, audio-visual, etc. As ITLAW Avocats is also a training organisation, Claudia Weber offers training courses in the matters stated above.

Jean-Christophe Ienné
Tel: +33 6 4797 0582 / Email: jean-christophe.ienne@itlaw.fr

Before joining ITLAW Avocats, Jean-Christophe Ienné studied law at Panthéon-Assas University in Paris and passed the bar examination in 1992. He worked as a lawyer for more than two years with a law firm specialising in information technology law and for 20 years with a boutique firm specialising in intellectual property law, audio-visual law, media and press law. He joined ITLAW Avocats in 2017.

He specialises in the information technology, internet, television, audio-visual and film production, press, publishing, music and performing arts, and advertising sectors, with regards to both counsel and litigation.

Jean-Christophe Ienné practises a wide range of activities, such as negotiation and drafting of complex contracts such as software licensing agreements and cloud contracts, licences auditing and litigation. As ITLAW Avocats is also a training organisation, Jean-Christophe Ienné offers training courses in the matters stated above.

Arthur Poirier
Tel: +33 6 2569 1613 / Email: arthur.poirier@itlaw.fr

Before joining ITLAW Avocats, Arthur Poirier worked for almost two years as an in-house lawyer for the insurance company Cardif, where he was in charge, amongst other things, of supporting compliance with the GDPR. Arthur Poirier drafts and negotiates IT contracts (cloud contracts, implementation contracts, data processing agreements, software licence agreements, among others) and notably helps companies comply with the GDPR and the E-Privacy Directive.

As ITLAW Avocats is also a training organisation, Arthur Poirier offers training courses, especially in data privacy matters, contract law, IT contracts, e-commerce and e-marketing.

ITLAW Avocats

281, rue de Vaugirard, 75015 – Paris, France
Tel: +33 1 8362 6175 / URL: www.itlaw.fr

Germany

Christian Kuß, Dr. Michael Rath & Dr. Markus Sengpiel
Luther Rechtsanwaltsgesellschaft mbH

Trends

German companies are heavily investing in artificial intelligence, big data and deep learning. According to a study of IDG Research Services, 57% of German companies already employ AI technology; while the services sector and consumer IT are dominated by foreign companies, especially from the US. The German industrial sector is quickly adopting and advancing these new technologies. The German economy rests mainly on the industrial sector, most prominently on its well-known automotive companies. The backbone of the German industrial sector consists of mid-sized manufacturing companies, the so-called "*Mittelstand*". Many of these companies are acting on a global scale and are leaders in their respective business sectors. It is therefore of some concern that mainly large German companies prioritise technologies such as machine and deep learning, while the "*Mittelstand"* and smaller companies are still comparatively reluctant to invest in this trend. In order to accelerate the development and to secure Germany's attractiveness as a business location, the German Federal Government launched its Artificial Intelligence Strategy in November 2018 and pledged to invest EUR 3 billion until 2025. Most of the technologies used in the industrial sector are likely to affect business-to-business relationships, manufacturing processes, the supply chain and final products. Machine learning and AI are still widely used as a tools to optimise existing processes; however, only one quarter of German companies intend to use these technologies to develop new products and services. Yet, many companies are currently in the process of integrating machine learning into their business activities and these figures might already change in the near future.

Germany's automotive companies make use of artificial intelligence in order to foster innovation in the areas of autonomous driving and e-mobility. In 2019, 58% of patents related to autonomous driving originated from Germany. Nevertheless, the German car manufacturers are in fear of being pushed out of the market by companies like Google or Apple, who are also heavily investing in autonomous driving. With such new competitors on the horizon, German car manufacturers are joining forces in order to stay ahead of the curve. But these new technologies do not only boost innovation in the automotive sector. Numerous start-ups are developing new products and services, and universities are conducting comprehensive research on how artificial intelligence can be employed in innovative ways. In the European Union, Germany ranks No. 1 as the country with the highest number of AI-related start-ups.

While the business and research communities are eager to advance the process, politicians and the media are cautioning to be aware of the risks the new technologies might pose. This relates in particular to the labour forces, where people fear being replaced by artificial intelligence and robots. Workers' unions especially remain rather sceptical towards these new technologies. Furthermore, privacy concerns arise when adopting new AI technologies;

e.g. Amazon's Alexa being a cause of heated debate. These concerns are inhibiting the widespread use of AI technology in Germany. As a result, the German Government is facing the challenge of finding a viable compromise between these conflicting interests, which leads to a rather constrained approach to artificial intelligence in Germany.

Key legal issues

In Germany, the discussion of the legal ramifications of AI has only just begun. It is heavily driven by the underlying ethical questions. Humanity should not blindly exploit all possibilities of artificial intelligence. How and for what purposes artificial intelligence should be used, first and foremost, is a question of ethics. Ethical principles instruct human beings in their actions and decision-making, taking into account (social) values. Simultaneously, these principles define limits that people should not cross and attempt to balance the risks and the opportunities. The ethical discussion has led to five main principles: beneficence; non-maleficence; autonomy; justice; and explicability. While the legal discussion focuses on particular questions, the proposed solutions often refer to one or more of the ethical principles.

The spectrum of legal questions discussed is diverse. One topic relates to whether and how the technology itself, i.e. the underlying algorithm, can be protected by intellectual property law. As the training of artificial intelligence requires large amounts of data, data protection is a highly debated topic in Germany: if the data used relates to an identified or identifiable natural person, it is considered personal data and therefore protected by the General Data Protection Regulation (GDPR). As such, its processing has to comply with the requirements of the GDPR. Similar problems arise when texts, images or videos from the internet are used to train the artificial intelligence: these works are protected by copyright law. If these works are "read" by the artificial intelligence during the training, this might lead to (partial) reproduction of the protected work. Yet, the copying of protected works requires the consent of the author. In order to answer these questions, the existing laws have to be applied to artificial intelligence.

However, artificial intelligence also raises numerous questions, which cannot be addressed by referring to existing laws. For example the problem of liability: who should be liable if the artificial intelligence causes harm to a human being. One might think of autonomous driving where the car causes a crash: the liable person could either be the manufacturer, the driver, the owner or the artificial intelligence itself, if endowed with a legal personality.

Ownership/protection

Protection of AI

The development, implementation and training of artificial intelligence systems (AI Systems) requires considerable investments. In order to protect these investments, the question arises of who the owner of the AI System is and how it can be protected against competitors using the technology to advance their own products or services.

An AI System consists of various different components: hardware; software; databases; sensors that record and transmit data; and active parts acting in accordance with output of the artificial intelligence, e.g. robot arms, car brakes or a graphical or vocal user interface. Furthermore, several companies and people are involved in the development and production of an AI System. These facts leave plenty of room for various intellectual property rights, in particular to protect each component of the AI System. Due to the various people and components involved, it is usually not possible to protect the AI System as a whole. This might only apply if the AI System is less complex and essentially developed by one company.

Patent protection

Nevertheless, when we focus on the artificial intelligence itself, i.e. the software and the algorithm, particular legal issues arise to protect them. In general, it is not possible in Germany to apply for a patent if you want to protect a software solution. Patents shall only be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible to industrial application. According to the German Federal Supreme Court, an invention in the field of technology requires an instruction for the controllable use of the forces of nature to achieve a causally overseeable result.[1] Computer programs as such do not use the forces of nature to achieve a result. Computer programs are based on the rules of logic, but the activity of the human mind is not one of the controllable forces of nature. Therefore, programs for computers or algorithms are not patentable inventions under the German Patent Act.[2] However, the patentability of a computer program shall only be excluded to the extent to which protection is being sought for the subject-matter or activities referred to as such.[3] Therefore, it is possible to apply for a patent if the inventor wants to protect a "computer-implemented invention". A computer-implemented invention is an invention that includes computer programs, but also other technical components, like an anti-lock braking system.[4]

Patent protection is possible if the computer program is embedded in the process of a technical device. The Federal Supreme Court has established a three-stage test to assess whether a computer-implemented invention is patentable. At the first stage, the court examines whether the claimed invention relates to a field of technology (*Technizität*). Therefore, the non-technical components, i.e. the software, has to be distinguished from the technical components. Only the technical components can justify patent protection. The Federal Supreme Court generally affirms the necessary technicality with regard to universal computers, i.e. not the software itself, but the software running on a universal computer. At the second stage, the court analyses whether patent protection is claimed for a program "as such". This is the case if the invention does not contain instructions which serve to solve a concrete technical problem with technical resources. Finally, at the third stage, whether the other requirements for patent protection are fulfilled are checked: the invention has to be new; involve an inventive step; and has to be industrially applicable. Therefore, patent protection cannot be claimed for the algorithm or the software of an AI System as such, rather only in combination with hardware components.

The distinction between the virtual and the physical sphere leads to problems when we think about new forms of research using the possibilities of artificial intelligence. In the past, research was conducted through observations of the real world. The typical inventor conducts experiments in a laboratory. Nowadays, these experiments are replaced by simulations calculated with artificial intelligence: a well-known example is the folding of protein structures with Google's deep mind engine. If such simulation results in a new invention, it is highly debated whether such results can claim patent protection as they are based on logic in the virtual space and not on the forces of nature in the physical space.

Copyright protection

If we focus on the software element of an AI System, this component can be protected as a computer program under the German Copyright Act. Computer programs are programs in any form, including design material. The protection applies to all forms of expression of a computer program. However, the particular value of an AI System lies in the underlying algorithm and the "weights" of its neural network, caused through the training of the artificial intelligence. Therefore, the question arises of whether these parts of an AI System can

be protected through the Copyright Act. With regard to the algorithm, one has to keep in mind that the algorithm and the computer program are not the same. The algorithm is the abstract form of a computer program.[5] The software allows this algorithm to be read and processed by a CPU. Since the algorithm is the abstract concept of a computer program, the algorithm cannot be protected through the German Copyright Act. The law states that ideas and principles which underlie any element of a computer program, including the ideas and principles which underlie its interfaces, shall not be protected by copyright.[6] It is the common understanding in Germany that algorithms are such general ideas and thus not protected by copyright. The weights might be (a part of) a computer program, which is protected by copyright law. If a neural network is being trained and learns to process inputs to create the correct output, this learning is reflected in the weights of each neuron. The weights resemble the memory of a human brain. However, the problem with copyright protection is that the weights are not a "work" created by a human being.

The German Copyright Law is focused on the protection of the author and his relation to his work. The Copyright Law does not only protect the economic interests of the author, but also his moral rights. This understanding is the general foundation of copyright law in continental Europe, but differs from the approach in the US and the UK. Based on this approach, only works from a human being can be protected under the Copyright Act. Copyright protection is not denied if the author uses technical resources as mere tools to create his work (computer-assisted work), but it is necessary that the work is characterised by human achievement. If there is no human imprint or if it is only subordinate, copyright protection is excluded. Therefore, the weights of a neural network are not subject to copyright protection as a computer program. This might be different if the neural network is trained through monitored or reinforced training, because the development of the weights could be attributed to a human being. In the case of unattended learning, no link to a human being exists. Therefore, copyright protection for computer programs does not apply.

However, the weights could be protected as a database under the German Copyright Act.[7] A database is a collection of works, data or other independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means and whose obtainment, verification or presentation requires a substantial qualitative or quantitative investment. With regard to the protection of the weights, the consideration of which investments have to be taken into account is particularly problematic, because the training itself (compared with the development of the AI System) does not require substantial investments. Furthermore, whether the weights can be considered as "independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means" is also problematic. The value of the weights does not rest within one neuron, but in the trained neural network as a whole. Therefore, protection as a database will not apply in most cases.

Protection as a trade secret

Finally, the algorithm and the weights could be protected as trade secrets. The EU Trade Secrets Directive and the German Trade Secrets Act (GeschGehG) have lately been introduced in Germany and caused some changes to the law. In particular, the requirements for the protection of a trade secret have changed. A trade secret is information which is neither generally known nor readily accessible, either in its entirety or in the precise arrangement and composition of its components, to the persons in the circles who normally handle this type of information, and is therefore of economic value and subject to the circumstances after appropriate secrecy measures by its lawful owner. In fact, it is therefore important that

the holder of the trade secret takes appropriate measures of secrecy in order to protect his trade secret. Such measures can be non-disclosure obligations, but also technical protective measures, like encryption. This becomes particularly important if the holder hands over the AI System (and thus the algorithm and the weights) to a third party for use. Furthermore, so-called "reverse engineering" is explicitly allowed by the Trade Secret Act. If the holder wishes to prevent this, he only has the option of contractually prohibiting reverse engineering.

Summary

To summarise, AI Systems can be protected. Copyright protection as a computer program is only sufficient to a limited extent, since it does not include the algorithm and the weights. In this respect, only protection as a trade secret is possible, which is linked to appropriate measures for secrecy.

Data Protection

Automated decision-making

If artificial intelligence is used to process personal data, this use has to comply with Art. 22 of the GDPR. The provision grants the data subject the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The legal effect of this right of a data subject is a general prohibition for the use of artificial intelligence for automated decision-making based on personal data in general. The aim of this provision is to prevent a human being from being subjected to a decision made by a machine which significantly impacts the life of this human being. A human being shall not be the object of logic without a person reviewing the decision. However, the GDPR foresees three exceptions from this general rule, if: (a) the automated processing is necessary for entering into, or performance of, a contract; (b) it is authorised by Union or Member State law; or (c) it is based on the data subject's explicit consent. Where exceptions (a) or (c) apply, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

However, the general prohibition only applies if the decision is not finally reviewed by a human being. Currently, most use cases for artificial intelligence aim to support a human being. For example, a doctor is supported by an AI System to detect cancer or a driver is warned through an audio signal that he is crossing a lane. In these scenarios the artificial intelligence does not make the final decision. It is always a human being who analyses the result of the AI System and, using other sources of information, like his knowledge and experience, comes to a final conclusion. In all these cases, the prohibition set out in the GDPR does not apply. However, not every human interaction is sufficient to circumvent the prohibition. The person must be able to override the automated decision and replace it with a decision based on its own considerations. Even if the AI System does not have the authority for a final decision, we have to consider the effect an AI-proposed result has on the individual who has to reach a final conclusion. Even if the individual is entitled and able to actually deviate from the proposal of the AI System, he will not necessarily do so: if he decides against the proposal of the AI System and later on it appears that his decision was wrong and the proposal from the AI System was correct, he will be under pressure to justify his decision. This conceived pressure alone can prevent an individual from exercising his decision-making power.

Duty to inform

The data controller is obliged to inform the data subject of the existence of automated decision-making, including profiling and, at least in such cases, to provide meaningful

information to the data subject on the logic involved and the scope and intended effects of such processing. The controller must therefore first inform the data subject whether he uses automated decision-making. If this is the case, the data controller has to explain to the data subject how the logic involved works and which consequences the decision can have for the data subject. The data controller must provide the information in a precise, transparent, comprehensible and easily accessible form in clear and simple language. Thus, the data controller has to explain a complex technical process in such a way that anyone understands it. This task becomes particularly difficult if the data controller uses trained neural networks to apply automated decision-making. In the case of neural networks, even an expert is often unable to understand how the neural network reached a decision. Various methods are currently being developed to understand how artificial intelligence has achieved a specific result. However, the data subject itself will most likely not be interested in receiving a technical description of the logic involved. He is regularly interested in which parameter needs to be changed in his specific case and how, so that the automated decision turns out differently. In accordance with a ruling of the Federal Court of Justice, the logic, i.e. the algorithm itself, does not have to be shown or explained to a data subject. The German data protection authorities emphasise that not only does the result have to be explained, but also the whole process and how the decision has been reached.

Data accuracy and forecasting decisions

Personal data shall be accurate and, where necessary, kept up to date. If AI is used to make predictions about how individuals are likely to behave, there can be a conflict with the principle of data accuracy. Artificial intelligence can be used, for example, to predict whether a natural person will be able to repay a credit. The results reflect a probability of whether or not a particular event will occur. This does not guarantee that the individual will actually cause a particular event. The predicted result can therefore be wrong. However, "accurate" means that the probability value must be calculated correctly according to the method used.

Data protection impact assessment

If AI is used to process personal data, it must be checked in advance whether a data protection impact assessment is necessary. Where the processing of personal data, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of a natural person, the data controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, in particular if new technologies are used. A data protection impact assessment shall also be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. If AI is used to process personal data, a data protection impact assessment must be conducted to manage interaction with the data subject or to evaluate personal aspects of the person concerned. The data controller must deal intensively with the risks of artificial intelligence and take appropriate remedial action.

Storage limitation and data minimisation

Artificial intelligence regularly requires a multitude of training data. If the training data is personal data, it must be deleted as soon as the purpose for which it was collected has been achieved. The processing of personal data by artificial intelligence must be reduced to the necessary extent. Self-learning artificial intelligence develops itself further when information that has been processed leads to new results. If these results are based on personal data, the question arises as to whether this violates the obligation to delete personal data with the

purpose of achieving it. Artificial intelligence can regularly no longer reverse adaptations without being deleted in its entirety. However, the algorithm is adjusted without directly storing personal data in the algorithm.

Antitrust/competition laws

Antitrust and competition law might be affected if companies use the same online platform to sell their products or services and the online platform is offering an AI-driven service that changes the prices of all participants to optimise the sales of their goods and services. This results in the same price for all products and services fulfilling the same needs of the customers. Under antitrust law, this constellation known as hub and spoke situation leads to an unlawful price-fixing agreement between the participants. In these cases, the companies do not communicate with each other but rather through a mediator, such as an online platform. According to the ECJ, the fact that the mediator can potentially coordinate the market behaviour and the companies' tacit acquiescence to that business model can constitute a violation of antitrust law. However, German antitrust law does not forbid collusive behaviour in general. It differentiates between explicit collusion, where the market participants directly communicate, and implicit collusion, where the actors coordinate their behaviour without direct communication. As long as the competitors only act in the same way, without any explicit agreements, this does not violate antitrust law. The line is crossed if the competitors through their parallel behaviour eliminate competitive conditions of the market. Yet, at this point, algorithms are not capable of autonomous pricing decisions and due to the complexity of the process this is not likely to change soon. Nevertheless, if and how implicit collusion through artificial intelligence should be regulated by antitrust law is already being discussed in Germany.

Similar questions arise trough the increasingly wide-spread use of blockchain technology. Unlike in hub and spoke situations, at least in the public blockchain, there is no central mediator. Still, coordination occurs on an abstract level. Therefore, the principles regarding platforms can be applied here as well: If companies participate in the blockchain they simultaneously agree to the coordination and sharing of information. This, too, might result in a breach of antitrust law. Finally, a general problem in addressing collusion through AI is that it might prove impossible to attribute its behaviour to a company that could be held accountable.

Board of directors/governance

Since the GDPR entered into force, data protection law is an area of law which media, authorities and the public pay special attention to. The use of personal data within an artificial intelligence or big data context should strictly comply with privacy laws in order to avoid negative publicity or fines. Compliance with data protection laws is also relevant for the board of directors as violations might lead to personal liability. Furthermore, the management has to take important business decisions with particular care. Otherwise, there is a risk that they will be personally liable for any damages incurred. Pursuant to Sect. 93 (1) German Stock Corporation Act the board of directors must "apply the diligence of a prudent and conscientious manager in the management of the company". However, the management is not liable if it acts in accordance with the Business Judgement Rule, Sect. 93 (1) German Stock Corporation Act. One requirement is that the management acts on the basis of appropriate information when taking a decision. To that end it is common practice to consult experts or consultants. However, the use of AI can also prove helpful, as AI can

conduct complex calculations and produce realistic forecasts. A legal obligation to use artificial intelligence for business decisions does not exist (yet).

Implementation of AI/machine learning/big data into businesses

"AI made in Germany" is to become an international brand, synonymous with modern, secure AI applications for the common good that are based on European values.[8] This sentence summarises the German Federal Government's Artificial Intelligence Strategy which it launched in November 2018. The strategy is not only focused on the promotion of Germany's economy, but also aims to create benefits for the people and the environment. The German Government recognises artificial intelligence as a key driver of productivity and as a generator for economic growth. Although Germany is already extremely well positioned in many areas of AI, the Federal Government aims to transfer the existing strengths to areas where no or little use has been made of the potential of artificial intelligence. The strategy focuses on three key areas: (1) investments in research by creating 100 additional professorships for AI to ensure that AI has a firm place within Germany's higher education system; (2) safeguarding a responsible development and use of artificial intelligence that serves the good of society and is based on a human-centred approach; and (3) integration of artificial intelligence in the ethical, legal and cultural sphere. One year later, the government's enthusiasm seems to have faded: Of the initially promised EUR 3 billion, only EUR 1 billion has been budgeted, which enticed criticism from experts and the business community. It is currently being discussed whether a ministry of digitalisation should be created within the ongoing legislative period. Chancellor Merkel reacted reluctantly; it remains to be seen if these plans actually become reality.

In Germany, currently no specific law regulates AI, big data or machine learning. The first regulations that touch on these matters – for example, Art. 22 of the GDPR – are discussed above. The German Copyright Act has been amended in 2018 to adapt it to the current needs of the knowledge society. It now contains a provision allowing text and data mining and the automated analysis of a large number of works for the purpose of scientific research.[9] It is permissible to reproduce the source material, including automatically and systematically, in order to create, particularly by means of normalisation, structuring and categorisation, a corpus which can be analysed. The corpus can be made available to a specifically limited circle of persons for their joint scientific research, as well as to individual third persons for the purpose of monitoring the quality of scientific research. Even if the source material is protected by copyright law, e.g. pictures or texts on the internet, they may be reproduced and handed over for scientific purposes. In addition to these changes, all relevant governmental authorities have issued statements and opinions for the use of artificial intelligence and big data within their relevant area. The authorities often use these statements to clarify ongoing legal issues and present their understanding of the law. Although this opinion is not legally binding, it can serve as a guideline on how to use artificial intelligence in compliance with the law.

In 2017, Germany passed a law allowing cars to drive highly or completely automated. Although the car is driving partly autonomously, the law requires the driver to stay receptive while handing over control to the car. According to this law, the car still needs a driver, i.e. a person closely monitoring the car and the traffic and who at all times is able to retake control. It is the driver (and the owner) who will be liable if the car crashes during the use of the automated functions. The functions may only be used "within the scope of their permitted use". For example, if the function is developed and tested for motorways, the driver shall

not be allowed to use it in city traffic. This act has already led to substantial discussions about how autonomous driving should be regulated in Germany: those in favour have argued that autonomous driving will make the roads safer and reduce the number of car crashes and persons injured or killed in traffic. Critics point out that it is irresponsible to allow drivers to use the functions because substantial questions relating to autonomous driving have not yet been solved.

In the end of 2018, the minister for traffic announced that legislation allowing fully autonomous driving, i.e. the car drives entirely without a driver, would be passed in 2019. This was mainly a result of pressure from the automotive industry that felt inhibited by the fact that legislation was lagging behind the advances in technology. So far, no such law has entered into force. Consequently, it continues to be unclear who should be liable if the artificial intelligence causes harm to another person. At the moment, the majority of commentators suggest that the manufacturer should be liable. Recently, however, the big car manufacturers have curbed the enthusiasm regarding autonomous driving and announced that it might well take another 10 years before a self-driving car might be ready for the road. Presumably the main reason being that the technology is currently too expensive for large-scale production. Nevertheless, the topic remains far up on the agenda.

* * *

Endnotes

1. BGH, Beschluss vom 27.3.1969 – X ZB 15/67, GRUR 1969, 672 – Rote Taube.
2. Sect. 1 (3) No. 3 German Patent Act (PatG).
3. Sect. 1 (4) German Patent Act (PatG).
4. Bundesgerichtshof, Urteil v. 13.05.1980, Az.: X ZB 19/78.
5. Sect. 69a German Copyright Act (UrhG).
6. § 69a (2) German Copyright Act (UrhG).
7. § 87a German Copyright Act (UrhG).
8. https://www.bundesregierung.de/breg-en/news/ai-a-brand-for-germany-1551432.
9. Sect. 60d German Copyright Act (UrhG).

Christian Kuß
Tel: +49 221 9937 25686 / Email: christian.kuss@luther-lawfirm.com
Christian Kuß studied law with a focus on IT law at the Westfälische Wilhelms-University Münster (Germany) from 2002 to 2007 and subsequently obtained his LL.M. in Bristol (England). He advises national and international clients on legal issues pertaining to IT, copyright and data protection law. He specialises in drafting and negotiating IT contracts, including licensing, IT outsourcing and IT project agreements as well as service level agreements. Another focus of his work is advising on data protection law, especially regarding whether future data information systems are allowed as well as examining and assessing internal data protection structures. Christian Kuß also advises national and international clients with regard to regulatory matters in the field of telecommunications.

Dr. Michael Rath
Tel: +49 221 9937 25795 / Email: michael.rath@luther-lawfirm.com
Dr. Michael Rath is a German lawyer, a certified specialist in information technology law and also a Certified ISO/IEC 27001 Lead Auditor. The focus of his advisory services is on IT law, data protection law and the protection of intellectual property. Dr. Michael Rath is, *inter alia*, a member of the German Association of Law and Informatics (DGRI) and an accredited conciliator for IT disputes brought before the DGRI conciliation office. He advises national and international companies on IT law, data protection, e-discovery, the award of IT contracts, IT outsourcing and the implementation of (IT) compliance requirements. He frequently holds seminars on these topics and publishes articles on current IT and data protection law issues.

Dr. Markus Sengpiel
Tel: +49 221 9937 25761 / Email: markus.sengpiel@luther-lawfirm.com
Dr. Markus Sengpiel is a German lawyer and has been managing Luther Rechtsanwaltsgesellschaft mbH together with Elisabeth Lepique as Managing Partner since 1 July 2014. He mainly advises clients from the IT, media and biotech sectors. He has worked together with other, partly external advisors in large transactions covering a variety of legal areas. Dr. Markus Sengpiel is the author of various publications on internet and consumer protection law. He regularly gives lectures on IT, outsourcing, media, copyright and competition law.

Luther Rechtsanwaltsgesellschaft mbH

Anna-Schneider-Steig 22, 50678 Cologne, Germany
Tel: +49 221 99370 / Fax: +49 221 99370 110 / URL: www.luther-lawfirm.com

Hong Kong

Alan Chiu, Charles To & Salina Ip
Ella Cheong & Alan Chiu Solicitors & Notaries

Trends

Hong Kong, being a Special Administrative Region of the People's Republic of China, operates under the common law system and is one of the most important financial hubs in Asia and globally. As early as 2007, the Hong Kong Government had started exploring how it could make use of technology and Artificial Intelligence ("AI") to transform Hong Kong into a "smart city".

The government has developed various initiatives and made investments to initiate growth in technology and science. For instance, building the Cyberport and the Hong Kong Science and Technology Park. The Cyberport has blossomed into an innovative digital community with over 1,000 companies contributing to key clusters of digital technology, namely Financial Technology ("FinTech"), eCommerce, big data and AI. In 2019, the Hong Kong Monetary Authority began to issue virtual banking licences as a key component of smart banking initiatives. Eight consortiums were granted a licence, including consortiums backed by tech companies like Alibaba and Tencent.

Another development is the ability of AI to provide automatic investment advice. The Securities & Futures Commission ("SFC") issued guidelines in April 2019 for platforms offering online investment services. These guidelines include ensuring security and reliability, maintaining proper records, and asking for compliance with all applicable laws and regulations when offering e-services (https://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-on-online-distribution-and-advisory-platforms/guidelines-on-online-distribution-and-advisory-platforms.pdf).

AI is being adopted in almost every industry. Besides finance and banking, the use of AI is spreading expansively in healthcare and education. AI assists in diagnosis, speeding up out-patients processes, reducing the contact between clinicians and patients, and between individual patients. AI is used in finding candidate drugs to combat infectious diseases. In education, students' concentration, behaviour and performance in class are being recorded and processed by AI, to provide teaching schedules tailored for each individual student's ability, interests and needs.

Despite all these promising developments and the growing use of AI, the speed of technology adoption in Hong Kong remains slow compared to Mainland China. The same is observed in the development of technology and AI-specific regulations. While there are existing data protection laws and banking-related regulations, as new technology emerges the respective enforcement agencies have only issued general guidelines and frameworks for compliance, without going into specific details.

Ownership/protection

Generally, when a company creates an AI algorithm, the algorithm is owned by the company unless otherwise specified in writing. In the development of an AI algorithm, a vast amount of data is used to train, improve and develop the AI algorithm. Such data often does not originate from the company and may contain third-party user data. Furthermore, as the AI algorithm develops and improves over time, the logic of the AI algorithm is often a "black box" and unknown even to the company.

Due to the transformative nature of AI, we set out below some of the issues AI creators, providers and users should consider.

Determination of intellectual property right ownership. This is particularly applicable to machine learning-based AI systems. AI algorithms developed by an AI may contain logics generated from training data belonging to AI users, which in turn are created by the AI itself. Therefore, ownership of IP rights arising from such AI may be complex and can only be properly determined by contracts. Copyright and patent are the key IP rights that may be involved in the Hong Kong context, whilst database rights may also be addressed in some overseas jurisdictions such as the European Union.

Transferability of training data and the training data-generated AI logics. Often, when a user uses an AI algorithm provided by a service provider, the user would have provided certain data to the service provider. The user should review the terms and conditions to ensure who owns the training data, and how the service provider can use the data, including whether the service provider can subsequently transfer such data to other third parties. Furthermore, when determining which AI service provider to use, a user should consider whether they will be able to transfer any data set to another third-party service provider. For example, if a user was using Google's AI service, could the user easily switch to Microsoft's AI service in the future?

Indemnities in relation to potential IP infringement related to AI. An AI system could infringe a third party's IP rights (especially copyright and patent) as part of its training process. However, unless specifically restricted by the computer code, a modern AI system would have the freedom to choose its data sources and generate its own innovations. Take, for example, an AI system which develops during training and its processes become a black box. How can such potential infringement by the AI be proved when the AI algorithm is unknown and how may the liability be extended when the infringement had no actual human intervention? Whilst patent infringement is akin to a strict liability tort and is hence applicable to AI, establishing infringement and determining liability of copyright infringement by an AI system (which requires proof of access to the work allegedly being copied) may be challenging and controversial.

Antitrust/competition laws

At present, antitrust or competition concerns are rarely discussed in the context of AI in Hong Kong. It is more a theoretical issue than a practical concern for now. In particular, Hong Kong's Competition Ordinance (Cap. 619) only came into effect on 14 December 2015, and hence it is still a relatively new topic in Hong Kong. There are only a handful of prosecution cases for violation of the Competition Ordinance. However, as more and more companies start to incorporate AI into their business model to determine pricing and market segment strategy without human intervention, the Competition Commission will sooner or later have to address the issue of whether such actions taken by AI algorithms will constitute breaches under the Hong Kong competition law regime. We anticipate that when such circumstances arise, case laws from the United Kingdom, Australia, the EU and other common law jurisdictions will be taken into account.

Board of directors/governance

The implementation of AI as part of the board of directors in Hong Kong is not something new. Back in 2014, an algorithm was appointed to the board of directors in a venture company based in Hong Kong. The algorithm does not possess all the rights its human directors have, but the algorithm was able to vote on whether the company makes an investment in a specific company or not. Even though, under the Hong Kong Companies Ordinance, an algorithm does not satisfy the qualities of a corporate director, it was a clear indication of the trend that AI could play in the governance of a corporation.

When a company considers incorporating AI into its board, the board must understand how data is obtained, managed and fed into the AI system to ensure it would be effective in assisting corporate decision-making and, most importantly, adhering to the fiduciary duties as a board director. Careful considerations must be taken in deciding the degree of delegation and power an AI can have. Any essential management functions should not solely rely upon an AI. AI should not be the only source upon which board members rely on in governing a business or making decisions. Moreover, the data being processed and stored in the AI must be securely protected in order to safeguard the company's interest. Ultimately, AI is there to augment decision-making and not to replace human beings. In any event, an AI is not a legally recognised director under Hong Kong laws; the human board of directors should only consider AI as a tool, and the human board of directors are still ultimately responsible for any decisions made.

Regulations/government intervention

Hong Kong currently has no AI-specific laws or regulations. Development of new technologies has largely relied on strict approval processes and compliance with general guidelines by the authorities. Nevertheless, we explore below the laws and regulations that are often or may be applicable when considering the use of AI.

AI makes use of a large amount of data, which often includes personal data (i.e. data which is capable of identifying a living individual). Hence, the Personal Data (Privacy) Ordinance (Cap. 486) which governs the collection, handling and usage of personal data is of great importance. This Ordinance was enacted in 1996 and has only been slightly updated since then. As such, this Ordinance is more principle-based and provides general guidelines rather than technology-specific rules. In particular, no AI-specific provision is provided. According to the General Data Protection Regulation of the European Union, a data subject shall have the right to opt not to be subject to a decision based solely on "automated processing", including "profiling", which produces legal effects or similarly significant effects concerning him or her, save for a few exemptions. From the Hong Kong perspective, there is no reason why the use of personal data in "automated decision-making" by AI shall not be bound by this Ordinance. For instance, data subjects should be notified of the purpose(s) of data collection, such as processing by "automated decision-making", before or during personal data collection. The Hong Kong Privacy Commissioner has also recommended that data users develop transparent privacy policies and practices when using big data analytics to assess individuals' personal data.

The Securities and Futures Ordinance (Cap. 571) was enacted to consolidate and modernise existing ordinances regulating the financial sector, where AI is increasingly being used. It highlights the roles of investment advisers and traders and any liability they may face.

The Hong Kong Bill of Rights Ordinance (Cap. 383) incorporates the International Covenant on Civil and Political Rights into the laws of Hong Kong. It is the foundation for protection

of human and constitutional rights of citizens. This Ordinance may play an important role in future debate and determination of what human rights AI may enjoy.

The Copyright Ordinance (Cap. 528) would impact how copyright generated by AI should be dealt with, including the ownership and use of such copyrights, as well as the applicability of moral rights (which are generally understood as "human rights"). The Copyright Ordinance does not expressly address whether a work generated by a computer may qualify for copyright protection. It is always questionable whether an algorithm exercises independent labour, judgment and skills in creating the work and whether a work generated by AI is original. However, it is clearly stated under the moral rights section of the Copyright Ordinance that the right to be identified as an author is not conferred to any computer-generated work. Case laws in the United States confirm that copyright only protects work that is founded in the creative powers of the mind and the Australian courts also declared that a work generated with the intervention of a computer could not be protected by copyright. Similarly, there is no answer to the question of whether the work generated by AI would infringe another's copyrighted work. It remains to be seen how the Hong Kong courts would stretch the current copyright law to apply to AI or whether there is a real need to amend the law to catch up with the technological advancement.

The Patent Ordinance (Cap. 514) was amended in 2016 and the new patent regime came into effect in December 2019. The newly enacted Ordinance introduces an original grant patent application where the Hong Kong Patents Registry begins conducting independent examination. The Patent Examination Guidelines issued by the Patents Registry sets forth that computer programs which provide technical contribution can be patentable. With the increasing acceptance of computer program-related inventions (including AI) as patentable subject matter in many jurisdictions, including China, the US and Europe, we believe the Hong Kong Patents Registry would take the stance that an AI-related invention can be patentable, provided that it offers technical contribution. This Ordinance would also impact patent ownership in AI-generated inventions spanning to patent infringement by AI, both of which are likely to come to the forefront of patent innovation and disputes as the number of AI inventions rise.

Lastly, the Electronic Transaction Ordinance (Cap. 553) was enacted to facilitate the use of electronic transactions for commercial and other purposes. The Ordinance expressly recognises the legal status of electronic records, electronic signatures and the service of documents by electronic mode. This Ordinance is of particular relevance when considering the potential applicability of smart contracts involving blockchain.

The use of AI is ever rising across every industry. However, the legal system in Hong Kong has not quite caught up with the pace AI is growing. There is a need to ensure that these intelligent machines can fit into the existing societal framework and that the deductive reasoning they perform is free of biases or discrimination.

Though enforcement agencies are quick to issue guidelines and frameworks, there are currently no plans to introduce any artificial intelligence-specific legislation, as this may not be a top priority for Hong Kong now.

Alan Chiu
Tel: +852 3752 3852 / Email: alan.chiu@ellalan.com

Recognised by *Asian Legal Business* (2015) as one of the top lawyers under the age of 40 in Asia, Alan has received close to 30 awards as a leading lawyer in Hong Kong and China.

Alan focuses on both contentious and advisory IP matters and also covers data privacy, advertising law, competition law, entertainment law, e-commerce, digital forensic, internet security, mediation and arbitration.

With an IT forensic background, Alan advises extensively on artificial intelligence, blockchain, crypto-currency, and cybersecurity matters. He also has extensive experience in handling digital forensic issues in civil and criminal proceedings concerning counterfeiting, software copycats and instant message authenticity. He is an Adjunct Professor of Law at the Hong Kong Shue Yan University and currently a member of the InnoTech Committee of the Law Society of Hong Kong and the INTA Internet Committee.

Charles To
Tel: +852 3752 3852 / Email: charles.to@ellalan.com

Charles has a diversified practice covering commercial, corporate, entertainment, licensing, intellectual property, advertising, data privacy, e-commerce, employment, and general commercial matters in the TMT industry.

Charles served as Senior Legal Counsel for Tencent and Fox Networks where he advised the businesses' international commercialisation of their services, covering music, video OTT, mobile games, advertising, social media, and cloud technology. He was recognised as a five-star employee by Tencent, a highly distinguished recognition.

He is experienced in handling corporate matters for Fortune 500 companies and technology start-ups as well as clients in the media, life sciences, telecommunications and retail sectors.

He is a committee member of the InnoTech and the Employment Law Committee and is deputy leader of IP Vetting Group for "Sing Tao Legal Mailbox" of the Law Society of Hong Kong.

Salina Ip
Tel: +852 3752 3852 / Email: salina.ip@ellalan.com

Salina has extensive knowledge in worldwide patent practice through drafting original patent specifications, prosecuting patent applications, providing patentability searches and opinions, filing strategy and portfolio management for leading multinational companies and institutions. She is also experienced in helping individual clients, start-ups, government bodies and tertiary institutions in building up and managing their global IP portfolios.

She has worked with a wide range of technologies spanning pharmaceutical, microbiology, biotechnology, nanotechnology, mechanical as well as AI-related technologies.

At ELLALAN she also focuses on handling patent licensing, technology transfer, patent invalidation and infringement analysis, and assisting listed companies and conglomerates in patent litigation and invalidation proceedings in Hong Kong and Mainland China.

Ella Cheong & Alan Chiu Solicitors & Notaries

26/F The Hennessy, 256 Hennessy Road, Wan Chai, Hong Kong
Tel: +852 3752 3852 / URL: www.ellalan.com

India

Divjyot Singh, Kunal Lohani & Kumari Poorva
Alaya Legal Advocates

Introduction

Computing devices are able to mimic human behaviour, to an extent, through 'artificial intelligence'. 'Artificial intelligence' is the decision-making ability of a machine, which often involves the processing of large amounts of data, literally 'big data', by the use of algorithms. This 'big data' can be used to develop 'intuitive learning' or 'thinking' in a machine i.e., 'machine learning'. Evidently, the relationship between 'artificial intelligence' (AI), 'machine learning' (ML) and 'big data' (BD) is inescapable.

India has a natural advantage in this field, coupled with an obvious requirement given the population – India has readily collectible large and diverse data, and also the technical ability to utilise such data. Fast-paced advancements in technology, excessive consumerism, and technological agility have contributed to the dynamic situation that we have today. In this chapter the authors have analysed the current trends in India relating to 'artificial intelligence', 'machine learning' and 'big data', and have examined attendant legal aspects with respect to ownership, antitrust, data protection, governance and regulatory matters.

1. Trends

1.1. Artificial Intelligence, Machine Learning and Big Data trends in India

Why was involvement in AI made necessary?

AI is predicted to contribute $15.7 trillion to the global economy in 2030.[1] We stand on the brink of a technological revolution led by AI which will fundamentally alter the way we live, work and relate to one another.[2] AI has affected our lives more than we realise. From waking up to Siri's news updates to falling asleep to a movie suggested by Netflix's recommendation engine, the technology underlying the Fourth Industrial Revolution has penetrated our daily lives.[3]

Since other countries are making rapid progress in the field of AI, and globalisation being inevitable, it is imperative that India begins to see AI as a critical element of national security strategy, focuses on AI-based innovation and establishes AI-ready infrastructure to prepare India's jobs and skills market for an AI-based future to secure its strategic interests.[4]

AI, ML and Big Data Trends

In the absence of any official big data repository and disclosure requirements regarding the manner of use of big data, it is difficult, at this juncture, to make an accurate assessment of any trend in India in this regard. However, analysing the flow of investments in the public and private sector, the following trends may be deduced:

I. Government thrust towards innovation and development of AI

The framework for regulating AI and its applications is in its embryonic stages and there is much to traverse. It is evident from the following that the Government is working towards creating an AI-friendly technological ecosystem in India:

a. In 2017, The Ministry of Commerce and Industry set up an AI Taskforce which highlighted various sectors of importance[5] for the AI regime and the challenges in adopting AI in India.

b. In 2018, NITI Aayog,[6] was directed to initiate programmes on AI and its applications. The Ministry of Electronics & Information Technology ('MeitY') constituted four committees to develop a policy framework and analyse issues like leveraging AI, key policy enablers required across various sectors, and legal and ethical issues to AI.[7]

c. In January 2020, NITI Aayog recommended that an AI-explicit computer framework 'AIRAWAT'[8] be set up to satisfy the processing needs of innovation hubs, start-ups, AI researchers and students.[9]

II. Pioneering efforts of the private entities in the AI sector

Private initiatives in India have been far ahead in the development and use of AI than the Government. From utilising various applications powered by AI to providing various online services like MakeMyTrip, Firstcry and Flipkart, which learn from consumers' online behaviour for making intelligent goods and services suggestions, corporates have been engaging in the use of AI for a long time. Big conglomerates are infusing AI to automate day-to-day operations. The insistence on automation of daily tasks is further necessitated by the fast growth of business.

Indulgence of the private entities in AI is evident from the investments being made by them, specifically in the areas of e-commerce, anomaly detection, banking and finance, and retail. Flipkart uses AI-powered robots at sortation centres to process 4,500 shipments an hour with twice the speed and 99.99% accuracy. Swiggy uses AI-powered chatbots for customer support and an AI-ML model for search result optimisation.[10]

In India, many large corporations like Google and Walmart Labs are acquiring small start-ups for their AI innovations. Investments by private entities in AI-specific start-ups and the facilitation of an AI-friendly ecosystem by Government initiatives has resulted in blossoming of AI start-ups. In 2019, Indian AI start-ups received a global investment of $762.5 million dollars.[11]

It is noteworthy that the developments pursued by the Government in AI are primarily in collaboration with private entities. For instance, NITI Aayog's collaboration with IBM for developing precision agriculture using AI for doubling farmers' income by 2020, by using a machine learning process along with different computer algorithms for crop classification and area estimation.[12] Additionally, the Government of Andhra Pradesh collected information from a range of databases, and processed the information through Microsoft's Machine Learning Platform to monitor children and devote student-focussed attention on identifying and curbing school drop-outs.[13]

1.2. Applications of AI

Integration of AI in our lives is affected by several factors including the digital divide, inequitable internet access, local economy, geographical location, and not to forget the 'culture' and 'adaptability' quotient.

Private and public sectors have perceived the abundant applications in AI, ML and BD and have begun their endeavours to exploit them. Permutations and combinations of different types of machine learnings[14] are used to suit the purpose of the programme.

I. Healthcare Sector of India

a. In 2018, India ranked 145th in terms of healthcare access and quality rating.[15] India also has a high rate of health issues, particularly diabetes; with 19% of the patients[16] in the world being of Indian nationality. One of the consequences of diabetes is diabetic retinopathy which, if left untreated, can lead to blindness. *Microsoft* and *Forus Health* are working with *NITI Aayog* on a device called *3Nethra* for early detection of diabetic retinopathy using AI-based retinal imaging API's, which delivers the cloud intelligence so that it is closer to the eye. The system automatically grades the images and identifies if the patient has diabetic retinopathy.[17] It is a blessing for a country like India, where there are only 20,000 ophthalmologists for 1.3 billion people.[18]

b. An Indian healthcare start-up called NIRAMAI has developed a device to detect breast cancer in women at a much earlier stage than traditional methods using ML. It checks the thermal images against the positive and negative reports using Big Data analytics, AI and ML.

II. E-Commerce Sector

a. It is expected that the Indian e-commerce market will grow to US$200 billion by 2026, which may be attributed to increasing internet and smartphone penetration.[19] Using AI and machine learning algorithms, the online shopping experience has been personalised for every customer. They predict buyer behaviour based on past searches and orders and recommend products that would be most interesting to the customer.

b. AI and ML are used by e-commerce entities to stock warehouses in accordance with preferences in a geographical area. Machine learning algorithms are used to predict future demand for the products and accordingly fill the shelves.

III. Defence Sector

a. Apart from the huge success of AI in the automation of activities in the commercial sector, AI is being developed and infused in the defence and national security sector of India. The need for such implementation is aggravated by the fusion of AI into defence activities by other nations across the globe.

b. The reported developments of India involved in AI in the defence sector include:

i. Development of more than 200 DAKSH Robots, a Remotely Operated Vehicle (ROV) which is used to defuse explosives by the Indian Army.

ii. Development of RoboSen, which is a mobile robot created for the purposes of patrolling, reconnaissance and surveillance, by the Indian Army. RoboSen is capable of autonomous navigation in a rough terrain with the ability to circumvent obstacles and provide continuous video feedback.[20]

iii. Development of NETRA – Network Traffic Analysis by Centre for Artificial Intelligence Research (CAIR) to monitor traffic on the internet. NETRA is capable of analysing voice traffic going through video conferencing applications and can intercept messages with specific keywords for reconnaissance and intelligence collection purposes.

1.3. Key Legal Issues

'*With great power comes greater responsibility*' – a proverb which became popular during the French Revolution, essentially responsible for bringing an accountable and law-abiding form of Government, has never been more befitting than in the current AI revolution. 'Accountability' is essential to the continuous development of AI and its application. It

follows that it is hardly possible to think about the applications of AI without any legal implications.

a. Ownership/Protection

i. Are AI applications to be categorised under copyright law and/or under patent law?

ii. Is AI a mere 'tool' and therefore the owner of the 'tool' should be identified with the intellectual property generated by such 'tool', or is the AI application itself the creator of the intellectual property in question and therefore should be recognised as its owner?

iii. Should BD generically or at least in respect of certain areas be regarded as 'critical infrastructure' and if 'yes', is there a need to regulate access and use of the same?

b Antitrust/Competition Laws

i. Whether or not access and use of Big Data has ascribed such an advantage to certain enterprises which causes or is likely to cause an 'appreciable adverse effect' on competition in the market?

ii. Whether or not non-price competitive factors should be a consideration for approval of proposed combinations?

iii. Whether or not collusion through AI applications are anti-competitive under competition law?

c. Board of Directors/Governance

i. What is the impact of AI in the decision-making process at Board level?

ii. What is the role of AI in corporate governance?

2. Ownership/Protection

2.1. With the rapid advancement in the field of AI and its applications that cover almost every aspect of our lives, the creators of AI have become aware of the need to have ownership of AI applications and to protect the rights attached with such AI applications. The AI applications may be categorised into and protected under the following categories:

2.1.1. The Copyright Act, 1957 ('Copyright Act') – Under Section 2(o) of the Copyright Act, both the 'source code' and the 'object code' of AI applications are protected as 'literary works'. The author of the AI applications, i.e. the developer, is considered to be the owner of such AI application, except in the event when the author generates or creates an AI application in the capacity of an employee during the course of employment. The Copyright Act also permits fair use and reverse engineering.

2.1.2. The Patents Act, 1970 ('Patents Act') – Under Section 3(k) of the Patents Act, computer programs are not patentable *per se*. An AI application may be patented if it is attached to an invention along with hardware and it is proved that hardware is an essential component of such invention along with the software. For instance, Google LLC filed patent application no. 3023/KOLP/2014 titled 'Location History Filtering' and was subsequently granted a patent after the examiner raised objections under Section 3(k) of the Patents Act. In response to the objection, the applicant proved that the claims were not related to computer programs but a computing device, which enhance its technical effect.

2.1.3. Trade Secrets – In India, the design, idea and structure of an AI application may be protected as a 'trade secret' based on its nature and distribution through contracts or under law of torts.

2.1.4. Licence Agreements – Access to AI applications can be granted by way of licence agreements by the owners of such AI applications. Such licence agreements are broadly divided into two categories: exclusive licences; and non-exclusive licences. The Copyright

Act recognises the concept of 'exclusive licence'.[21] Under the Copyright Act, an exclusive licensee enjoys the rights comprised in the copyright of a work which is akin to that of the owner and includes the right to prosecute, defend and enforce the intellectual property rights.

2.2. Ownership of intellectual property created by AI applications – Under the Copyright Act, copyright subsists in the author only if the author '*is a natural person, a human being, and not an artificial person*'[22] and that for the purposes of registration of a copyright, details of only a natural person may be provided as the author of a work. The 'tool' used for generating intellectual property is considered only as a machine (i.e. artificial person) and thus is not considered as the 'owner' of such intellectual property.

The use of AI applications has increased with the advancement of machine learning and AI applications are used for generating intellectual property based on 'intelligence'. This gives rise to the debate that the intellectual property rights in AI-generated work should be assigned to the 'AI applications'. The gap between the existing laws and the advancement in AI may act as a hindrance in the generation of new work. Thus, there arises a need for a review of the existing laws to keep up with the advancement in the field of AI and its uses.

2.3. Categorisation and Ownership of BD

2.3.1. BD is used by the AI applications to discern a pattern from chaos using ML. It can be classified into two categories:

a. Personal Data – Governed and protected under 'Right to Life', a fundamental right granted under the Constitution of India, and provisions of the Information Technology Act, 2000 ('Information Technology Act').
b. Data other than personal data – presently not governed by any specific legislation.

2.3.2. India presently does not have any specific legislation governing data protection or privacy. However, in *Justice K.S. Puttaswamy and Ors. v. Union of India* (UOI) and *Ors*.,[23] the Supreme Court of India, read the 'right to privacy' into the other existing fundamental rights.

The data of natural persons (i.e. personal data) is protected under the right to privacy and the individual is the owner of such data. Such data when anonymised, ceases to be 'personal data' and is available for analysis as far as creativity allows. Compilation of the anonymised data and interpretation thereof may be protected under the copyright law.

2.4. Recognising the advances being made in the field of AI, it is imperative to have a data repository where anonymised personal data and other relevant data can be stored, pooled together, and made accessible based on identified parameters. It would seem that BD merits the status of 'critical infrastructure', allowing others to build upon the existing data, in a healthy competitive environment.

NITI Aayog is in the process of launching a programme to develop a national repository of annotated and curated pathology images.[24] The policy also talks about having a decentralised data marketplace that is based on blockchain technology which will attract data providers and model builders to build AI applications.

3. Antitrust/Competition Laws

3.1. The Competition Act, 2002 ('Competition Act') seeks to prevent any adverse effect on competition, promote and sustain competition in markets, protect the interests of consumers, and ensure freedom of trade carried on by other participants in markets, in India.[25] The Competition Act amongst other things, prohibits:

a. abuse of dominant position;

b. anti-competitive combinations; and
c. anti-competitive agreements.

3.2. The advent of AI and the increasing use of big data has evidently accorded a dominant position to certain enterprises by allowing them to analyse and predict customer behaviour patterns and also develop cost efficiencies.

From a competition law perspective, an enterprise is said to have a dominant position in the relevant market[26] if it enjoys '*a position of strength which enables it to: (i) operate independently of competitive forces prevailing in the relevant market; or (ii) affect its competitors or consumers or the relevant market in its favour*'.[27] While enjoying such a position is not prohibited in itself, certain enterprises have been alleged to breach the Competition Act and abused their position[28] in the market.

As an example, the Competition Commission of India (CCI)[29] has noted that Amazon and Flipkart have '*large repositories of data due to its unparalleled market base and market power*' and they analyse the data to '*target advertisements based on consumer preferences and marginalise other competitors which are unable to capture the market due to lack of access to data*'. Lack of such access and cost associated with the development of complex self-learning computing algorithms has resulted in creation of high entry barriers on account of network effects.

Although e-commerce entities essentially follow a marketplace model of e-commerce, i.e. acting as an online intermediary between sellers and consumers, they have now introduced private labels which are claimed to be given preferential treatment. It has also been alleged that the e-commerce entities use the data collected from the sale of products of third-party sellers on its marketplace to set optimal prices and specification(s) for their private label products.

The CCI, by its order dated 20th January 2020 in *Delhi Vyapar Mahasangh v. Flipkart Internet Private Limited and Amazon Seller Services Private Limited*,[30] has initiated an investigation focused on deep discounting, preferential listing and market power, but it still remains to be seen how the CCI plans to combat such behaviour.

3.3. CCI has further been empowered to regulate mergers, acquisitions and amalgamations over a monetary threshold and prohibits any '*combination which causes or is likely to cause an appreciable adverse effect on competition within the relevant market in India*'.[31]

Although the quantum of data which could fall under the control of a single entity has not been a factor of consideration by CCI while approving a proposed combination, such non-price factors may result in repudiation of a proposed combination, keeping in mind '*the extent of barriers to entry*'[32] it might create, and the a '*likelihood that the combination would result in removal of a vigorous and effective competitor or competitors in the market*'[33] among other factors.

3.4. Competing enterprises have sometimes resorted to coordinate their production and pricing activities to mimic a monopoly, for increasing their collective and individual profits by restricting market output and raising the market price. In response to such explicit or tacit collusion, the Competition Act prohibits anti-competitive agreements.[34] Anti-competitive agreements include any agreement that '*directly or indirectly determines purchase or sale prices*[35] *or directly or indirectly results in bid rigging or collusive bidding*'.[36]

The law as it stands does not provide for the use of AI applications as a means of collusion among competitors, but it is plausible that such arrangements may be deemed to be anti-competitive. For instance, if two or more enterprises, instead of agreeing on an explicit price, agree to implement a joint pricing algorithm that coordinates prices on their behalf.

3.5. The legal framework related to competition law will need to evolve so that AI is not available as a shield for enterprises to engage in activities which are otherwise prohibited.

For example, the use of AI-based pricing software by competing enterprises resulting in collusion among themselves by determining similar prices for their goods or services.

4. Board of Directors/Governance

4.1. Introduction

The Board of Directors (Board) is responsible for the management of the affairs of the company, and implementation of corporate governance. We are not delving into the merits of the statement, given that powers of the directors may be curtailed in accordance with Companies Legislation.[37] For the present purposes it is brought to focus that the Companies Legislation and other statutes[38] enjoin certain duties on the directors.[39]

A director should, amongst other things:

a. Act in good faith in order to promote the objects of the company for the benefit of its members as a whole, and in the best interests of the company, its employees, the shareholders, the community and for the protection of the environment.
b. Exercise duties with due and reasonable care, skill and diligence and shall exercise independent judgment.
c. Not involve himself in a situation in which he may have a direct or indirect interest that conflicts, or possibly may conflict, with the interest of the company.
d. Not achieve or attempt to achieve any undue gain or advantage either to himself or to his relatives, partners, or associates and if such director is found guilty of making any undue gain, he shall be liable to pay an amount equal to that gain to the company.
e. Not assign his office.

The focus of the Board in the course of discharging its responsibilities is to engage in developing a corporate strategy which essentially endeavours to upgrade technology to gain a competitive advantage, increase production and reduce the cost of labour. In a nutshell, more often than not, the aim of this is to maximise the profits of the company. The involvement of AI in respect of governance is not hard to imagine.

4.2. The Role of AI at Board level

Involvement of AI in corporate governance may be viewed at two levels. First, utilisation of AI by the Board for its decision making, and secondly, utilisation of machine learning for substituting one or more directors or perhaps even the entire Board.

A director is enjoined with the duty of exercising independent judgment, acting in good faith, not involving themselves in conflict of interest situations, and not assigning its office. It would follow that AI may be used at Board level by the directors, as long as the 'duties' are faithfully discharged. Substitution of directors by AI is presently not envisaged under the Companies Legislation. The existing Companies Legislation clearly stipulates that only 'individuals' shall be elected as directors.[40]

In other jurisdictions, AI has been used by companies to conduct day-to-day business. A Hong Kong-based venture capital firm used VITAL, which is a machine learning program capable of making investment recommendations in the Biotechnology sector to the Board.[41] VITAL has been made an observer in the Board and corroboration by VITAL in all investment decisions was made mandatory.[42] Similarly, a California-based software company runs all its corporate decisions through an AI tool, which further gives its recommendations.[43]

Thus, under the present legal framework in India, the Board may use AI application assessments to make an informed decision while discharging its duties. Accordingly, it

needs to be ensured that algorithms in question answer the requirements of law. AI tools can give the company a competitive advantage and can be used to complete tasks involving due diligence and other administrative work for the Board but it cannot undertake the decisions of a director on the Board.[44]

4.3. Governance Issues and Liability of the Board

The Board is empowered to take all decisions in respect of the company, except to the extent curtailed by provisions of the Companies Legislation and by the constituent documents. AI may be used to analyse customer demographics, analyse internal communication of employees to filter company data from leakage, reviewing online news to point out competitors of the company, track capital allocation, etc.[45]

However, the Board must be equipped to deal with the surmounting challenges presented by the use of AI, be ready to address the various issues, including legal concerns, take appropriate measures in handling the implementation of AI and the arising governance issues. Such issues include, data privacy, cyber security, biased programming in AI, lack of transparency on functioning of the AI.

In the course of exercise of powers by the directors, the duties cast on the directors as discussed above, must be fulfilled. Certain protocols should be developed and followed to ensure that the legal requirements are not directly or indirectly compromised in the guise of using AI. Before the official launch of any AI application, the Board should undertake alpha and beta testing to reduce product failure risk.

Failure on part of the Board to address the implications arising out of the use of AI may result in penal liability.[46] In the evolving regulatory expectations, lapse in governance can have serious implications involving reputational damage, fall in stock price, and legal actions. Further, where personal data is involved, directors can be made liable for the failure to provide safety measures for data protection under the Information Technology Act.[47] Further, intermediaries such as mutual funds or asset management companies have to frame additional policies or report cyber-attacks as well as include measures that they have taken to counter and mitigate such risks.[48]

4.4. Solutions for the Board for Risk Management

Risk management measures at the Board level include:

a. Establishing protocols and having in place an independent mechanism to ensure that the protocols are adhered to in the use of AI. The protocols should serve to ensure amongst other things, compliance with applicable law.
b. Have in place a review mechanism to ensure that the protocols are evaluated on a periodic basis.
c. A separate mechanism in respect of processing of data.

5. Regulations/Government Intervention

5.1. The rapid advancements and extensive applications of AI and ML have triggered profound interest making them issues of national relevance. There is an urgent need for the Government to consider the development, funding and widespread implications of AI. Currently, there are no specific laws in India that relate to AI, BD or ML.

The Government's intent at this stage seems to be in the promotion of AI and its application. Its strategy is to '*maximize the 'late mover's advantage''* in the AI sector for '*consistently delivering home-grown pioneering technology solutions in AI as per its unique needs to help leap-frogging and catch-up with the rest of the world*'.[49]

The Government is speeding up the process for formulation of laws, guidelines and policies, specifically governing and regulating AI, BD and ML.

5.1.1. NITI Aayog Report. The Report suggests:

a. Building an attractive IP regime for AI innovation and recommends setting up a task force, comprising jointly of The Ministry of Corporate Affairs and Department of Industrial Policy and Promotion (DIPP), to examine and issue appropriate modifications to the intellectual property laws.
b. Instituting a data privacy legal network to protect human rights and privacy and creation of sectoral regulatory guidelines covering privacy, security and ethics.

5.1.2. MeitY constituted four committees[50] for developing a policy framework on AI. The recommendations made by the said committees include:

a. Development of an Open National Artificial Intelligence Resource Platform (NAIRP) to become the central hub for knowledge integration and dissemination in AI and ML.
b. Stakeholders need to deliberate on whether AI systems should be recognised as a legal person and establishment of an insurance scheme or compensation fund to compensate for damages in the event of a civil liability claim.
c. Sharing of best practices – use of procurement contracts by the Government to emphasise on the best practices around security, privacy and other issues.
d. A committee of the stakeholders to be constituted to look into the aspects in a holistic manner. Review of the existing laws to understand the modifications required for adoption of AI applications.
e. AI framework should define broad principles and the organisations should be allowed to design their internal programs in compliance with the set principles with flexibility to adapt to the developing technology.
f. Standards are to be set to address the AI development cycle. The Bureau of Indian Standards (BIS) has set up a new committee for standardisation in AI.
g. The Government has proposed the development of rigorous safety parameters and setting up of safety thresholds so that AI applications are designed '*in such a way that it does not harm the people and property during its interaction*'.[51]

5.1.3. In the AIRAWAT approach paper, NITI Aayog proposed:

a. Setting up a specialised AI-computing infrastructure which will power the computing needs of Centres of Research Excellence, International Centres Transformational AI and Innovation Hubs, start-ups, researchers, students, government organisations, etc.[52]
b. Setting up of an inter-ministerial task force with cross-sectoral representation to spearhead the implementation of AIRAWAT.
c. The task force will seek funding for the implementation of AIRAWAT.

5.2. One of the committee reports[53] has deliberated whether AI poses a threat to humanity. It was opined that in the current state, AI applications are intelligent machines for specific tasks only. It stated that '*even if a machine with higher intelligence is developed, there is no reason to believe that it would be interested in dominating the world due to lack of intent*'.[54] If machines with higher intelligence are developed, the ways to control would also be developed in parallel.

6. Propositions

6.1. As is evident from the foregoing, there is an urgent need to develop a legal regime specific to AI, ML and BD. The following suggestions are made on the basis that the role of AI is set to become even more profound at all levels:

a. Develop a data repository where anonymised personal data and other relevant data can be stored, pooled together, and made accessible based on identified parameters.
b. Review of existing laws. Existing laws need to be reviewed to keep up with the advancement in the field of AI and its diverse applications.
c. Enactment of special legislations related to AI, ML and BD.
    i. The AI legislative framework should define broad parameters for the various stakeholders which include developers and users, and should have enough room to evolve based on stakeholder requirements. Such legislative framework should be enabling in character and allow innovation. Each stakeholder group should be required to design their internal programmes and protocols in view of the legislative framework.
    ii. With a view to encourage innovation, the regulatory regime should have in place a mechanism to distinguish between error of judgment (where the person is innocent) and error of intent (where there is an element of *mens rea*).

6.2. Considering that the advancements in AI are at a global level, India must seek to enhance its participation in various AI projects in co-ordination with international bodies. A good example is the World Health Organization working closely with The Ministry of Health and Family Welfare, Government of India to provide technical support for AI initiatives pursuant to the Government's commitment to end tuberculosis by 2025.

* * *

Endnotes

1. PwC, "Sizing the prize: What's the real value of AI for your business and how can you capitalise?" 3 (2017). (Available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.)
2. Klaus Schwab, "The Fourth Industrial Revolution: What It Means and How To Respond", Foreign Affairs, December 12, 2015. (Available at: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.)
3. Brinda Sapra, "AI for All: How India Can Become an Artificial Intelligence Superpower" Next Billion, November 1, 2019. (Available at: https://nextbillion.net/india-artificial-intelligence-superpower/.)
4. Shashi Shekhar Vempati, "India and the Artificial Intelligence Revolution", Carnegie India, August 11, 2016. (Available at: https://carnegieindia.org/2016/08/11/india-and-artificial-intelligence-revolution-pub-64299.)
5. Manufacturing, Fin-Tech, Healthcare, Agriculture, Education, Retail, Aid for Differently Abled Persons, Environment, National Security and Public Utility Services.
6. NITI Aayog (National Institution for Transforming India) is the premier policy 'Think Tank' of the Government of India, providing both directional and policy inputs. While designing strategic and long-term policies and programmes for the Government of India, NITI Aayog also provides relevant technical advice to the Centre and States. (Available at: https://niti.gov.in/.)
7. Ministry of Electronics and Information Technology, "Committee A on platforms and data on Artificial Intelligence", "Committee B on leveraging A.I for identifying national missions in key sectors", "Committee C on mapping technological capabilities, key policy enablers required across sectors, skilling, reskill", "Committee D on cyber security, safety, legal and ethical issues" (2018).
8. AI Research, Analytics and Knowledge Assimilation.

9. NITI Aayog, "AIRAWAT-ESTABLISHING AN AI SPECIFIC CLOUD COMPUTING INFRASTRUCTURE FOR INDIA" (January, 2020) (Available at: https://niti.gov.in/sites/default/files/2020-01/AIRAWAT_Approach_Paper.pdf).
10. Rahul Sachitanand, "Here's why Indian Companies are betting big on AI", *Economic Times,* available at*:* https://economictimes.indiatimes.com/tech/internet/heres-why-indian-companies-are-betting-big-on-ai/articleshow/67919349.cms?from=mdr.
11. AIM Research, "Report: Indian AI Startup Funding in 2019", January 27, 2020.
12. Press Information Bureau, Government of India, "NITI Aayog to Collaborate with IBM to develop Precision Agriculture using Artificial Intelligence", (May 4, 2018).
13. Arindrajit Basu, "We need a better AI vision", The Centre for Internet Society, October 12, 2019 (Available at*:* https://cis-india.org/internet-governance/blog/fountain-ink-october-12-2019-arindrajit-basu-we-need-a-better-ai-vision).
14. Sumit Das, Aritra Dey, Akah Pal, Nabamita Roy, "Applications of Artificial Intelligence in Machine Learning: Review and Prospect", 115-No.9 *International Journal of Computer Applications* 31–32 (2015).
15. Press Trust of India, "India ranks 145 of 195 countries in healthcare access and quality, far below China", *Hindustan Times,* May 23, 2018, available at: https://www.hindustantimes.com/health/india-ranks-145th-below-china-bangladesh-among-195-countries-in-healthcare-access-quality/story-31UgnP7QxpvqbeHJoLdtFP.html.
16. Microsoft News Center India, "Forus Health democratizes eye care with an 'Intelligent Edge' in its retinal imaging devices", April 6, 2018. (Available at: https://news.microsoft.com/en-in/features/forus-health-3nethra-ai-azure-iot-intelligent-edge-eyecare/.)
17. *Ibid.*
18. *Ibid.*
19. Microsoft News Center India, "Forus Health democratizes eye care with an 'Intelligent Edge' in its retinal imaging devices", April 6, 2018. (Available at: https://news.microsoft.com/en-in/features/forus-health-3nethra-ai-azure-iot-intelligent-edge-eyecare/.)
20. Maj Gen P.K. Chakravorty, "Artificial Intelligence and Its Impact on the Indian Armed Forces", Indian Defence Review, May 5, 2017. (Available at: http://www.indiandefencereview.com/news/artificial-intelligence-and-its-impact-on-the-indian-armed-forces/.)
21. The Copyright Act, 1957 (14 of 1957), s. 2(j).
22. *Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd* (1996(38) DRJ 81).
23. AIR 2017 SC 4161.
24. NITI Aayog, "National Strategy for Artificial Intelligence" (2018).
25. The Competition Act, 2002 (Act No. 12 of 2003), Preamble.
26. 'Relevant Market' means 'the market which may be determined by the CCI with reference to the relevant product or geographic market or with reference to both'; as per The Competition Act, 2002 (Act No. 12 of 2003), s. 2(r).
27. The Competition Act, 2002 (Act No. 12 of 2003), s. 4 (Explanation (a)).
28. The Competition Act, 2002 (Act No. 12 of 2003), s. 4(1).
29. Case No. 40 of 2019, Order dated January 13, 2020.
30. *Ibid.*
31. The Competition Act, 2002 (Act No. 12 of 2003), s. 6(1).
32. The Competition Act, 2002 (Act No. 12 of 2003), s. 20(4)(b).
33. The Competition Act, 2002 (Act No. 12 of 2003), s. 20(4)(i).
34. The Competition Act, 2002 (Act No. 12 of 2003), s. 3(1), stipulates '*No enterprise or association of enterprises or person or association of persons shall enter into any*

agreement in respect of production, supply, distribution, storage, acquisition or control of goods or provision of services, which causes or is likely to cause an appreciable adverse effect on competition within India'.

35. The Competition Act, 2002 (Act No. 12 of 2003), s. 3(3)(a).
36. The Competition Act, 2002 (Act No. 12 of 2003), s. 3(3)(d).
37. The Companies Act, 2013 (Act 18 of 2013).
38. Indian Trust Act, 1882 (Act 2 of 1882).
39. The Companies Act, 2013 (Act 18 of 2013), s. 166.
40. The Companies Act, 2013 (Act 18 of 2013), s. 149.
41. Nicky Burridge, "Artificial intelligence gets a seat in the boardroom", Nikkei Asian Review, May 10, 2017. (Available at: https://asia.nikkei.com/Business/Artificial-intelligence-gets-a-seat-in-the-boardroom.)
42. *Ibid.*
43. Martin Petrin, "Corporate Management in the age of AI" 3 UCL Working paper series (2019).
44. *Supra* note 44.
45. Erman Akdogan, "Blockchain as the Board, AI as the Director — Corporate Governance 2.0", *The Startup*, November 22, 2019. (Available at: https://medium.com/swlh/blockchain-as-the-board-ai-as-the-director-corporate-governance-2-0-a07401350358.)
46. The Companies Act, 2013 (Act 18 of 2013), s. 166 (7).
47. The Information technology Act, 2000 (Act 21 of 2000), s. 85.
48. SEBI Circular No. SEBI/HO/IMD/MIRSD/CIR/P/2019/12 and SEBI/HO/IMD/MIRSD/CIR/P/2018/147.
49. NITI Aayog, "National Strategy for Artificial Intelligence" (2018).
50. Ministry of Electronics and Information Technology, "Committee A on platforms and data on Artificial Intelligence", "Committee B on leveraging A.I. for identifying national missions in key sectors", "Committee C on mapping technological capabilities, key policy enablers required across sectors, skilling, reskill", and "Committee D on cyber security, safety, legal and ethical issues" (2018).
51. Ministry of Electronics and Information Technology, "Committee D on cyber security, safety, legal and ethical issues" (2018).
52. NITI Aayog, "AIRAWAT: Establishing an AI specific cloud computing infrastructure for India, An approach Paper", (January 2020).
53. Ministry of Electronics and Information Technology, "Committee D on cyber security, safety, legal and ethical issues" (2018).
54. *Ibid.*

Divjyot Singh
Tel: +91 9811 151 683 / Email: divjyot.singh@alayalegal.com

Mr Divjyot Singh is a practising lawyer in New Delhi, India. He is an alum of The National Law School of India University, Bangalore, having graduated in 1995. He is founding partner of Alaya Legal Advocates. He started his career as a litigation counsel on the commercial and corporate side, and over a period of time, has become involved in advising the Information Technology industry. His particular area of expertise lies in respect of issues arising in the use of Information Technology. He advises clients at policy and implementation level on risk assessment and management in respect of the use of AI and the legal consequences arising therefrom.

Kunal Lohani
Tel: +91 9971 388 182 / Email: kunal.lohani@alayalegal.com

Mr Kunal Lohani is an associate lawyer with Alaya Legal. He handles, amongst other things, assignments relating to infrastructure and energy projects. Information Technology including AI and informational privacy are one of the key areas of his practice. He is a part of the competition law team. Having a business background, Kunal has witnessed the critical role that AI plays in maintaining supplies and inventory. He is able to put to use his learnings in the practice of law. Kunal is an alum of Guru Gobind Singh Indraprastha University.

Kumari Poorva
Tel: +91 8010 287 722 / Email: poorva.kumari@alayalegal.com

Ms Kumari Poorva is a qualified company secretary and associate lawyer with Alaya Legal. She handles amongst other things, joint ventures, acquisitions and private equity investments. Poorva is closely involved in advising clients on policy and governance matters. Intellectual property and data protection are key areas of her practice. She is a part of the competition law team. Poorva is an alum of Faculty of Law and Shri Ram College of Commerce, Delhi University.

Alaya Legal Advocates

C-17, II floor, LSC I, Paschimi Marg, Vasant Vihar, New Delhi 110057, India
Tel: +91 11 4167 4456 | 57 | 58 / URL: www.alayalegal.com

Italy

Massimo Donna & Lavinia Carmen Di Maria
Paradigma – Law & Strategy

Trends

Over the past year, big Italian industrial corporations seem to have dramatically increased deployment of AI solutions to boost their core businesses. Examples range from Leonardo, the big defence contractor, which has recently promoted AIRtificial Intelligence together with the Italian Air Force (*Aeronautica Militare*) to bring together startups with AI solutions potentially applicable to the aviation sector to ENI, one of the world's petrochemicals giants, which has recently announced the development, with IBM, and already the deployment of an AI solution called Cognitive Discovery, to optimise its exploration and discovery operations. Another well-established Italian manufacturer, the brakes specialist Brembo, has recently enriched its offering with sensor-rich AI solutions.

Smaller businesses are also rushing to deploy AI solutions. Recently, the Artificial Intelligence Task Force at AGID, the agency in charge of the execution of the Digital Agenda, has mapped the Italian AI ecosystem, finding that hundreds of well-established companies as well as startups are deploying or offering AI solutions. For their part, higher education institutions are rushing to offer AI classes to their students. To name one, the *Politecnico di Milano* has set up a unit to monitor the adoption of AI in Italy and facilitate its students' employment in the sector.

Among the most widespread AI solutions, one can count language processing, demand forecast, predictive maintenance, image processing, fraud detection and virtual assistants/chatbots.

On the whole, it appears that, whereas Italian businesses show a great degree of interest for the potential of AI, the actual adoption of AI solutions is still at a very embryonal stage.

To fully appreciate where the development of AI solutions currently stands in Italy, it should be remembered that Italy's entrepreneurial fabric is very different from that of its European neighbours. In fact, most Italian businesses are SMEs which successfully compete in the international arena thanks to their agility and technological capabilities. Of course, the risk with SMEs is that they lack the necessary capital to adequately invest in research and development. This has prompted the government to set up a number of industry focus groups to support and advise Italian businesses on the adoption of technological solutions, including AI.

The government is also painfully aware that the growth of the tech sector in Italy has been historically stifled by the failure to nurture a decent size Venture Capital (VC) environment. In fact, VC investment is instrumental to the funding of high-growth tech businesses, including those that focus on AI. In order to tackle this issue, the Italian Government has set up a National Innovation Fund, which will invest as much as €1 billion over the next few years in startups focusing on AI, Internet of Things (IoT) and Blockchain solutions.

It probably took longer than expected for the National Innovation Fund to start operating, but its teething issues appear to have been tackled now, with its governance having been addressed at the end of 2019.

Ownership/protection

Most recently, the discussions around the intellectual property implications of AI have centred on (i) the opportunity to envisage new types of IP protection for AI algorithms, (ii) whether works created by AI could be granted IP protection, and (iii) whether the training or deployment of AI may breach third-party IP rights.

(i) Since no specific statutory protection is granted to algorithms, most commentators agree that AI should be protected by way of copyright. However, since copyright protection can only be granted to the means by which an idea is expressed and not to the idea itself, algorithms can only be protected insomuch as the software that embeds them can qualify for protection. This may not seem an adequate level of safeguarding for algorithms, particularly in light of the fact that software programs can be decompiled to allow the study of their internal workings. However, since the patentability of AI, as that of any other software, would only be granted in the presence of technical character, copyright remains the most reliable form of protection.

Of course, if we adopt a broader functional definition of AI where it is composed of both algorithms and the data-sets that are fed to it, then AI protection may be also be granted under articles 98 and 99 of the Industrial Property Code (*Codice della Proprietà Industriale*), which protect know-how. In fact, as long as the data-sets are kept secret (hence, such protection would not be actionable in the case of data-sets originating from cooperative or open source arrangements), they could be regarded as know-how. Finally, data-sets may also be regarded as non-creative databases and, as such, be granted *ad hoc* protection as *sui generis* IP rights under the Copyright Statute (*Legge sul Diritto d'Autore*). In this respect, although to date Italian Courts have not yet ruled on this matter, it seems fair to argue that rapidly changing data-sets may be regarded as databases which undergo a process of constant amendment and integration rather than a continuous flow of ever-new databases. In fact, the latter approach would not allow for database protection.

(ii) Whether or not works created by AI could be granted IP protection is not, as one may think, a futurist concern, but a very current one. In fact, whereas as of the date of writing not many instances of AI-created artistic work have presented themselves which require adequate protection, the matter of whether data-sets originated by the workings of the IoT may qualify for IP protection has been brought to our attention. In fact, although data-sets resulting out of successive iterations within a series of IoT devices might, in theory, qualify for database protection, to date no statutes or case law have provided any clarity as to whom should be regarded as the right holder(s).

(iii) Also, algorithms may be regarded as in breach of copyright if they are fed with copyright-protected work during the training stage. In fact, depending on the task that the algorithm is required to perform, learning data may include visual art, music, newspaper articles or novels which are covered by copyright. However, as long as such training data are not used to replicate the protected works, their use during the learning stage appears to be permitted.

In a context in which case law has not yet had the opportunity to validate most of commentators' theories on AI's intellectual property implications, in 2019 Italian Administrative Courts had a chance to rule on the relationship between algorithmic transparency and intellectual property. Such opportunity arose in relation to a case in which Italian state-school teachers disputed

the procedure by which they had been assigned to their relevant schools. In fact, since 2016, it has been an algorithm deciding which school teachers are assigned to, which is based on a number of set parameters – among which paramount importance is placed on seniority. It soon emerged that a number of teachers were unsatisfied at being assigned to schools in remote regions, which in turn forced them to endure long daily commutes or even to relocate altogether. When some teachers blamed the new algorithm and requested details of its internal workings, the Ministry of Education asked the software vendor which supplied the algorithm to prepare a brief explaining how the algorithm worked. However, after examining the brief and finding it too generic, the teachers asked to be provided with the source code, and when the Ministry rejected the request, several teachers' unions sued the Ministry before the Administrative Court (*TAR Lazio*). The ruling of TAR Lazio (*CISL, UIL, SNALS v MUIR #3742* of 14 February 2017) shed some light on some very relevant legal implications resulting from the widespread use of AI algorithms in decision-making applications. In fact, the Administrative Court ruled that an algorithm, if used to handle an administrative process which may have an impact on the rights or legitimate interests of individuals, is to be regarded as an administrative act by itself and, therefore, must be transparent and accessible by the interested parties. The Court also ruled as to what constitutes transparency. Attempts by the Ministry of Education to appease the objecting teachers by presenting them with the software vendor's brief were not regarded by the Court as having been sufficient. According to the Court only full access to the source code allowed interested parties to verify the validity of the algorithm's internal processes, the absence of bugs and, in general, the adherence of the algorithm to the criteria upon which the relevant decisions should have correctly been made (the Court, however, seemed to conflate the algorithm with the source code, but since the algorithm debated before TAR Lazio is not of a machine-learning nature, this did not seem to affect the Court's reasoning on the specific transparency issue at stake). As for the issue of the balance of IP protection and the teachers' rights to algorithmic transparency, protection from the breach of IP rights to the algorithm was indeed raised as an objection by the Ministry of Education to the teachers' request for sight of the source code, but the Court stated that it assumed the licensing agreement between the software vendor and the Ministry included adequate provisions to protect the vendor's IP rights and went on to say that even if such provisions had not been stipulated, that would not prevent an interested party's access to the source code, as such party could only reproduce, and not commercially exploit, the source code.

Antitrust/competition laws

Although the Italian Competition Authority (AGCM) has not yet taken any definitive stance on the impact that AI may have on competition, it has signalled that the issue is under consideration. In fact, it appears that the main concern is that businesses which collect great amounts of data, such as, for example, search engines, social media and other platform businesses, may end up stifling competition by preventing competitors and new entrants from accessing such data. The assumption behind this is that businesses are increasingly data-driven and may suffer detrimental financial consequences should they not be allowed to access the relevant data. As a way to tackle this, it has been proposed that Big Data be regarded as an essential facility. The application of the Essential Facility Doctrine (ESD) to AI would mean that dominant enterprises may be required to let competitors access the data-sets that they have collected in order to avoid being regarded as exploiting their dominant position. In other words, the ESD would also apply to Big Data. However, data can be easily and cheaply collected by new entrants and are by definition non-exclusive, insomuch as consumers can (and often do) disclose a similar set of data to different service providers

as a consideration for the services that they benefit from. It appears, therefore, that the ESD would only apply to Big Data to the extent to which the data at hand are by their own nature or, by the way their collection must be performed, difficult to gather or exclusive.

Since it appears that the ESD can only find application in particular cases where data cannot be easily collected or, for other reasons, are a scarce resource, it has been proposed that the risk of the creation of "data-opolies" be tackled by way of specific public policies aimed at incentivising data-sharing.

The joint report of the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*), the Italian Electronic Communications Watchdog (*Autorità per le Garanzie nelle Comunicazioni*) and the Italian Fair Competition Authority (*Garante della Concorrenza e del Mercato*) (FCA) of 20 February 2020 appears to confirm such positions; however, at the same time cautioning that too stringent a data protection regime would prevent data-sharing, as a result creating entry barriers and hampering competition. However, the joint report implies that the GDPR has so far showed sufficient flexibility, among other things introducing the right to data portability which facilitates data re-usage.

Of course, data-sharing policies will have to be structured in such a way as to incentivise the sharing of those data which are necessary to secure fair competition, while preventing the sharing of information aimed at such unfair practices as price fixing. Unlawful information-sharing practices may also be implemented by way of the deployment of *ad hoc* AI tools; for example, with a view to enforce unlawful cartels. In fact, algorithms may be used to monitor the competition's prices in real time and enforce cartel discipline. In this case, the Competition Authorities will have to assess whether swift price adjustments, or the adjustment of relevant commercial practices within a relevant market, are the result of the deployment of unilateral pricing algorithms (which is, *per se*, permitted) or a case of enforcement of cartel discipline, which must be swiftly sanctioned.

The FCA is also in charge of enforcing certain consumers' rights. In this context, the FCA sanctioned Facebook for having misled potential service subscribers by stating on its website that Facebook was going to be "free forever". In fact, the FCA found that such statement was misleading as under its current business model Facebook does monetise customers' data and that potential subscribers should have been duly informed. Such decision appears to have resulted in a general obligation for digital platform businesses to disclose to potential customers and subscribers how they monetise their data.

Board of directors/governance

Company Directors are under the obligation to perform their duties with diligence and appropriate technical skills. The recently adopted Insolvency Code has further stressed the need for Directors to ensure that appropriate reporting and monitoring systems are put in place in order to provide timely warning of the company's financial conditions. Failure to adopt such systems may trigger the Directors' personal liability towards creditors who can prove that they have suffered financial damage as a result of the company's lack of adequate internal procedures.

In this context, a Director's diligence must be assessed against the most current technology, including AI. Therefore, Directors must consider the opportunity to adopt any appropriate AI tool to secure suitable internal monitoring systems. To this end, Directors must secure a direct and continuous line of communication with the company's management, including the Chief Information Officer and the Chief Data Officer, in order to be constantly updated on the latest available AI tools and the opportunity of their internal deployment.

In Italy, companies are liable for certain crimes committed by their top-level or, in certain circumstances, mid-level managers on behalf or in the interest of their employer. In order

for companies to avoid liability, they need to prove to have adopted an *ad hoc* compliance programme and to have enforced its compliance, also by way of appointing a supervisory body (*Organismo di Vigilanza* or *OdV*). In particular, in order to be exempt from liability, businesses need to provide adequate evidence that they have put in place a set of appropriate internal procedures, and that the relevant managers could only commit the relevant crimes by eluding such procedures.

Initially the crimes for which employers might be liable were bribery-related, but over time other crimes were added, such as network and digital-device hacking, manslaughter, etc. The required internal procedures typically span over a number of business functions such as finance, procurement, HR, etc. As many such procedures are increasingly AI-based (e.g. in recruitment processes initial CV screening is often carried out by way of an AI tool, potential suppliers' track-records are assessed algorithmically, etc.) the OdV will need to include individuals with adequate expertise to assess whether the deployed AI conforms with the applicable legislation and, if not, act swiftly to remedy the situation.

Regulations/government intervention

No specific legislation has been adopted as regards AI. The consensus seems to be that the current statutes are sufficient to tackle the challenges that AI is bringing to businesses and households.

This approach appears sensible, as an adjustable judicial interpretation of the current statutes should be preferred to the introduction of *ad hoc* sector-specific regulation, which may prove too rigid to apply to the ever-changing characteristics of AI.

So, for example, it has been considered that the liability for damage caused by AI-enhanced medical devices should fall within the field of application of the standard product liability regime; algorithms monitoring personnel in the workplace (e.g. in fulfilment centres, supply chains, etc.) should comply with the specific legislation on staff monitoring (article 4 of law 300 of 1970) and with the employer's general obligation to safeguard the staff's physical and psychological health (article 2087 of the Civil Code), etc. Even when a lively debate erupted a few years back on the legal implications of autonomous vehicles, most commentators seemed to believe that current tort statutes would suffice to regulate such a new phenomenon.

Over the next few years, as AI will become increasingly pervasive and disrupt industries and habits to an extent not easily conceivable at the time of writing, it will probably be necessary to adopt *ad hoc* legislation. However, we expect that AI will be mostly regulated at the EU level.

As an exception to the above, it should be noted that in Italy employers can monitor their staff by way of the "tools" that the staff use to carry out their duties. Employment Courts have recently clarified that, in the case of digital devices, each single app downloaded on the device must be considered as a stand-alone tool and can only be used by the employer for monitoring purposes if they are instrumental to the performance of work duties.

Civil liability

Although case law has not yet had the opportunity to rule on the liability regime of AI, in literature the opinion that the deployment of AI tools should be regarded as dangerous activity seems widely accepted. Therefore, according to article 2050 of the Civil Code, businesses deploying AI solutions would be considered responsible for the possible damage that such solutions may cause, unless they prove that they have put in place all possible measures

to prevent the cause of such damage. However, some commentators have observed that businesses deploying AI solutions may not even be in a position to adopt damage-mitigating measures, as algorithm providers do not allow access to the algorithm's internal workings. It has therefore been opined that AI solution providers should be held liable for damage caused by algorithms. On the other hand, others have stressed that regarding any AI deployment as a dangerous activity does not seem fair and would deter the widespread adoption of AI *vis-à-vis* other countries with less draconian liability regimes. However, such concern has been countered by the observation that, as the potential damage brought by widespread AI adoption has not been fully assessed yet, the EU Precautionary Principle should apply, which would open the floodgates to regarding AI as a dangerous activity and to the application of article 2050, at least for the time being.

The role of "AI Agents" in the context of IoT platforms has also been widely discussed. For example, in which capacity do AI Agents operate when placing an order as a result of their sensors detecting that a quantity/level of certain goods have decreased below certain levels? Such agents cannot be regarded as representatives as a representative must be legally capable, therefore some commentators have argued that AI Agents could be subject to the same very limited legal representation regime as slaves used to be subject to in ancient Rome. It is hard to assess whether such creative legal thinking will be backed up by Courts, however these attempts to come to terms with AI Agents must be read in the context of a wider debate as to whether the advent of AI warrants the adoption of *ad hoc* legislation or not.

In fact, whereas some observers claim that the disruption brought by AI calls for the adoption of *ad hoc* regulation, others point out that such *ad hoc* measures would necessarily be too specific and risk being already behind the AI-development curve by the time they become effective. Such observers opine that the broad-based Civil Code provisions on tort and contractual liability would better adjust to the ever-changing AI technical landscape and use cases.

Criminal issues

Over the last few years, Italy has consistently been adopting AI solutions for crime-prevention purposes. Crime-prevention algorithms have been licensed to law enforcement agencies in a number of medium to big cities, including Milan, Trento and Prato. Such AI deployment has been a complex exercise, since in Italy, four different police forces (i.e. *Polizia di Stato, Carabinieri, Guardia di Finanza* and *Polizia Locale*) carry out sometimes overlapping tasks and only share certain databases.

Integrating data coming from such a variety of sources may prejudice data quality, leading to unacceptable biased outcomes. Moreover, data collection at a local level may be patchy or unreliable if carried out with low-quality or unreliable methods. In fact, typically, local law enforcement agencies rely on *ad hoc* budgets set out by cities, municipalities or local police districts. Therefore, poorer areas affected by severe budget constraints may have to rely on outdated Big Data systems or algorithms, giving rise to unreliable data-sets which, if integrated at a higher state level, may corrupt the entire prediction algorithm. Biased data-sets may also derive from historical data which are tainted by long-standing police discriminatory behaviours towards racial or religious minorities.

Wouldn't it be great if the police could know in advance who might be committing a crime or be the victim of a crime? While many believe this is already possible thanks to the latest predictive policing AI tools, critics fear that such tools might be riddled with old-fashioned racial bias and lack of transparency.

Predictive policing may, then, cause resentment in communities of colour or communities mostly inhabited by religious or cultural minorities. Such resentment may grow to perilously high levels unless the logic embedded in the relevant algorithms are understood by citizens. However, transparency may not be possible, either due to the proprietary nature of algorithms (which are typically developed by for-profit organisations) or because machine-learning algorithms allow for limited explicability. Therefore, it has been suggested that accountability may replace transparency as a means to appease concerned communities. So far, Italian law enforcement agencies have been cautious in releasing any data or information as regards the crime-prevention algorithms.

Discrimination and bias

In addition to what has been pointed out in relation to the use of AI for crime prevention, controversies have arisen as to the possible discriminatory consequences of the use of AI for human resources purposes. In particular, the potential use of AI as a recruitment tool has led some commentators to argue that biased data-sets could lead to women or minorities being discriminated against.

Italy has of course implemented the EU anti-discrimination directives, and the use of discriminatory criteria by AI-enhanced recruiting tools would trigger the liability of both the recruiter and of the algorithm supplier.

Equally, should the recruiting algorithm be fed with biased, incorrect or outdated data, candidates who did not get the job could be entitled to compensation if they could prove that such data were used for recruiting purposes.

It appears less likely that algorithms would be used to single out personnel to be laid off in the context of rounds of redundancies. In fact, the criteria by which redundant staff are picked out are typically agreed upon with the unions' representatives; whereas in the absence of an agreement, certain statutory criteria would automatically apply.

On the contrary, algorithms could be used to carry out individual redundancies; for example, within management. In fact, managers' (*Dirigenti*) employment can be terminated at will (although the applicable national collective agreements provide for certain guarantees) and algorithms could be used to pick out the managers whose characteristics match certain AI-determined negative patterns. However, the required granularity of the data-set for this specific task makes the use of AI still unlikely in the context of individual redundancies.

National security and military

As mentioned earlier, Italian defence contractors are among the most enthusiastic adopters of AI solutions in Italy. Certain defence contractors also manufacture aircraft, helicopters and other devices for civilian use, selling such products to a number of foreign states, including China; some critics have found this concerning, especially at a time in which Sino-Italian relationships have been boosted by the recent entering into force of a memorandum of understanding on the Belt and Road Initiative.

Such criticisms seem to originate from the current specific circumstances, in which China is being challenged by certain countries to re-negotiate trade deals. The fact that the relationship between an AI superpower such as China and Italy has touched a raw nerve cannot conceal the reality that Italy and China have been good trading and technological partners for decades, having established a mutually beneficial relationship which dates back to a time when China was not considered a commercial (or military) threat to the western powers.

Massimo Donna
Tel: +39 02 3655 2788 / Email: md@paradigma-law.com
Massimo is head of the Technology Group at Paradigma – Law & Strategy. He advises clients on a broad range of technology and complex commercial matters. Massimo also advises clients on employment tech matters. Massimo was educated in Italy and Spain, trained in Italy and New York City and practised law as a foreign lawyer in London. Massimo also served as a senior in-house lawyer at various multinational tech companies. His mother tongues are Italian and English and he is also fluent in Spanish and French. Massimo routinely lectures on a range of technology law matters.

Lavinia Carmen Di Maria
Tel: +39 02 3655 2788 / Email: ldimaria@paradigma-law.com
Lavinia is an associate at Paradigma – Law & Strategy, where her practice focuses on complex IT contracts, Blockchain and Artificial Intelligence.

Paradigma – Law & Strategy

Piazza Luigi Vittorio, Bertarelli 1, 20122 Milan, Italy
Tel: +39 02 3655 2788 / URL: www.paradigma-law.com

Japan

Akira Matsuda, Ryohei Kudo & Haruno Fukatsu
Iwata Godo

1 Trends

1.1 Overview of the current status of AI in Japan

The Japanese government and private sector are making huge investments in artificial intelligence ("AI") technologies as key drivers of future competitiveness in Japan's aging society after the decrease in birth rate. Several policy and funding programmes are being implemented by Japanese governmental authorities. Under such governmental initiatives, the collection of big data through IoT and the development of data analysis technology through AI are making rapid progress in Japan.

Not only computers and smartphones but various types of equipment and devices, such as vehicles and home appliances, are connected to the Internet, and the digital data collected via such equipment and devices is utilised.

Technologies being utilised for business purposes include: mobility, mainly automated driving; smart cities and smart homes and buildings (big data provides infrastructure managers and urban planners with invaluable information on real-time energy consumption which makes it easier to manage urban environments and devise long-term strategies); and healthcare and wellness for healthy lives. In addition, many domains and business sectors, such as manufacturing, production control (and supply chains generally), medical/chirurgical treatment, nursing, security, disaster management and finance are also seeking to maximise synergies with the IoT and AI.

Under these circumstances, the Japanese government has announced a general policy regarding the use of AI and IoT described in section 1.2 below, and discussions are being held focusing on certain key legal issues described in section 1.3 arising from the use of AI and machine learning.

1.2 The government's view

The Japanese government established an Artificial Intelligence Technology Strategy Council in 2016, which published the Artificial Intelligence Technology Strategy in March 2017. Furthermore, in January 2016, the government issued its 5th Science and Technology Basic Plan (2016–2021) that sets out the goal for Japan to lead the transition from "industry 4.0" to "society 5.0", in which all aspects of society (not just manufacturing and other industries) are transformed by new information technologies and systems.

In May 2018, the Cabinet Office adopted the "Declaration to be the World's Most Advanced IT Nation and the Basic Plan for the Advancement of Public and Private Sector Data Utilization", which also outlines the government's policy to advance technologies using AI and IoT. Based on the updated Declaration in June 2019, the Japanese government published

"AI Strategy" in July 2019, which contains measures which the Japanese government should implement promptly under governmental initiatives in order to utilise AI and IoT for resolution of social problems.

Although companies using AI were expected to exercise self-restraint and avoid aggressive development, the "Conference toward AI Network Society of the Ministry of Internal Affairs and Communications" published the Draft AI Research & Development Guidelines in July 2017 and the Draft AI Utilization Principles in July 2018. In August 2019, the Conference published the "AI Utilisation Guidelines" which were based on and elaborate the "AI Utilisation Principles". These guidelines and principles cover matters to be kept in mind in order to reduce risks associated with systems using AI, such as the opaqueness of AI's determination processes and loss of control.

In December 2018, the government's "Conference on Principles of Human-centric AI Society" published seven core AI principles, including corporate accountability, to ensure process transparency when a company takes decisions through the use of AI technology.

1.3 Key legal issues

Key issues around AI are outlined below. Issues arising under intellectual property law, civil law, personal information/data privacy law, and competition law are covered in sections 2–6.

1.3.1 Contract regarding utilisation of AI technology and data

In order to promote and facilitate the free flow of data and utilisation of AI among businesses, the Ministry of Economy, Trade and Industry formulated the Contract Guidance on Utilization of AI and Data ("Contract Guidance") in June 2018. The Contract Guidance identifies key elements that businesses should focus on in establishing fair and appropriate rules governing data utilisation, provides a rationale for each specific use category and explains approaches that businesses should consider in negotiating and coordinating the details or terms of contract. The Contract Guidance includes an AI section and a data section. A brief outline is provided below. This Contract Guidance was updated in December 2019 in order to reflect the 2018 amendment of the Unfair Competition Prevention Act ("UCPA").

1.3.1.1 Outline of the Contract Guidance (AI Section)

The Contract Guidance classifies typical contractual formulation issues into three types:

(a) Issue 1.
Issue: Who owns the rights to AI technology development deliverables: the vendor; the user; or both?
Solution: For each item, such as raw data, machine learning datasets and AI products, the Contract Guidance defines intellectual property rights and methods to establish rights and terms of use.

(b) Issue 2.
Issue: How should provisions concerning the utilisation and protection of data be stipulated?
Solution: The Contract Guidance identifies important points to consider in selecting a data trade intermediary (neutrality, income for stable operations, obligations and responsibilities with respect to security and transparency, etc.), and several alternative methods that may be used to determine the scope of use and restrictions according to the nature and type of data (confidentiality, frequency of provision, etc.).

(c) Issue 3.
Issue: Who assumes responsibility for the performance of models and how is this achieved?

Solution: The Contract Guidance proposes a method to limit the scope of responsibility of vendors based on the understanding that it is difficult to ensure the seamless performance of models.

1.3.1.2 Outline of the Contract Guidance (Data Section)

The Contract Guidance categorises data utilisation contracts into three types ((i) data provision, (ii) data creation, and (iii) data sharing), and explains the structures, legal nature, issues, proper contract preparation process, and provides model contract clauses for each contract type.

(i) Data provision type contracts: One party which owns the data grants the other party the right to the data.
(ii) Data creation type contracts: The parties create/compile the new data together and negotiate their respective rights and obligations to utilise the new data.
(iii) Data sharing type contracts: The parties share data using a platform which aggregates, stores, processes, and analyses data.

1.3.1.3 Considerations regarding cross-border transfers

The Contract Guidance also provides points of note regarding cross-border transfers, including the determination of the law applicable and the selection of a dispute resolution method, and how to comply with overseas regulations on data transfers (such as the PRC's Cyber Law or the GDPR).

1.3.2 Criminal liabilities for traffic accidents caused by automated driving cars

In Japan, criminal liabilities for traffic accidents caused by automated driving cars are discussed with reference to five different levels based on the degree of control/autonomy of vehicles which have been proposed by the Automobile Engineering Society. Levels 0 to 2: automated functions only assist driving by drivers who are natural persons, which means that drivers (natural persons) remain in control of the driving. Therefore, traditional legal theories apply to accidents in those cases. Traffic accidents caused by Level 3 or higher automated driving systems are discussed below.

1.3.2.1 Level 3

At Level 3, the system performs all driving tasks, but drivers need to respond to requests for driving instructions from the systems or to failures. Drivers are still obliged to look ahead and concentrate while the systems perform the main driving tasks.

1.3.2.2 Level 4 and Level 5

At Level 4 or higher, natural persons are not expected to be involved in the driving and are not obliged to anticipate or take action to avoid traffic accidents. Therefore, the issue of the drivers' criminal liability does not arise.

The main points of discussion are as follows: is it appropriate to hold AI liable criminally by considering that AI has capacity to act and can be held responsible/accountable? Does it make sense to recognise AI's criminal liability? And, how can AI designers and manufacturers be held criminally liable on account of product liability when the product is partially or completely controlled by AI?

1.3.3 Labour law issues

1.3.3.1 Issues relating to the use of AI for hiring and personnel evaluation purposes

As companies have wide discretion in hiring personnel and conducting performance evaluations, it is generally considered that the utilisation of AI in this HR context is not illegal in principle. However, legal or at least ethical problems could arise if the AI analysis

is inappropriate, and would, for instance, lead to discriminatory treatment. This point is actively debated.

Another bone of contention is whether companies should be allowed to use employee monitoring systems using AI for the purposes of personnel evaluation, and the health management of employees from a privacy perspective.

1.3.3.2 Labour substitution by AI

Another point actively discussed is the replacement of the labour force by AI (robots in particular) and whether the redeployment and transfer of employees to another department, or their discharge because of labour substitution by AI where it leads to the suppression of a department, can be permissible. However, these discussions are part of the traditional employment law discussions on redundancies.

2 Ownership/intellectual property rights regarding AI

2.1 Overview

AI draws on developments in machine learning and rapid advances in data collection and processing. The process for developing machine learning/algorithms and statistical models using AI and outputting AI products utilising these models involves the handling of valuable information such as data, programs, and "know-how" (see section 2.2.1 below for the summarised contents of the recent amendment to the Copyright Act).

2.2 Learning stage

2.2.1 Raw data

A huge amount of "raw data" is collected and accumulated by cameras and sensors installed and operated for business activities, as well as by using methods such as data input. Such raw data will be subject to data protection regulation in Japan, where a specific individual's personal information is distinguishable from such raw data.

When the raw data corresponds to works such as photographs, audio data, video data, and novels, creators of these works acquire the copyrights, unless otherwise agreed by contract. Accordingly, using such raw data without permission of the copyright holders can be a copyright infringement.

However, the Copyright Act was amended to ensure flexibility and legal certainty for innovators which became effective on January 1, 2019, introducing the following three provisions and removing perceived copyright barriers to AI:

- New Article 30-4, which allows all users to analyse and understand copyrighted works for machine learning. This means accessing data or information in a form where the copyrighted expression of the works is not perceived by the user and would therefore not cause any harm to the rights holders. This includes raw data that is fed into a computer program to carry out deep learning activities, forming the basis of AI.
- New Article 47-4, which permits electronic incidental copies of works, recognising that this process is necessary to carry out machine learning activities but does not harm copyright owners.
- New Article 47-5, which allows the use of copyrighted works for data verification when conducting research, recognising that such use is important to researchers and is not detrimental to rights holders. This Article enables searchable databases, which are necessary to carry out data verification of the results and insights obtained through text and data mining.

In contrast, when raw data can be deemed as "trade secrets" satisfying all requirements, namely, confidentiality, non-public nature, and usefulness (Article 2, Paragraph 6 of the UCPA), such raw data is protected under the UCPA.

With the revision to the UCPA which became effective on July 1, 2019, big data, etc. that does not qualify as trade secrets but that is subject to certain access restrictions (such as ID and password setting) or restrictions limiting data supplies to third parties will also be protected under the UCPA, as "data subject to supply restrictions".

Raw data that does not correspond to works, trade secrets, or data subject to supply restrictions cannot be protected under the Copyright Act or the UCPA. Accordingly, companies that wish to secure legal protection for raw data *vis-à-vis* third parties need to secure protection through contracts made with the third parties (i.e. terms of use).

2.2.2 Training data

The collected and accumulated raw data is then processed and converted into "training data", which is data aggregated in a format suitable for AI machine learning.

The training data obtained by subjecting the raw data to processing and conversion, such as pre-processing for learning and adding of correct answer data, can be protected under the Copyright Act as "database works" (Article 12-2 of the Copyright Act) if the training data constitutes an intellectual creation resulting from "the selection or systematic construction of information". That is, the creator of the training data is the copyright holder, unless otherwise agreed by contract.

"Know-how" relating to a method for processing the raw data into a dataset suitable for learning by AI shall be protected under the UCPA if the processing method falls under the definition of trade secret under the UCPA.

Know-how is often obtained through a process of collaborative operations between the vendor and the user. In such a case, if the contract between the vendor and the user does not provide for any agreement regarding the ownership of the right to the know-how, both the vendor and the user may claim the right to the know-how. Accordingly, in order to avoid disputes, the vendor and the user should expressly agree with each other on the ownership of the right and the terms of use in the contract.

In addition, the description regarding the protection of raw data in section 2.2.1 also applies to training data.

2.2.3 Program for learning

A "program for learning" is a program adapted for the input of training data and the generation of "learned parameters".

The algorithm of the program for learning is protected under the Patent Act as an invention of a program if it satisfies the requirements for patentability, such as novelty and inventive step.

Also, a "learning approach" that is determined artificially, including the selection of training data, the order, frequency, and combining method of learning, and a method of adjusting parameters, is protected under the Patent Act as an invention of a learning approach if the learning approach satisfies the requirements for patentability.

The source code of the program is protected under the Copyright Act as a program work (Article 2(1)(x) and Article 10(1)(ix) of the Copyright Act) if the source code satisfies the requirements for works. For the copyright of a program work, the so-called "program registration", such as the registration of a copyright (Article 77 of the Copyright Act), can be made at the Software Information Center ("SOFTIC").

If a created program for learning or learning approach falls within the trade secret definition under the UCPA, it is protected under the UCPA.

2.2.4 Learned model

2.2.4.1 Learned parameters

In many cases, learned parameters themselves obtained by inputting training data into the program for learning are not protected under the Patent Act, the Copyright Act, or the UCPA.

Accordingly, companies that wish to secure legal protection of the learned parameters in relation to third parties need to consider protecting them, mainly by concluding contracts with the third parties to whom they intend to supply the learned parameters.

2.2.4.2 Inference program

An "inference program" is a program that incorporates the learned parameters and is necessary for obtaining constant results (AI products) as outputs derived from the input data.

In addition, as to the protection of the inference program, the above description regarding the protection of the program for learning also applies.

2.3 Use stage

2.3.1 Overview

When certain data is input to the "learned model", the learned parameters and the inference program are applied to the input data. Regarding this data, the results of predetermined judgment, authentication, assessment, and proposal are computed. Thereafter, the data is output as an "AI product" in the form of voice, image, video, letter or numeric value.

2.3.2 In the presence of creative contribution or creative intent by humans

Under the current legal system, an AI product may be protected under the Copyright Act or the Patent Act as a work or an invention made by a human, if it can be deemed that the "human" using AI is engaged in creative activity using AI as a tool in the process of producing the AI product. In this case, the creator or the inventor is the person engaged in creative activity using AI as a tool.

A situation where creative activity is performed using AI as a tool is similar to a process where, for example, a person uses a digital camera as a "tool", adjusts the focus and the shutter speed to produce a photograph as a work, and the person who has taken the photograph owns the copyright.

Thus, when creative contributions by, or creative intents of, humans are part of an AI product, the "AI user" who has made the creative contribution is basically recognised as the right holder of the AI product under the default rules of the Copyright Act and the Patent Act.

Therefore, unless otherwise agreed by contract, the right holder of training data, the right holder of an AI program or a program for learning, or the right holder of a learned model would not be the creator or the inventor.

Accordingly, where a vendor who provides a platform for product creation by AI wishes to appropriate all or part of the rights to an AI product created by a user, it is necessary to stipulate the ownership of the right to the AI product and in terms and conditions of service or the contract with the user.

2.3.3 In the absence of creative contribution by, or creative intent of, humans

Where there is no human creative activity using AI as a tool, it is currently considered that this AI product should not be regarded as a work or an invention and should not be protected under the Copyright Act or the Patent Act.

At present, as part of the discussion on future legislation, it is asserted that, from the viewpoint of suppressing free riding or securing creative incentives, even AI products obtained without human creative contribution need to be protected by intellectual property rights including copyright. However, such discussions still remain at a very preliminary stage of the legislative debate.

2.3.4 Issues regarding misleading AI-created content

Under current laws, the rights in and to an AI product vary greatly depending on whether human creative contribution is admitted in the AI product production process. However, it is difficult for third parties to distinguish and determine the presence or absence of human creative contribution from the appearance of the AI product.

Accordingly, there could be cases where content which is actually produced by AI and does not fall within the IP definition of a work could be mistakenly treated as a work protected under the Copyright Act, and if the fact that the content is produced only by AI is revealed after a business relationship has been established among many parties, this would destroy licence relationships and undermine business schemes.

3 Competition law

3.1 Overview

How to deal with AI/big data under competition law in Japan is under review, but discussions at regulator level are still at a preliminary stage and not yet reflected in any actual enforcement policy. Currently, mainly two aspects are being discussed: the first is digital cartels (whether the existence of a cartel can be admitted where prices are fixed through the use of algorithms); and the second is the impact of data on anti-competitive effect analysis – especially, data aggregation in the context of large digital platformers such as GAFA, both in the context of merger control and abuse of a superior bargaining position.

The local competition authority, the Japanese Fair Trade Commission ("JFTC") published a report on data and competition policy in June 2017 ("JFTC Report"). In the JFTC Report, the JFTC has made a detailed analysis of the correlation between data and competition law in Japan, and it is worth noting that the JFTC has made its position clear that if data-driven activity has an anti-competitive effect in a relevant market, such activities will be the target of enforcement in the same manner as traditional anti-competitive activities.

3.2 Digital cartels (algorithms cartels)

In Japan, digital cartels are discussed in accordance with the four categorisations made by the OECD: (i) the computer as messenger; (ii) hub and spoke; (iii) predictable agent; and (iv) autonomous machine. Cartel activity in Japan requires an agreement between the parties, which could be an issue for categories (iii) and (iv). Digital cartels are also covered by the JFTC Report, and the JFTC has made its position clear that if an anti-competitive effect is caused by a digital cartel and cartel requirements are met, the JFTC will crack down on those digital cartel activities. However, so far there have not been any enforcement cases in respect of digital cartels in Japan.

3.3 Data aggregation and anti-competitive effect

According to the JFTC Report, when analysing the anti-competitive effect resulting from the aggregation of data, certain factors must be taken into consideration, such as: (i) whether there is an alternative method to obtain such data; (ii) economic analysis on the usage of data (including its size); and (iii) correlation with AI.

If a company acquires blue chip start-up companies with a small market share from an economic standpoint but having developed cutting-edge technology, software or know-how, such acquisitions could be anti-competitive but fail to show negative implications in a merger control analysis (or could even not be caught by merger control regulations). Furthermore, as a result of the network effect, market entry by new entrants could be hampered. Accordingly, the traditional market definition theory based on market shares from an economic perspective might not work well for the digital market where data plays a far more important role (i.e. free market and multifaceted market). Similarly, in the context of merger control, when a corporation with aggregated data (i.e. digital platformer) is going to merge, when deciding whether it has a dominant position in a given market, it is possible to take into consideration the rarity of the data and whether there are alternative methods to collect such data, in addition to the traditional economic analysis based on past revenue.

These aspects are also discussed in the JFTC Report; however, the regulator is still in the study phase regarding these new theories, and the JFTC's thinking is not yet finalised and reflected in its decisions.

3.4 Latest trends: the JFTC's position on enforcement against digital-related vertical restraints

The JFTC publicly announced in December 2018 that they would carefully watch digital platformers in Japan (i.e. GAFA and the likes), looking for horizontal restrictions (i.e. cartels) and vertical restrictions (i.e. abuse of a superior bargaining position (which is a similar concept to "abuse of dominance", but dominance is not required, and the abuse of a superior bargaining position will suffice)). A typical example of abuse of a superior position is a situation in which a party makes use of its superior bargaining position relative to another party with whom it maintains a continuous business relationship to take any act to unjustly, in light of normal business practices, cause the other party to provide money, services or other economic benefits. In connection with this exercise, the JFTC conducted a survey of the contracting practices of large digital platformers in January 2019. In this connection, the Japan Cabinet proposed a Bill for the Digital Platform Transparency Act, which is expected to be adopted in the ordinary Diet session in 2020. This Act would regulate large-scale online malls and app stores, by requiring certain disclosure and to take measures to ensure fairness in operations in Japan.

4 Data Protection

4.1 Overview

The main data protection legislation in Japan is the Act on Protection of Personal Information ("APPI"), which was significantly overhauled in May 2017 to strengthen data protection. Bi-lateral adequacy referrals on cross-border data transfer restrictions between the EU and Japan came into effect on January 23, 2019. We will explain the AI and big data-related issues from a data protection perspective in Japan, by distinguishing three phases: collection; use; and transfer of personal data. Specific rules apply to anonymised data, which are not described here but can be relevant to big data and data mining. The APPI is scheduled to be amended in 2020 and the details for the amendment are expected to be clear in the middle of 2020. It is expected that the concept of pseudonymised personal data would be newly introduced, which will promote the usage of such data in the context of feeding the AI.

4.2 Phase 1: Collection of personal data

Under the APPI, consent from the data subject is not required upon collection of personal data from such data subject (except for sensitive personal data). However, under the APPI, the purpose of use must be either disclosed or notified to the data subject prior to collection, and

proper collection of personal data is required. Accordingly, if a business operator is collecting personal data from data subjects in order to use such data for analysis or development of AI-related systems, it should limit the categories of personal data to be collected to the extent reasonably expected by the data subject, and ensure transparency.

4.3 Phase 2: Use of personal data

The use of personal data by the business operator is limited to the purpose of use disclosed or notified to the data subject prior to such use. In case the business operator uses collected personal data for development of AI-related systems or analysis related to AI, such usage must be covered by the disclosed or notified purpose of use of the personal data. If such usage is not covered, the business operator must modify the purpose of use and disclose or notify to the data subject of such modification. We note that in contrast with the GDPR, profiling itself is not regulated under the APPI.

4.4 Phase 3: Transfer of personal data

Under the APPI, if a business operator is transferring personal data to a third party, such business operator must obtain the prior consent of the data subject, unless such transfer is made in conjunction with entrustment, joint use or business succession (i.e. M&A), or such transfer falls under exemptions specified under the APPI (i.e. public interests). In terms of AI-related software or systems, such system or software normally does not contain personal data, and in such case, the transfer of software or systems will not trigger any consent requirement under the APPI.

5 Regulation/government intervention

5.1 Overview

This section covers regulations, including proposed regulations, and government intervention with respect to AI, big data and deep learning.

5.2 Special laws on automated driving

The Japanese government aims for practical use of Level 3 automated driving (see section 1.3.2.1) at express highways and Level 4 automated driving (see section 1.3.2.2) at depopulated areas by around 2020. In order to achieve such goal, the Road Transport Vehicle Act ("RTVA") and the Road Traffic Act ("RTA") were amended in 2019. The following outlines and explains these amendments.

5.2.1 RTVA

(a) After the amendment comes into force, if the automated driving system conforms to safety standards, driving a car using such system on a public road is allowed.
(b) The Minister of Land, Infrastructure, Transport and Tourism sets conditions for using an automated driving system (such as speed, route, weather and time of the day) according to the amended RTVA.
(c) The certification of Director of the District Transport Bureau is newly required for the replacement or repairment of equipment using automated driving technology such as dashboard cameras and sensors.
(d) The permission of the Minister of Land, Infrastructure, Transport and Tourism is newly required for modification of programs used for automated driving systems.

5.2.2 RTA

(a) The definition of "driving" has been expanded to include driving using an automated driving system.
(b) Although using mobile phones with hands and focusing on the screen whilst using a car navigation system was universally prohibited by the RTA before its amendment,

the amended RTA allows these actions in automated driving under certain conditions. However, drink driving, sleeping and concentrating on reading and using a smartphone when driving are still prohibited.

(c) Recording and keeping information for confirmation of operating conditions of the automated driving system are newly required.

5.3 Special laws on AI development and utilisation of data

In line with the fast development of AI technology and the increasing significance of data, laws have been enacted or amended to further promote AI development and utilisation of data. For example, the Act on Anonymously Processed Medical Information to Contribute to Research and Development in the Medical Field was enacted in 2017 and came into force in May 2018. Under this law, universities and research institutions can utilise patients' medical information held by medical institutions as big data in a more flexible manner. In addition, the UCPA was amended in 2018, as explained in section 2.2.1 above.

Furthermore, the Telecommunication Business Act and its sub-legislation was amended (effective April 2020) and the duty to place cyber security measures on IoT devices will be imposed. Another amendment is expected in 2020 to introduce its extra-territorial application. Also, as explained in section 3.4 above, the Platform Transparency Act is expected to be adopted in the ordinary Diet session in 2020.

5.4 Guidelines, etc. for AI

In addition to laws and regulations, the government is publishing various guidelines to facilitate the utilisation of AI technology and big data. For details, see section 1.2 (various guidelines by the Japanese government), section 1.3.1.1 (Contract Guidance (AI section)) and section 1.3.1.2 (Contract Guidance (Data section)) above.

6 Civil liability

6.1 Overview

This section covers civil liability issues linked to the utilisation of AI.

6.2 AI and civil liability

When AI causes any damage to an AI user or a third party, the entities that can be held liable may be (1) the AI user, and (2) the AI manufacturer broadly interpreted. With regard to "the AI user", the following issues may arise: (a) whether or not AI should be held liable in tort if it causes any damage to a third party; and (b) what could be the AI user's liability where AI performs a contract on its own. For the "AI manufacturer", liability under the Product Liability Act could arise.

6.3 Liability of AI users

6.3.1 Liability in tort

If an AI user is found negligent with respect to the utilisation of AI, the AI user will be liable for damages in tort (Article 709 of the Civil Code). In determining whether or not the negligence of the AI user can be established, the concept of negligence is not considered to have a different definition or scope especially for the utilisation of AI from the traditional interpretation of negligence.

In order to find AI users negligent, the AI users need to be able to foresee the occurrence of specific results and to avoid such results arising from the act of AI. However, the act of AI is almost unforeseeable for the AI users given that its judgment process is not known to them at all. From this standpoint, it is unlikely that the AI users will be negligent (although being aware of uncontrollable risks inherent in the black box and still using the AI could be negligence).

Nevertheless, there may be a case where AI users are required to perform a certain degree of duty of care for the act of AI. At least at the early stage of AI introduction, it is not appropriate to rely fully on the act of AI and AI users are likely to be required to comply with a certain degree of duty of care by monitoring the act of AI.

6.3.2 Liability under contracts executed by AI

There could be cases in which AI executes a contract; for example, by placing an order automatically after checking the remaining stock of commodities in a household or of products in a factory. When the execution of the contract by AI is appropriate, the contract is regarded as valid. However, if AI makes a mistake in executing the contract (for example, when it purchases unnecessary goods or when the price is significantly higher than as usual), it is questionable whether the AI user should be liable under such contract.

When the AI user entrusts AI with the execution of a contract, it is considered that the user expresses its intention to "sign the contract using AI" to the counterparty. Similarly, the counterparty expresses its intention to "accept the contract offer made by AI". Since the intentions of the AI user and the counterparty match one another, the contract is deemed duly executed between the AI user and the counterparty.

The contract is valid and effective in principle even when a mistake is found in the contract offer made by AI, because the intention of the AI user to "sign the contract using AI" and the intention of the counterparty to "accept the contract offer made by AI" match each other. AI's execution of a contract is considered "invalid due to mistakes" only in exceptional circumstances where the motive of the AI user can be deemed to have been expressed to the counterparty.

6.4 Liability of AI manufacturers

The manufacturer of a product will be liable for the damage arising from the personal injury/bodily harm or death or loss of damage to property caused by a defect in such product (Article 3 of the Product Liability Act). Accordingly, if AI has a "defect" (i.e. "lack of safety that it should ordinarily provide"), the AI's manufacturer will be liable under the Product Liability Act.

No established view exists at present as to when AI should be regarded as "lacking safety that it should ordinarily provide", and further discussions are expected.

Akira Matsuda
Tel: +81 3 3214 6282 / Email: amatsuda@iwatagodo.com
Akira Matsuda is a partner at Iwata Godo and head of the AI/TMT practice group. He is an attorney-at-law admitted in Japan and based both in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions and capital markets, as well as international disputes (litigation/arbitration). Mr. Matsuda is also advising many Japanese and foreign clients for data security issues, in terms of Japanese laws, Singapore PDPA, and GDPR including structuring of global compliance systems.
A graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Ryohei Kudo
Tel: +81 3 3214 6237 / Email: rkudo@iwatagodo.com
Ryohei Kudo is a partner at Iwata Godo. He is an attorney-at-law (admitted in Japan and New York) and patent attorney. His practice focuses on IP and a wide variety of domestic and international dispute resolution. His practice also includes cross-border transactions, M&A, corporate commercial work, corporate governance, shareholders' meetings, and general corporate law. Before joining Iwata Godo, he worked for the Government of Japan (Ministry of Defense). A graduate of the University of Tokyo (J.D. & LL.B.) and Columbia Law School (LL.M.).

Haruno Fukatsu
Tel: +81 3 3214 6031 / Email: haruno.fukatsu@iwatagodo.com
Haruno Fukatsu is an associate at Iwata Godo. She is an attorney-at-law (admitted in Japan). Her practice focuses on general corporate matters and a wide variety of domestic dispute resolution. Her practice also includes corporate governance, shareholders' meetings and M&A. Additionally, Ms. Fukatsu has advised many clients for data protection and data security issues in terms of Japanese laws and GDPR. She graduated from the University of Osaka (LL.B.) and the University of Kyoto (J.D.).

Iwata Godo

Marunouchi Building 15F, 2-4-1 Marunouchi, Chiyoda-ku, Tokyo 100-6315, Japan
Tel: +81 3 3214 6205 / Fax: +81 3 3214 6209 / URL: www.iwatagodo.com

Korea

Won H. Cho & Hye In Lee
D'LIGHT Law Group

Trends

As one of the world's top countries in terms of IT, Korea has great interest in intelligent information technology. The Intelligent Robots Development and Distribution Promotion Act, establishing and promoting a policy on the sustainable development of the intelligent robot industry, was enacted as early on as December 2008. When the match between South Korean Go's grandmaster Lee Sedol and Google DeepMind's artificial intelligence ("AI") program, AlphaGo, was held on March 2016, AI became a sensation to South Koreans. Together with the boom brought by the match of the century and the government's support, intelligent information technology and its market are growing rapidly.

The Korean government established and operated an advisory committee for the intelligent information society in October 2015. After the announcement of the "Plan for Intelligent Information Society Strategy" in January 2016, the government announced that it would invest ₩1 trillion (US$863 million) in AI research over the next five years. In addition, the government-constituted task force for the strategy, comprising 10 government institutions and private experts, held seminars and conference to share concerns and ideas with the public, finally announcing the "Mid- to Long-Term Intelligent information Society Plan For the 4th Industrial Revolution" in December 2016. The plan describes intelligent information technology as a technology which implements data processing abilities, such as recognition, perception, inference, etc., at a human level, by converging AI technology and data utilisation technology. Data utilisation technology refers to the internet of things ("IoT"), cloud computing, big data and mobile ("ICBM") technologies, in preparation for the 4th Industrial Revolution. Put simply, huge amounts of various data collected by IoT will be transferred, saved and accessed in great speed everywhere by cloud computing and mobile technologies, and will then be processed by AI. Recently in December 2019, the "National Strategy for Artificial Intelligence" was announced.

Ownership/protection

Big Data

Big data represents the information assets characterised by high volume, velocity and variety to require specific technology and analytical methods for its transformation into value. The definition and concept of big data are still vague and developing, and this makes ownership and protection issues more complex.

One of the most complex issues is the ownership of big data using external data. If a set of big data consists of data created and uploaded by Facebook users, can we say the big data is owned by the producer of the big data? Or is it owned by the users? To make the issue even

more complicated, the privacy issue may be introduced. Is the user's consent required? If so, to what extent does a producer need to obtain consent from the user? If not, can the user refuse or request to stop the use of his data? This is not a novel, fresh issue, and there are a number of studies and papers on the subject, but the government has not yet made an official statement in relation to it; thus, how big data can be protected under the current Korean legal system should be reviewed, unless new legislation is enacted.

In Korea, collections of data such as databases are protected under the Copyright Act if certain conditions are met. If the collection has a creative nature in terms of the selection, arrangement or composition of its materials, it is protected as a compilation work. In case such creativity is not present, its producer can be protected if the collection is a database, which is defined as a compilation with materials systematically arranged or composed so that they may be individually accessed or retrieved; and the producer has made a substantial investment in human or material resources for the production of the database, or for the renewal, verification or supplement of their materials.

Because big data collects an enormous amount of data in various forms, it is not unlikely that data is selected or selected in a creative way. Consequently, a big data set is not a compilation work, and the producer can be protected under the Copyright Act only if it is systematically arranged with sufficient investment. A big data set is processed before storage, but the data processing method is different from that applied to a conventional database. If the court or authority finds the data to be arranged in a systematical way, the person who made a substantial investment for the production of the big data would be protected under the Copyright Act.

Database producers have the rights to reproduce, distribute, broadcast or interactively transmit the whole or considerable parts of a relevant database, but individual materials of the database shall not be considered as the considerable parts of the relevant database. A database will be protected for only five years, which is considerably shorter than that of other types of copyright works, which are protected for 70 years after the death of the producer.

Creation by AI

As AI technology develops, it is not surprising to hear the news that an AI system has composed music, drew a picture, wrote an article, and so on. Currently, the Copyright Act in Korea protects works which are creative productions expressing human thoughts and emotions. Clearly, AI is not accepted as human, so a creation by AI is not protected under the Copyright Act. Some propose to protect a creation by AI as a work made for hire, which is a work made by an employee during the course of his duties. The employer will be the author of a work made for hire if such work is made public under the name of the employer, unless otherwise stipulated in the contract or work regulation. No matter how attractive the idea is, the application of the principle of work made for hire does not seem to be an answer, as the employee should be a human and works should contain human thoughts and emotions.

The ownership and the protection of data and works of the 4th Industrial Revolution are not clear or sufficient under the current Korean legal system. A new and comprehensive legislative framework will be required in the near future.

Antitrust/competition laws

Big data enables a company to establish a very effective marketing strategy for each individual customer, by giving companies a better idea of what the customer wants and the channel they typically use when buying. Being aware of the power and value of big data, the market and the government are now starting to fear that big data could create barriers to entry and market power, especially where a company holds datasets that require enormous time

and money to establish or cannot be easily accessed by competitors. Big data holders may have an unfair advantage over competitors, resulting in harm to consumers and competitors.

The 2018 economic policies released in December 2017 by the Ministry of Economy and Finance ("MOEF") pointed out that the data-based industry, which includes big data and AI, is vulnerable to a monopoly by a small number of frontier companies. Any practical regulation or restriction is yet to be adopted, but the MOEF announced that it will monitor the data-based industry for unfair trade and competition.

The Korean government also announced that it will disclose public data and provide means to access and utilise data containing private information owned by government authorities.

Board of directors/governance

Data governance is a data management concept concerning the capability of an organisation to ensure that high data quality exists throughout the complete lifecycle of data, thus ensuring that value is derived from it. It is generally achieved through a combination of people and processes, with technology used to simplify and automate aspects of the process.

Regarding data governance at the level of national or public society, such as with regards to the population census, traffic volume, unemployment rate, etc., the Korea Information Society Development Institute ("KISDI") issued a report proposing to upgrade the data governance of national statistics by: 1) strengthening the National Statistical Office by making it independent from other government authorities, and providing it with stronger powers to adjust its budget; 2) carrying out business process reengineering, which will enable the automated collection of data in the course of daily work; 3) establishing the basis and system to utilise private data in national statistics; 4) collecting and combining administrative records held by central government and local municipal governments; 5) adopting an autonomous quality assurance system for private data, to ensure standardisation and credibility; and 6) developing a sustainable data management practice, which will allow the use of data in research while protecting privacy and data more effectively than before.

Regulations/government intervention

There are numerous acts in force which are partially related to the intelligent information society; for example, the Framework Act on National Informatization, the Software Industry Promotion Act, the Act on the Development of Cloud Computing and Protection of its Users, the Intelligent Robots Development and Distribution Promotion Act, the Special Act on Promotion of Information and Communications Technology, and the Activation of Convergence Thereof, Etc. Most of the aforementioned acts are concerned with how to encourage and accelerate the development of the intellectual information technology. To integrate and harmonise regulation over the intelligent information society, in February 2017, the bill for the Basic Act on Intelligent Information Society was submitted to the National Assembly, and is under review. Again, the Act proposes rules to facilitate the development of the intelligent information society, but does not contain any detailed regulations on practical issues such as ownership, antitrust, governance, etc.

In June 2018, the Ministry of Science and ICT ("MSIT") published ethical guidelines and a charter of ethics for the intelligent information society, aimed at reinforcing ethics of responsibilities in developing and providing intelligent information technologies and services as well as preventing their misuse by users, ultimately to achieve the human-oriented intelligent information society. These do not have any binding legal effect, but stipulate the key principles of the intelligent information society for people.

In January 2020, the three major pieces of legislation which promote and govern the use of data, the Personal Information Protection Act ("PIPA"), the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. ("Network Act"), and the Credit Information Use and Protection Act ("Credit Act"), have been amended as follows:

- PIPA adopted the concept of anonymised data and pseudonymised data. The former is partially replaced or deleted personal data so that an individual cannot be recognised or identified without use of additional data. The latter is not explicitly defined in PIPA, but it can be interpreted as data from which an individual cannot be recognised or identified even if additional data is used or applied. PIPA allowed pseudonymised data to be processed for statistical, scientific research, or public interest record-keeping purposes, and exempted major obligations applicable to typical personal data, such as the user's prior consent to collect data and release of data after a certain period of time. Of course, PIPA imposed other requirements and restrictions to protect personal data. For example, the combination of pseudonymised data owned by two different personal data controllers can only be done by professional agencies, a personal data controller should separately maintain the additional data that can be combined with the pseudonymised data which enables identification of individuals, and processing of pseudonymised data for the purpose of identifying an individual is prohibited. PIPA would not be applicable to anonymised data, as anonymised data is not interpreted as the personal data under PIPA.
- The main amendment to the Network Act was the deletion of provisions related to the protection of personal data, so that PIPA would be the main legislation which governs matters related to protection of personal data.
- The Credit Act was amended to provide the legal basis for analysing and using big data in the finance sector. Similar to PIPA, pseudonymised data can be processed for statistical, scientific research, or public interest record-keeping purposes without the user's consent.

There are a few regulations which govern AI issues in a more practical manner. In August 2013, the Capital Market and Financial Investment Business Act allowed for the adoption of a robo-advisor in the financial industry. A robo-advisor is required to satisfy certain conditions on the part of the investor, such as the direct analysis of an investor's propensity, their investment in at least two items, the readjustment of their portfolio in every quarter, their evaluation by qualified external experts and more, in order to give advice on investment and manage assets. Also, the Ordinance in relation to Safe Driving and Test Driving of AI Vehicles stipulates mandatory requirements such as functions, devices and labels for AI vehicles.

Implementation of AI/big data/machine learning into businesses

The most well-known AI-implemented business in Korea is AI interpreting services. Papago, created by Naver, Korea's largest portal site company, is capable of interpreting 14 languages; and Genie Talk, created by a collaboration between the Electronics and Telecommunications Research Institute ("ETRI") and Hancom, the Korean word processor software developer, is capable of interpreting nine languages.

There are more than six major smart speakers in the Korean market, which provide daily information, the time, weather and music, and some of them can be connected to a smartphone, TV or other home appliances (washing machines, refrigerators and air conditioners) which have IoT sensors, and it is expected to be more competitive as Samsung is to launch its own smart speaker in 2020.

AI is also playing an active role in the financial sector. Robo-advisors are providing tailor-made portfolios to clients by analysing the client's investment tendency, size of investment, preferred investment region, and so on. A chatbot which provides a 24-hour answering service to simple questions, an AI service which manages pension assets via its website and a mobile application are currently available in the Korean financial market.

In the medical sectors, establishing a medical image big data station is a hot topic. There are more than five image data centres run by major hospitals. Korean hospitals are aiming to quickly adopt AI solutions in order to increase the accuracy of diagnoses. Also, AI services are being applied to telecare services and x-ray image interpretation.

The Ministry of Justice has launched an online chatbot service called Bubby, which provides legal information on real estate, leases, layoffs and inheritance. In addition to this, DR & Aju Law Firm has introduced an intelligent legal information system, developed by Intellicon Meta Lab, which helps a person to draft legal documents by automatically understanding the meaning of a sentence and changing word expressions into legal terms.

In addition, AI care robots for elders, AI English teachers for kids, AI manufacture or agricultural environment controllers to increase product efficiency, AI cleaners which search and delete photos of women taken without their consent and more AI are being implemented and used in Korea.

Civil liability

It is expected that AI will play a massive role in the intellectual information technology society. Hence it is important to discuss the principles for the compensation of harm or loss incurred by AI. For example, if a car driven by AI hits a pedestrian, who would be the one to compensate the pedestrian – the driver, the car owner, the car manufacturer, the programmer of the AI, or, if possible, the AI itself? Currently, there are debates over whether AI can be covered under the conventional principles of the Civil Act, and there are some opinions that novel principles and legislation should be implemented for AI issues.

Under the Korean Civil Act, a person who causes loss to or inflicts injuries on another person through committing an unlawful act, intentionally or negligently, should provide compensation for damages arising therefrom. However, a person would not be considered negligent or in default unless the result of an act was foreseeable and could have been avoided.

If an AI's behaviour is to be governed by the fault liability principle, the supervisor's liability, the employer's liability, the structure possessor's liability and the animal possessor's liability, these principles may be considered respectively.

The supervisor's liability is applicable when a person who has caused any damage to another is exempt from tort liabilities, because he/she is a minor or incompetent due to mental unsoundness. If so, the person who is under a legal duty to supervise such person shall be liable to give compensation for the damage, provided that the same shall not apply if the supervising person has not been negligent in performing his/her duty of supervision.

A person who employs another to perform a specific task is liable for compensating any loss inflicted on a third person by the employee in the course of performing the specific task: this is called employer's liability. However, this shall not apply where the employer has exercised due care in appointing the employee, and in supervising the performance of the specific task, or where the loss has been inflicted even if the employer has exercised due care.

Neither of the liabilities abovementioned are applicable to AI, because AI is not a person. Even if an AI is accepted as a legal entity or person in the future, it seems that no user,

possessor, owner or programmer could be found to have a legal duty to supervise or have employer-employee relations with the AI. Moreover, they would be exempted because they had exercised due care and were not negligent in supervising, as they had no means to supervise the AI, due to its autonomy.

The structure possessor is liable to damages caused to another person by reason of any defect in the construction or maintenance of a structure, although if the person in possession has exercised due care in order to prevent the occurrence of such damages, compensation for the damage shall be made by the owner. A structure is defined as any artificial thing, so AI would fit into this category. The hard part will be to define what is a defect of an AI. Because AI learns how to act by deep learning or machine learning using big data, it is not easy to say that an AI is defective, even if an AI made a wrong decision as a result. Furthermore, a possessor is just a user who does not know how AI works, or could not notice a defect of AI, if any.

Lastly, every owner of an animal is liable for any loss inflicted on a third person by the animal, unless the owner has not been negligent in taking due care for the custody of the animal, according to the animal's species and nature. This seems to be an attractive principle to be applied to AI because of the common features shared between animals and AI, in that they make decisions by themselves, and such decisions are unpredictable to their owners. However, in most cases an owner would have a much higher level of control and power over an animal than they would over AI. Consequently, it is questionable whether an owner who does not have control over AI can be responsible.

If an AI's behaviour is to be governed by the strict liability principle, the structure owner's liability and product liability may be implicated.

A structure owner is liable for a defect of a structure if the possessor is not involved in the construction or maintenance of such structure. Although the structure owner is strictly liable for the defect, the defect of an AI is hard to be defined or examined.

According to product liability, a manufacturer shall compensate for damages to the life, body or property of a person caused by a defect of a product. Here, the definition of defect again becomes a problem. There are three types of defect defined for product liability:

- "Defect in manufacturing" means the lack of safety caused by the manufacturing or processing of any product not in conformity with the originally intended design, regardless of whether the manufacturer faithfully performed the duty of care and diligence with respect to the manufacturing or processing of the product.
- "Defect in design" means the lack of safety caused by the failure of a manufacturer to adopt a reasonable alternative design in a situation where any damage or risk caused by the product would otherwise have been reduced or prevented if an alternative design had been adopted.
- "Defect in indication" refers to cases where damages or risks caused by a product could have been reduced or avoided if a manufacturer had given reasonable explanation, instructions, warnings or other indications concerning the product, but he/she fails to do so.

A defect in manufacturing is not applicable to AI, as AI will be developed in a way different from the originally intended design by deep learning. There would be no defect in design, because no alternative design is adoptable. An AI programmer or manufacturer would not be liable for defect in indication, either. Furthermore, the product liability can be exempted if 1) the manufacturer did not supply the product, 2) the existence of the defect could not be identified by the state of scientific or technical knowledge at the time when the manufacturer supplied the product, 3) the defect is attributable to the manufacturer who complied with

the standard prescribed by any act or subordinate statute at the time when the product was supplied, or 4) in the case of raw materials or components, the defect is attributable to the design or the instructions on manufacturing given by the manufacturer of the product for the relevant raw materials or components.

In summary, the conventional civil liability principles in Korea are not sufficient to cover damages caused by AI. The introduction of new principles and legislation after thorough discussion in relation to AI is desired.

Criminal issues

Under the conventional criminal liability principle in Korea, a natural person should be criminally liable. Can AI, then, be liable for a criminal act? There are three types of AI: weak AI; strong AI; and super AI. Weak AI can only perform based on the algorithm programmed by a human. In contrast, strong AI is a machine capable of performing any intellectual task that a human being can. Strong AI upgrades, modifies and develops the algorithm originally programmed by humans, resulting in behaviour deviating than that programmed by the original algorithm. Super AI is an AI machine which understands the human mind and/or even surpasses it. Although it may sound uncomfortable, we cannot deny that strong AI or super AI has the potential to be accepted as a natural person. However, this would not become reality in the near future, and the question of how AI can be punished or penalised arises. There is already an exception that a non-natural person can be criminally liable: companies are criminally liable for an employee's committed crime if a legal provision explicitly stipulates so. This exception cannot apply to AI, because the AI is the one who carried out the criminal action.

If AI cannot be criminally liable, can a user or a programmer of an AI be criminally liable for the AI's action? On one hand, there is no doubt that a person who uses AI as a tool to commit a crime will be criminally liable. On the other hand, it is arguable that a user or a programmer would be liable for the AI's autonomous criminal action. Conventionally, a person would be criminally liable if an action's criminal consequence is foreseeable and avoidable to that person. Although it is hard for a user or a programmer to predict the AI's action after deep learning, this means that no one will be liable for the AI's action, and, consequently, the user or programmer will not endeavour to prevent such criminal action. Some argue that a user or a programmer should be strictly liable for an AI's criminal action, but this would greatly discourage the use or development of AI.

As interest in AI and the intelligent information society grows, concerns and discussions on AI's criminal liability is increasing in Korea. AI's criminal liability will be determined by new legislation, and ample study, review, scrutiny, debate and discussions are required for balanced and righteous legislation.

The Korean government is aware of potential criminal action using AI, such as deep fake, and will establish rules and regulations to prohibit such wrongful use.

Discrimination and bias

Often, AIs are mistaken to be always emotionless, fair, neutral and equal. However, there is a risk that AIs may become discriminative and unjust if machine learning is carried out using a biased database. The MSIT's charter of ethics requires that decisions automatically made by intellectual information technology should not be socially prejudicial or discriminative.

In addition, discrimination results if AIs cannot be used or accessed by certain types or classes of people. Sharing the same concern, the MSIT's charter of ethics states the principle that

the deliverables and benefits of intellectual information technology should be equally owned by the public. The Intelligent Robots Development and Distribution Promotion Act also requires the government to prepare measures necessary for facilitating the development and distribution of intelligent robots to improve the convenience of using AIs, so that socially disadvantaged people, such as the disabled, the elderly and low-income earners, can enjoy opportunities for and benefits from free use of such robots.

National security and military

According to the information released by the Ministry of National Defense in September 2018, there are a number of projects underway to adopt AI and big data technology to enhance national security and military power. First of all, surveillance and reconnaissance will be performed by AI, enabling 24-hour supervision and greatly increasing accuracy. Soldiers will be trained using virtual reality, augmented reality and mixed reality, which provides a more realistic and detailed experience. Military equipment and assets will be managed and inspected by AI based on machine learning, so that they can be kept in consistent good condition. Finally, military hospitals, in cooperation with private hospitals, will establish the use of medical data as big data.

Won H. Cho
Tel: +82 2 2051 1870 / Email: whc@dlightlaw.com

As an experienced patent lawyer with extensive commercial transactional experience in various specialty industries including entertainment, ICT and healthcare, Won H. Cho is uniquely positioned to advise clients in a wide range of complex IP, corporate and regulatory matters. He started his career as an associate at Bae, Kim & Lee LLC ("BKL") and went on to serve as a partner of the firm, leading BKL's prominent intellectual property and technology transaction practices, spanning a total of 16 years. Mr. Cho also worked on secondment at Ropes & Gray (New York) in 2014 in the firm's Intellectual Property division. He has earned a reputation at home and abroad as an exceptional multi-disciplinary lawyer with deep and extensive career experience representing local corporations, multi-national companies, government agencies and non-profit organisations. Recently, he has been actively advising clients in the blockchain industry.

Mr. Cho is now an adjunct professor at KAIST-MIP (Master of Intellectual Property) and serves in leadership roles at various local and state organisations, including the Korea Fair Trade Commission Advisory Committee, Korean Intellectual Property Office, US Korea Law Foundation, Korea Licensing Executive Society, and the Korea Association of Entertainment Law, among others. Mr. Cho holds a B.A. from Seoul National University and received an LL.M. from the University of Texas.

Hye In Lee
Tel: +82 2 2051 1870 / Email: hil@dlightlaw.com

Hye In Lee is an associate at D'LIGHT, where she focuses on advising and assisting on litigation and legal issues in the ICT and FinTech industries, including blockchain systems. Ms. Lee also has extensive field experience in both international legal cases, such as global investment, M&A and international arbitrations, and local legal cases, including IP litigation, financing, investigation by the public prosecutor and/or the Korean Free Trade Commission, from her time as corporate counsel at Samsung C&T Corporation and Netmarble Corporation.

D'LIGHT Law Group

5th Floor, 311, Gangnam-daero, Seocho-gu 06628, Seoul, Korea
Tel: +82 2 2051 1870 / URL: eng.dlightlaw.com

Mexico

Alfredo Lazcano & Andrea Avedillo
Lazcano Sámano, S.C.

Introduction

Since Alan Turing, in the middle of the 20th century, raised the possibility of machines being able to think, the world has never been the same.

Although the concept of artificial intelligence ("AI") nowadays is no longer unrelated to a large sector of the world's population, the fact is that it is difficult to assume the total understanding of it. In very simple terms, it is indeed the ability of machines to emulate human thinking and, in this way, to perform tasks that, until a few decades ago, could only be executed by humans.

The improvement that AI has brought to our lives is undeniable: medical procedures are more precise; it helps scientific research; it diminishes the margins of human error in almost all work environments; it allows communications between people who are separated by thousands of miles; it can overcome language barriers; and, more recently, it can make predictions or directly affect the decision-making of the members of a particular society – or even of a whole country.

However, in our opinion, there are two major problems or challenges with AI: the first is related to the vertiginous development of AI; and the second refers to the profound inequality that exists in our world.

The first problem has to do with the fact that not even AI developers are able to know the limits of it, and what is more disturbing, they have no idea how to keep it under control. Elon Reeve Musk, founder of Tesla, Inc., as well as of several cutting-edge technology companies, states that "*AI doesn't have to be evil to destroy humanity – if AI has a goal and humanity just happens to be in the way, it will destroy humanity as a matter of course without even thinking about it, no hard feelings*".[1] In that sense, it is essential to create laws that regulate the development and use of AI, as well as to design policies to promote ethics, education and user protection.

The second challenge abovementioned implies that the higher the level of poverty in a given country, the greater to the delay in the use of AI in the daily life of its population. Likewise, countries with low education levels fail to include people in the use of technological tools that, in many cases, are costly and difficult to understand. Finally, when the economic growth of nations is low, it is difficult to allocate investment to technological development due to the lack of resources and the high demand for basic services and products of first necessity.

However, it is paradoxical that the lack of growth of a country limits its access to technological innovation and the use and development of AI, while the technological innovation and the use and development of AI, nowadays, can accelerate its growth.

This chapter will mainly address the second challenge applied to the situation in Mexico, as an explanation of the backwardness, for many unexplainable, that is observed in Mexico in the

face of the use and development of AI, and all that this entails. Likewise, the great potential that Mexico has to become the leader of Latin America in terms of AI and technology innovation will be exposed, pointing out the challenges that we believe the country must face in the following years.

Despite the economic, political and social complexity of a developing country like Mexico, it is a nation with several advantages, such as its geographical location and its demography, that it has not yet fully realised and that, if exploited in an appropriate manner, could place it at the forefront of what today some international observers call the *fourth industrial revolution* – a historic change in which AI is considered a technological element.

The situation in Mexico: trends

Unlike other leading jurisdictions in the field of AI (i.e. the US, which is in a privileged position thanks to companies such as Facebook, Amazon or Apple), Mexico is not yet distinguished by its innovation in terms of technological development, nor for an aggressive policy of AI implementation.

The use of Information and Communication Technologies ("ICT"), which is essential for the implementation of processes and tools created from AI, shows a considerable delay in Mexico compared to its northern neighbours: "*The incorporation of ICT in everyday life was slow at first, due to high costs and little penetration of networks.*"[2]

Certainly in a country with a population of almost 128 million people of which 41.9%[3] are in poverty, it is difficult, on the one hand, to make the necessary investment to implement the use of AI, and on the other hand, to permeate in all – or at least in the majority – of the social levels of the population.

Thus, for example, José Luis Becerra, editor of *Cio México*, a publication of International Data Group, points out that "*the great challenge that Mexico faces, is that only a small portion of its workers have the skills that will be enhanced with the revolution of AI*".[4] This phrase summarises the importance of both collective education around the use of AI, and access to the relevant means for its use.

In October 2018, the Mexican company Metrics Digital, with expertise in digital transformation and automation through AI, announced the First Market Maturity Study of AI in Mexico,[5] carried out with the collaboration of the newspaper *El Financiero*, the Employer Confederation of the Mexican Republic (Spanish acronym "COPARMEX"), the Graduate School of Business Administration and Management of the Technological Institute of Monterrey (Spanish acronym "EGADE Business School"), and the Aspen Institute.

The abovementioned study showed that, although in Mexico 42.3% of the workforce are digital natives, as for 2018, digital development and understanding of concepts such as Deep Learning or Machine Learning, are not yet fully adopted in Mexican companies, since the very concept of AI is known in its most basic sense and in very general terms; however, our market still shows little maturity in the country in terms of AI.

The good news is that a large percentage of the population recognises the benefits of using AI, compared to a much lower percentage that only sees risks in it. This indicates a receptive attitude and, although there is still a long way to go, in general the posture is positive; this is one of the signs of Mexico's potential as a market for the development and implementation of AI.

On the other hand, Metric Digital's study also showed very interesting data regarding the sectors in which it is planned to invest in AI. Contrary to what happens in more mature

latitudes, Mexico was thinking of investing in AI in the short term in the sectors of services, consumption and manufacturing.

Although companies understand the advantages of digitisation and of the application of AI, they do so exclusively in order to encourage consumption of the goods or products they offer, with the purpose of changing traditional business models; but they are reluctant to incorporate these techniques into their work centres. "*In Mexico, micro, small and medium enterprises* (Spanish acronym "PYMES") *are the backbone of the economy, generating 72% of employment and contributing up to 52% of the country's GDP. In 2015, 97% of the more than 4 million companies in the country were microenterprises, and 74% of these did not use the Internet or have a computer*."[6]

Mexican society is beginning to wake up to the reality that if digitisation continues to be postponed, this will be an obstacle to its growth; however, although there are many things yet to be done, the picture is in fact encouraging.

Its geographical position, as well as the number of inhabitants within the Mexican territory, make Mexico an attractive market for the development of AI-related technologies, given that the volume of data produced in the country represents, by far, the highest of Latin America. "*It is interesting to state that language is one of the variables that can offer some advantage to the country. With 437 million speakers, Spanish is the second most spoken native language in the world, behind Mandarin Chinese with 1,284 million, and above English, with 372 million. In this regard, Mexico is the country with the largest number of people who speak Spanish, which, coupled with its ascendancy over other Spanish-speaking countries, can help it assume leadership in the collection, communication and use of data*".[7]

Recent efforts

While it is true that Mexico's delay in terms of AI is unquestionable, in recent years encouraging efforts have been made to solve some of the problems outlined above and to include Mexico in the race of this so-called fourth industrial revolution.

On November 2013, the Government, led by President Enrique Peña Nieto, presented the public programme National Digital Strategy[8] (Spanish acronym "EDN"), which contains the guiding principles of a project created with the aim of improving connectivity and ensuring digitalisation of the country.

The EDN arises as a result of the constitutional amendment in telecommunications that was published on June 11, 2013 in Mexico. In the words of Peña Nieto, EDN "*will be the key to democratize access to instruments such as the Internet and Broadband, and to take full advantage of the endless possibilities that they can offer*".[9]

As mentioned above, the main objective of the EDN was to digitise services and processes, as well as to allow all Mexicans access to ICT, in order to modernise the Government and to contribute to the country's development.

Five years after its creation, in April 2018, the EDN achieved the establishment of the Artificial Intelligence and Deep Learning Subcommittee and its Technical Council, under the Inter-Secretariat Commission for the Development of Electronic Government (collegiate body established by the Presidential Agreement in charge of promoting and consolidating the use and advantage of ICT), aiming to "*have a high-level digital policy*".[10] Likewise, the work of the National Chamber of the Electronic Industry, Telecommunications and Information Technology (Spanish acronym "Canieti") was promoted in order to make a diagnosis of the needs of AI in the industry.

The advances were related to institutionalisation and leadership, as the beginning of the construction of a structure capable of implementing AI in all areas of public life.

The Administration of President Andrés Manuel López Obrador, who took office on December 1, 2018, has shown some interest in continuing the work of the EDN, even though it is being framed by many political observers as a left-wing Government, as opposed to its predecessor; in our opinion, the Public Agenda has been more oriented to reach certain goals aimed to support the most basic strata of Mexican society.

Indeed on December 9, 2019, López Obrador issued by publication in the Federal Official Gazette (Spanish acronym "DOF") the Regulations of the Office of the Presidency of the Republic,[11] in which the EDN is defined as "*the Federal Executive's action plan to seize the potential of information and communication technologies, including broadband and Internet services, as a catalyst for the country's development, by incorporating it into people's daily lives, and into the Federal Public Administration, through the use of informatics and the digital government development*". Moreover, the same Regulations set forth the Coordination of the EDN, which is part of the Office of the Presidency, as the body in charge of the EDN.

Nonetheless, it is remarkable to note that the public spending granted to the Office of the Presidency for 2020, and thus the Coordination of the EDN, was reduced by approximately 42%[12] compared to 2019.[13]

Results and challenges: what is next?

Thanks to the EDN, several policies were originally implemented and aimed to guarantee connectivity, digital inclusion and digital skills, such as the so-called "*Shared Network*", whose objective is to ensure that more than 90% of the population has a 4G broadband connection by 2024.[14]

Another programme promoted through the EDN was "*Code X*", created to promote the inclusion of girls and women in the use of ICT.

Regarding changes or advances in the legislation, it is important to mention that Mexico, through belonging to a Romano-Germanic legal system (i.e. Civil Law), has more rigid concepts, categories, rules and certain doctrines for amendments than in countries with a tradition of precedents, which, in our opinion, could make it difficult to modify laws that, due to their creation at the time, did not contemplate technological assumptions.

However, in addition to the aforementioned constitutional reform in telecommunications that had as its main purposes, among others, the universal coverage of services and the deployment of infrastructure, it is important to mention the creation of the relatively new Law to Regulate Financial Technology Institutions[15] ("Fintech Law").

The Fintech Law was published on March 9, 2018, in order to regulate the financial services provided by financial technology institutions. This law regulates mainly two institutions, namely: collective financing institutions; and electronic payment fund institutions. However, its provisions also foresee the use of virtual currency and novel models that are defined as those that "*for the provision of financial services use tools or technological means with modalities different from those existing in the market*".[16]

The Fintech Law represented an important advance in terms of technological innovation, applied to the financial sector. However, the real challenges in the years to come will be in its correct application by the financial regulatory bodies, as well as the appropriate inclusion of the new entities authorised under the Fintech Law within the Mexican financial system.

Together with the economic and social progress that our nation needs to achieve, it is absolutely necessary to break the paradigms that surround the concept of AI.

On the one hand, it is necessary to desensitise the working population in order to convey the fact that the use of tools associated with AI is not necessarily intended to replace human functions, but to increase their effectiveness and to improve processes. On the other hand, it is essential to invest in programs specialised in technological research so that Mexico promotes the creativity of its academic, labour and business sectors, and not only to repeat or copy models that could work better in other circumstances.

Of course, any aim without a plan of action becomes simply a good intention, so it is essential that both the Government and the private sector get involved in the law-making process and create public policies and programmes that reinforce learning and innovation, while protecting consumers and citizens in general.

The current Government of Mexico has the opportunity – which seems almost a responsibility – to turn Mexico into a leading country in terms of Big Data and generation of AI, despite the overall cut to public spending, and specifically within the EDN's scope, as we have explained previously.

We believe this is a chance for both private and academic sectors, led by industry stakeholders and researchers, to seek the promotion in Mexico of more discussion forums for the dissemination of high-tech knowledge and to undertake educational actions to boost the Government's interest in technological affairs.

Urgent reforms: intellectual property, antitrust and privacy

Throughout our professional experience, we have been able to notice that in the face of the global reality of AI, there are still important obstacles and gaps in the Mexican legislation that need to be urgently addressed by the current administration, as well as the Congress, to promote reforms which could strengthen and update the legal framework in the following areas:

(i) Intellectual property rights for AI and other emerging technologies.
(ii) Rules to encourage fair and equitable economic competition, both in access and in the use of data.
(iii) Measures to guarantee greater protection of personal data.

In fact, the first obstacle can be found in the Industrial Property Law ("IP Law"), which does not consider computer programs as inventions, which translates into an impediment to get them patented. However, in practice, the Federal Law on Intellectual Rights ("Copyright Law") is used to correct this omission of the IP Law, since the Copyright Law allows the protection of said programs primarily through International Law, i.e. international treaties. Therefore, Mexico needs to update its legislation on intellectual and industrial property as soon as possible, so that the specific safeguarding of emerging or novel technologies, such as AI programs, is contemplated.

A second barrier has been identified in the Federal Antitrust Law ("Antitrust Law"). AI requires data for its operation, and the data are goods – or rather, assets – that can, without a doubt, grant enormous competitive advantages to those who hold them. As such, the Antitrust Law must contain legal provisions that facilitate data access to the developers of digital services related to AI, and "*must be revised to ensure that the accumulation of data assets does not lead to the exclusion of other companies*".[17]

Last, but not least, there is another problem that is not unrelated to other jurisdictions, which in Mexico can be partially traced to certain gaps in the Federal Law on Protection of Personal Data in Possession of Individuals ("Privacy Law"), among other legal systems in Mexico related to the field of data. As we have seen, AI feeds precisely from data that, in many cases, are obtained

from the private – and even intimate – information of people. Therefore, it is important that the collection, storage and use of data in general are subject to laws and regulations that safeguard and give priority to the most basic rights of freedom and privacy of individuals.

Conclusions

A paradox involves a contradiction, and in the worst case, an impossibility. From our point of view, a fair part of the development of AI in Mexico could be in a paradoxical situation. On the one hand, the Mexican jurisdiction could be considered as the largest Spanish-speaking region generating data, and consequently a gigantic incubator of AI technologies; however, the economic difficulties that permeate developing countries like Mexico logically slow down the potential of their progress, contribution and technological leadership.

In recent years, the Government of Mexico has recognised the importance of AI, Big Data, Machine Learning and other essential technologies to face 21st century challenges, promoting the creation of some Government entities for the formulation of public policies in this regard. However, as the Mexican saying states: "*facts are true love, and not just the good reasons*", there is still much to be done.

Regarding legislation, although there have been some advances in the recognition and regulation of innovative technologies (i.e. the Fintech Law or even in the most recent bills of law in the gaming field), we really consider that it is imperative that the Executive and Legislative branches in Mexico, with the proactive participation of technology leaders and academics, seize the *momentum* that AI is taking worldwide, and boost the necessary legislative amendments to correct the deficiencies and regulatory gaps that have been pointed out by the private sector and the academy, with a special emphasis on the urgency of intellectual property, antitrust and privacy matters.

It is equally important to invest in the development of new technologies in order for Mexico to fully grasps the potential of growth it has. As pointed out by Professor Ignacio Ruelas, "*faced with the acceleration of global changes, governments have the opportunity and the important function, through the planning and execution of public spending, to create conditions and new markets where companies, educational institutions and public agencies interact with a same purpose: to create wealth, distribute it and resume the path of sustained growth*".[18]

* * *

Endnotes

1. Martin, S. (April 10, 2019). Elon Musk WARNING: Artificial Intelligence could be an 'IMMORTAL DICTATOR'. Retrieved May 20, 2019, from https://www.express. co.uk/news/science/1112515/elon-musk-artificial-intelligence-ai-news-google-deepmind.
2. Estrategia Digital Nacional 2013–2018. Retrieved May 13, 2019, from http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf.
3. *Informe anual sobre la situación de pobreza y rezago social 2020*. Secretaría de Bienestar. Retrieved March 18, 2020, from https://www.gob.mx/bienestar/documentos/informe-anual-sobre-la-situacion-de-pobreza-y-rezago-social.
4. Becerra Pozas, J. (2019). *Inteligencia Artificial en México, ¿estamos listos para dar el salto?*. [online] Noticias, Tecnología Empresarial, Seguridad. Available at: http://computerworldmexico.com.mx/inteligencia-artificial-en-mexico-estamos-listos-para-dar-el-salto/ [last accessed May 30, 2019].

5. Executive version available at: http://metrics.digital/estudio-de-madurez-de-la-inteligencia-artificial-en-mexico/ [last accessed June 14, 2019].
6. Gobierno Hábil. (2019). *Hacia a una estrategia de AI en México: Aprovechando la Revolución de LA AI*. [online]. P. 11. Available at: https://www.gobiernohabil.com/2018/09/rumbo-una-estrategia-de-inteligencia.html [last accessed May 24, 2019].
7. Girón, M. (2019). *México puede triunfar en Inteligencia Artificial Forbes México*. [online] Forbes México. Available at: https://www.forbes.com.mx/mexico-puede-triunfar-en-inteligencia-artificial/ [last accessed May 31, 2019].
8. Estrategia Digital Nacional 2013–2018. *Op. cit.*
9. *Ibid.*
10. Press note. (2018). Secretaría de la Función Pública. *Crea SFP Subcomisión de Inteligencia Artificial y Deep Learning de la CIDGE.* Available at: https://www.gob.mx/sfp/prensa/crea-sfp-subcomision-de-inteligencia-artificial-y-deep-learning-de-la-cidge [last accessed June 12, 2019].
11. *Reglamento de la Oficina de la Presidencia de la República*. Available at: https://www.dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09/12/2019.
12. *Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2020*. Available at: https://www.dof.gob.mx/nota_detalle.php?codigo=5581629&fecha=11/12/2019.
13. *Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019*. Available at: https://dof.gob.mx/nota_detalle.php?codigo=5547479&fecha=28/12/2018.
14. Gobierno Hábil. (2019). *Op cit.* P. 20.
15. *Ley para Regular las Instituciones de Tecnología Financiera.* Available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf.
16. *Ibid*. Artículo 4.
17. Gobierno Hábil. (2019). *Op cit.* P. 50.
18. Ruelas Ávila, I. (2019). *Gasto público en ciencia y tecnología, ¿por qué, cómo y para qué?*. [online] Nexos. Available at: https://educacion.nexos.com.mx/?p=2073 [last accessed March 18, 2020].

Alfredo Lazcano
Tel: +52 55 4358 7774 / Email: als@lazcanosamano.com

Alfredo Lazcano, Chair at Lazcano Sámano, S.C., Mexico City.

Alfredo was born in Mexico City, holds a Law Degree from the Universidad Iberoamericana (UIA), and since 2007 has been accruing professional expertise in various global cutting-edge technology sectors.

His duties in Lazcano Sámano, S.C. are: to pursue the best professional practices; to implement an ethical business strategy; to act as facilitator between the Law Firm's teams in legal and regulatory matters; and to ensure proper communication with Clients.

He is a Board Director and provides services as a Gaming, Sports & Entertainment Lawyer.

Andrea Avedillo
Tel: +52 55 5292 0065 / Email: aab@lazcanosamano.com

Andrea Avedillo, Head of Legal at Lazcano Sámano, S.C., Mexico City.

Andrea was born in Mexico City, studied Law at the Instituto Tecnológico Autónomo de México (ITAM), and since 2011 has been accruing professional expertise in various global cutting-edge technology sectors.

Her duties in Lazcano Sámano, S.C. are: to manage and execute the timely provision of legal and regulatory services in favour of Clients; to boost and conduct academic activity and the authoring of articles; and to lead the analysis of innovative legal issues.

She is a Board Director and provides services as a Corporate & Regulatory Compliance Consultant.

Lazcano Sámano, S.C.

Juan Salvador Agraz 97, Corporativo Paragon, Office 14, Santa Fe, Cuajimalpa, 05348, Mexico City, Mexico
Tel: +52 55 5292 0065 / URL: www.lazcanosamano.com

Netherlands

Louis Jonker, Berber Bosch & Lodewijk Heinsman
Van Doorne

Trends

The Dutch government and Dutch companies are incorporating more AI (solutions) in their day-to-day activities. While the European Union and the Dutch government focus on the ethics of AI, the Dutch supervisory authorities in the financial sector, the Dutch Central Bank (DNB) and the Dutch Financial Markets Authority (AFM) focus on responsible use of AI from a more prudential perspective, safeguarding the interests of customers of financial services. In the Dutch healthcare sector, on the other hand, a continuing national debate on what is generally referred to as 'data dilemmas' mainly circles around the huge desire to improve healthcare with big data analytics and AI solutions *versus* the strict statutory rules on doctor-patient confidentiality. See more on the financial sector and healthcare sector below in the section on 'Other leading sectors in the development and/or adoption of AI'.

Focus on ethics

While fostering a competitive landscape for AI, the European Union also focuses on the ethics in AI including the 'human-centric' approach to AI that is respectful of European values and principles.[1] The Dutch government underlines the human-centred approach for AI.[2] Currently, different codes and standards are being developed by the government (such as the Code on Good Digital Public Policy) as well as private initiatives such as NLdigital (Ethical Code on Artificial Intelligence)[3] and the NEN standards committee on AI and big data (delivering input for the CEN and ISO standards). The public-private institutions' collaboration ECP recently released a code of conduct as a starting point for the development of a legal and ethical framework that can be used for the assessment of an AI application. The code of conduct is used as a guideline for establishing the framework for the published Artificial Intelligence Impact Assessment (AIIA).[4] Companies and developers may use the AIIA to identify the relevant legal and ethical standards and considerations for the deployment of AI applications.

The competitive landscape and the state of the technology

In the Netherlands, there is a collaborative spirit in the development and stimulation of AI applications. There are initiatives arising, such as the Dutch AI Coalition, where more than 65 companies, civil society organisations and research institutes work together to stimulate the use and incorporation of AI.[5] The start- and scale-ups landscape currently counts over 300 companies mainly focusing on enterprise software, health, marketing and fintech.[6] Many existing companies are also incorporating AI and seek cooperation in one of the Smart Industry field labs.

The Dutch Ministry of Economic Affairs participates in the Dutch AI Coalition. In cooperation with industry and science, the government aims to make €2bn available for

investments in AI over the next seven years. €64m have already been allocated for 2019 and, according to the State Secretary of Economic Affairs, the government has the ambition to double that contribution for 2020.[7]

Key legal issues that are arising out of adoption of AI/big data/machine learning

Data protection

One of the main challenges that arises with the deployment of AI is complying with data protection legislation. For the use of AI, data is needed. Often, this (also) concerns personal data. The General Data Protection Regulation 2016/679 (GDPR) sets strict boundaries as to what and for which goal personal data can be used. The Dutch Data Protection Authority (DPA) supervises the processing of personal data, and thus also supervises AI applications that use personal data. In this regard, the Dutch DPA released a document in which the supervision of AI and algorithms is outlined.[8]

The Dutch DPA identified the following risks that arise with the use of AI and algorithms: (i) a risk of unfair, advantageous or discriminatory outcomes; (ii) the tendency when developing and using algorithmic systems to collect as much data as possible, giving a perverse incentive to train, collect, store and further process unnecessarily large amounts of data; and (iii) the algorithm becoming a black box.

The data controller is responsible for compliance with the GDPR. The GDPR includes various instruments, such as the Data Protection Impact Assessment (DPIA) and Prior Consultation, that can be used to monitor this responsibility.[9] According to the Dutch DPA, these instruments provide sufficient guidance on how it can shape its supervision on algorithms.

Furthermore, the GDPR imposes additional requirements when automated decision making is involved (without human intervention).[10] Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject. This is in line with the 'human-centric' approach to AI currently promoted at European level.

Transparency, discrimination and bias

Another challenge of AI is providing transparency. This has been the subject of discussion in a recent Dutch court case. The case was filed due to the use of a risk analysis system (SyRI) by the Dutch municipalities to combat fraud in areas such as benefits, allowances and taxes.[11] For the risk analysis, SyRI's algorithm used data from several different government databases.

Critics of SyRI filed a lawsuit with the opinion that residents of poor neighbourhoods were suspected in advance of fraud. According to the critics, there was a lack of transparency in the algorithm, since it was unclear what data exactly caused someone to be labelled as at risk of committing fraud. What was transparent was that SyRI was predominantly used in poor neighbourhoods, which was seen as discriminatory compared to people living in other neighbourhoods.

The government argued that SyRI purely connects data from multiple databases to find irregularities, which could point to possible fraud.

The court stated that transparency, for the sake of verifiability, is important because the analysis made by SyRI carries the risk of having (unintended) discriminatory effects. Considering the large quantities of data that qualify for processing by SyRI, including sensitive personal data, and the fact that risk profiles are used, the risk arises that with the

deployment of SyRI unintended connections are made on the basis of bias (such as a lower social economic status or migration background). On the basis of the legislation regulating the deployment of SyRI it cannot be assessed if this risk is adequately addressed, due to the absence of verifiable insight into the risk indicators and the functioning of SyRI. Therefore, with regard to the deployment of SyRI, the legislation is deemed insufficiently clear and verifiable.

The court ruled that the SyRI legislation regulating the deployment of SyRI is incompatible with article 8 of the European Convention of Human Rights (ECHR). The objectives of the SyRI legislation, to prevent and combat fraud in the interest of economic welfare, were compared with the intrusion into private life that the SyRI legislation makes. According to the court, this did not meet the 'fair balance' required by the ECHR in order to be able to speak of a sufficiently justified intrusion into private life. Consequently, the SyRI legislation is in breach of article 8 ECHR (the right to respect for private life).

However, this outcome does not necessarily mean that the use of an algorithm by the government is always incompatible with article 8 ECHR. The court concluded that the SyRI legislation in its current form does not pass the test of article 8 (2) ECHR. This does leave room for future use of methods similar to SyRI, albeit with legislation that does offer a more fair balance.

The government's view with respect to the adoption of AI

The Dutch government aims to accelerate the development of AI in the Netherlands. It has adopted a strategic action plan for artificial intelligence (Dutch AI Action Plan) in October 2019. In the Netherlands, AI is already used to predict traffic jams, prevent accidents and optimise the Dutch infrastructure. Currently, research is being conducted into the possibilities of AI for defence, mainly for the 'dull, dirty & dangerous' tasks. While the Dutch government notes that the current legal framework does not sufficiently address the unique character of AI and its risks, it is of the view that the European Union will need to set out the legal framework for AI (especially regarding privacy and liability). It has also identified the need for additional safeguards for the use and adoption of AI by the Dutch government. Currently, several standards and (ethical) codes exist and are being developed (including a special edition Donald Duck to educate children about AI and human rights).[12]

The Dutch government has developed guidelines for the application of algorithmic data analysis by public authorities with safeguards relating to:[13]

i. Awareness of risks.
ii. Explanation.
iii. Data recognition.
iv. Auditability.
v. Accountability.
vi. Validation.
vii. Verifiability.
viii. Provision of information to the public.

Other safeguards will have to be regulated by law. An example is the proposal to allow the processing of sensitive personal data during the development of algorithmic models, to the extent necessary to combat discriminatory effects. In view of the prohibition on processing sensitive personal data, such an exception can only be regulated by law. Additional legal safeguards will also be implemented for data analysis by the Dutch government with regards to profiling (as defined under the GDPR) and area-specific analysis which involves the processing of personal data and risks similar to those associated with profiling. The

Dutch government has stated that the government is not allowed to use algorithms (used for automated individual decision making only) that adapt to previously obtained results without any human intervention.

Application of AI in criminal investigations

The Dutch police develops and uses AI for a limited number of uses, such as to search seized data carriers for images with image recognition to find a particular object.[14] The Dutch police is an advocate of using AI in criminal investigations. In January of 2019, the police established the National Artificial Intelligence Police at Utrecht University.[15] Through this lab, Ph.D. students and police officers conduct research into how artificial intelligence can support police work.

Currently, research is mainly conducted into software that supports people in bureaucratic processes, such as chatbots that conduct conversations with citizens, simulation techniques that study how criminal networks develop, or software in the form of 'autonomous agents' who can carry out specific tasks independently. A focus of the research is for the software to be explainable, so that for instance the judge and citizens can have insight into the workings of the software. It is emphasised that the results of these self-learning AI systems must always be assessed and monitored by people.

The Dutch police has to comply with the applicable legal framework, such as the Police Data Act. Article 25 provides that every data subject has the right of access to (information on) the personal data processed relating to him or her. The exceptions of article 27 are slightly broader than under the GDPR. Access is restricted if it would obstruct judicial investigations or proceedings or have detrimental effects on the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties. The use of AI for automatic decision making by the police – without any human intervention and specific information given to the individual – producing adverse legal effects of significantly affecting the individual is prohibited (article 7a Policy Data Act).

One of the key issues concerning the use of big data and AI in criminal investigations is the right to a fair trial (article 6 ECHR).[16] The (legal defence of) suspects in criminal proceedings must be able to access the (relevant) data used for the criminal proceedings (equality of arms).[17] The use of AI for automatic decision making should entail that the motivation of that decision is sufficiently transparent, explainable and verifiable. The Dutch government has stated that no algorithms may be used that are too complex to reasonably explain.[18]

Other leading sectors in the development and/or adoption of AI

Especially sensitive data-driven regulated industries such as the financial sector and healthcare sector have been leading the discussions on how to deal with legal issues concerning big data analytics, AI and machine learning solutions.

AI in the area of investment advice

Back in 2016, one of the first AI-related regulatory attempts was a draft Decree to amend various other Decrees based on the Dutch Financial Supervision Act, in order to tighten the regulations in the area of automated investment advice.[19] The AI-related elements of the draft Decree were, however, withdrawn at the end of 2016 and it was decided not to impose any further requirements at that time.

This proved to be a mere delay. With the implementation of MiFID II[20] in the Dutch Financial Supervision Act, which entered into force on 3 January 2018, and the MiFIR[21] having entered into force on the same date, significant changes were introduced in investor protection

regulation that also impact automated investment advice. Especially for retail clients, reference is made to the ESMA Guidelines on certain aspects of the MiFID II suitability requirements,[22] the guidelines of which are applied by the Dutch Financial Markets Authority (AFM) when monitoring compliance with the Dutch Financial Supervision Act. These ESMA Guidelines require investment firms, amongst others, to provide their clients with a very clear explanation of the exact degree and extent of human involvement and if and how the client can ask for human interaction, but also with a description of the sources of information used to generate automated investment advice. In order to ensure the consistency of the suitability assessment conducted through automated tools, investment firms should also regularly monitor and test the algorithms that underpin the suitability of the transactions recommended or undertaken on behalf of clients. And when employing automated tools, investment firms should furthermore ensure that their staff involved in the activities related to the definition of these tools: (a) have an appropriate understanding of the technology and algorithms used to provide the advice (in particular, they are able to understand the rationale, risks and rules behind the algorithms underpinning the digital advice); and (b) are able to understand and review the automated advice generated by the algorithms.

Besides amended investor protection regulations, MiFID II and MiFIR also introduced closer regulation and monitoring of algorithmic trading and high-frequency algorithmic trading, including a duty to notify the Dutch Financial Markets Authority (AFM).

AI in the insurance sector

The Dutch insurance sector has also shown an increasing eagerness to adopt AI. Various Dutch insurers already use different types of machine learning applications in their processes. Some of the commonly used techniques are clustering, random forests, gradient boosting and deep neural networks. Also, Natural Language Processing (NLP) techniques are used, though primarily for back-office tasks such as in customer contact through virtual assistants.

To ensure insurers use AI responsibly, the Dutch Financial Markets Authority (AFM) and the Dutch Central Bank (DNB) published their joint exploratory study on AI in the insurance sector on 25 July 2019.[23] According to AFM and DNB, "*it is important that insurers, from the start, systematically define the restrictions in the use of AI and take its technical aspects into consideration. Knowledge of AI needs to be embedded within all levels of the organisation along with internal policies for its use. This must be anchored in clear governance structures. These are prerequisites for deploying AI responsibly and for triggering critical questions throughout the development and deployment stages*". Furthermore, AFM and DNB emphasise the importance of the social context in which AI is deployed (in terms of consumer behaviour and social acceptance). Finally, the potential negative impact of AI on the Dutch solidarity principle between groups of insured consumers has been identified. This all brought AFM and DNB to put forward 10 key considerations for the use of AI in the insurance sector, which are intended to serve to stimulate awareness among insurers and to help to encourage a meaningful dialogue.

AI in the financial sector in general

On the same date the joint exploratory study on AI in the insurance sector was published (25 July 2019), the Dutch Central Bank (DNB) also published its General principles for the use of AI in the financial sector.[24] These principles are divided over six key aspects of responsible use of AI, namely (i) soundness, (ii) accountability, (iii) fairness, (iv) ethics, (v) skills, and (vi) transparency (or SAFEST). From a prudential perspective under the Dutch Financial Supervision Act, soundness is DNB's primary concern. According to DNB, AI applications in the financial sector should in this respect be reliable and accurate, behave predictably, and operate within the boundaries of applicable rules and regulations.

Although, strictly speaking, these principles are not binding on market parties, they do serve as a starting point for DNB's supervision of the use of AI by supervised financial institutions, as DNB confirmed on 13 February 2020 in its position paper for a hearing/roundtable discussion on 17 February 2020.[25] It is safe to say that DNB needed to transform these principles into (unofficial) rules of law, as Dutch financial institutions are also working hard on developing and adopting algorithms. In this respect, for example, Dutch banks show a higher level of resilience compared to neighbouring countries. Because Dutch society embraces innovation relatively quickly, AI innovations find a good breeding ground in the Netherlands, although Dutch people remain wary of privacy issues.

AI in the healthcare sector

In the Dutch healthcare sector, the adoption of AI is a hot topic too, whether on a patient level or more in the area of population management. Besides, of course, applicable regulations on medical devices (currently still based on the Dutch Medical Devices Act[26] as an implementation of the EU Medical Devices Directive,[27] but as of 26 May 2020 based on the EU Medical Devices Regulation[28]) and all certification issues due to Brexit, the main discussion in the Netherlands concerning big data analytics and/or AI is about the need to share medical data *vs.* doctor-patient confidentiality.

Dutch healthcare providers are obliged to keep their patients' medical data confidential (article 7:457 sub 1 Dutch Civil Code). They may only share it with other healthcare providers that are directly involved in your treatment, or with temporary replacement providers in a confidential manner (article 7:457 sub 2 Dutch Civil Code). For any other data sharing, the patient's explicit consent is required. There is a statutory exemption for statistics or scientific research in the area of public healthcare (article 7:458 Dutch Civil Code), as well as a general 'conflict or rights' exemption, but these do not benefit third-party AI providers. And even if consent is provided to the healthcare provider that shares the patient data, this does not automatically mean that the receiving AI provider may use said patient data for analytics, algorithm development, machine learning, etc. The AI provider's processing activities will be subject to the GDPR[29] and the Dutch GDPR Implementation Act.[30] In those situations where the AI provider (also) wants to process the data received for its own purposes, which will anyway be the case with all intelligent self-leaning algorithm and machine/deep learning solutions, this will inevitably end up in a new consent requirement.

Taking into account the European Commission's recent European Strategy for Data,[31] which promotes data sharing in healthcare, and the upcoming review of the GDPR, changes may be expected in data protection regulations in this respect.

Ownership/protection

Copyright

In the Netherlands, legal protection of computer programs is regulated by Directive 2009/24/EC (the Software Directive). The Software Directive states in its recitals that algorithms are not protected *as far as* they are 'built up' out of ideas and principles (which in themselves cannot be copyright-protected).[32] A complex mathematical algorithm, however, could be protected under the Dutch Copyright Act (DCA). The algorithm must go beyond an existing mathematical or logical formula and possess its 'own original character and the personal mark' of the creator to be protected under the DCA.[33]

More of interest, and becoming more relevant, is the question of who the owner is of a work *made* by AI. Especially since AI solutions seem to be getting (more) capable of creating their own creative works.[34]

The DCA does not provide for copyright protection for works created by an AI application. Case law stipulates that a work must have its own original character and bear the personal mark of its creator to be granted copyright protection.[35] Furthermore, a work should be the result of creative human labour and creative choices, as a product of the human mind.[36] Legislation and case law stipulate that only works created by humans can be protected under Dutch copyright law.

Patents

Under the Dutch Patents Act 1995, patents are granted for inventions, for all fields of technology, if they are new, involve an inventive step, and are capable of industrial application.[37] A patent can thus be seen as an incentive for an inventor to innovate and invent. When an AI system is doing the inventing, it could be questioned if it will still be necessary to grant patents.[38]

While an AI system could invent something that is new and capable of industrial application, the question arises whether it is still possible to qualify an invention by an AI system as an inventive step. The standard for an 'inventive step' is that the invention should objectively contribute to the state of the art.[39] How it contributes to the state of the art is irrelevant, the end result is what matters. Furthermore, the invention should not be obvious to *the average craftsman*.[40] Considering these conditions, Dutch patent law leaves the possibility open to grant patents for automated inventions or inventions made by an AI application.

A consequence of AI developing more and getting 'smarter' could be that the capabilities of the average craftsman may rise (or the computer of the average craftsman), since inventions can become more obvious the smarter AI applications get.[41]

There is the question of who can claim the rights to the patent of an invention created by an AI application. Under the current legal framework, the AI system cannot hold the patent itself. The applicant for the patent is the rightsholder under the Patent Act 1995.[42]

Trade secrets

Technology, algorithms and AI can also be protected under the Dutch Trade Secrets Act 2018. Obtaining trade secrets is unlawful without permission of the holder of the trade secret. Trade secrets are information that (i) is secret in the sense that the information is not, as a whole or in the precise composition and arrangement of its components, generally known among or readily accessible to those within the circles normally dealing with that type of information, (ii) has commercial value because it is secret, and (iii) is subject to reasonable measures, given the circumstances, by the person who lawfully disposes of it, to keep it secret. Companies have to ensure that their trade secrets are actually kept secret in order to qualify for protection.[43]

Antitrust/competition laws

The Dutch AI action plan (SAPAI) states that in order to be a leader in AI, the (Dutch) markets have to be competitive. In practice, this entails that AI applications need to be developed by more than a handful of large companies.

Currently, many online platform markets, where AI is widely applied, consist of a few large companies with a big market share.[44] This is partly due to network effects (reinforced by data), economies of scale and synergy. The dominant positions for one or a few platforms, combined with self-reinforcing AI processes, can make it increasingly difficult for other platforms to challenge that position.

Large platforms can grow more easily than new entrants in terms of data, computing power and algorithms. Taking this into consideration, and the access to capital and highly educated staff, a limited number of companies are probably better able to develop their

(already relatively high quality) AI than upcoming competitors. The different volume of data platforms possess could become an entry barrier, or have the consequence that a large company can force unreasonable conditions upon other companies that wants to use its data or algorithms.[45] Even though the government considers this to be undesirable, they do acknowledge that considering efficiency and opportunities for innovation, the concentration of users around one or a few platforms can also be beneficial.[46]

Article 6 of the Dutch Competitive Trading Act forbids all agreements between companies which have as their object or effect to restrict or distort competition in the Dutch market (or in part of it). Article 24 forbids the abuse of significant market power. The Dutch government advocates that a European Supervisory Authority must further explain how the competition rules in the Treaty on the Functioning of the European Union and in articles 6 and 24 of the Dutch Competitive Trading Act should be interpreted in the digital economy.

To combat possible future issues, the government advocates that a European supervisor, in addition to competition laws, should be able to impose *ex ante* obligations on large platforms with a gatekeeper function; consumers and entrepreneurs being heavily dependent on it. The Dutch Competition Authority has also pledged to be extra alert to situations where large online platforms have unfair terms of access to the platform.[47]

Changing market conditions

The Dutch AI action plan states that because of the wider use of AI, an algorithm can be used to quickly adjust pricing to changing market conditions. This could develop into a new form of cartel: AI could be used to implement cartel agreements, and the risk of tacit collusion could increase when many companies use similar algorithms.

These new types of abuse will probably be harder to prove. Especially since it is difficult to ascertain whether it could (also) be qualified as parallel market behaviour, which is not prohibited under Dutch competition law. There are no precedents or similar cases which can be relied upon.

Netherlands Authority for Consumers & Markets (ACM)

The ACM has a dedicated team with expertise on new technologies and their effects on competition, such as AI-driven platforms, the use of algorithms and app stores. The ACM has identified that in almost all sectors, companies are making increasing use of algorithms and AI. This can contribute to faster production processes, more efficient logistics or more personalised selections and offers. However, there can also be risks for people; for example, by the possibility of discrimination.[48]

In its agenda for 2020, the ACM stated that it will pay special attention to the use of (self-learning) algorithms by companies. The ACM will start exploratory research into the use of algorithms and publish a working paper on mechanisms by which self-learning algorithms can achieve supra-competitive prices. Furthermore, the ACM will publish a working paper on how they will research algorithms in a practical sense.[49]

Recently, the ACM released a guidance paper for the protection of the online consumer, in which the (ab)use of algorithms to mislead consumers is considered.[50] This can help companies that use AI and/or algorithms to design their application accordingly. Some relevant guidelines are that companies must tell consumers of the use of an algorithm and explain how the algorithm is used. The algorithms should also comply with relevant consumer regulations. This should be tested and monitored by the company, as the company is responsible for its algorithm.

Endnotes

1. European Parliament, EU guidelines on ethics in artificial intelligence: context and implementation, September 2019.
2. Dutch Minister of Internal Affairs and Kingdom Relations, letter to the Dutch House of Representatives, 8 October 2020 (reference number 26643, nr. 642).
3. https://www.nldigital.nl/wp-content/uploads/2020/01/Ethische-code-AI-NLdigital-English.pdf.
4. https://ecp.nl/wp-content/uploads/2019/01/Artificial-Intelligence-Impact-Assessment-English.pdf.
5. https://nlaic.com/over-nl-aic/#en.
6. StartupDelta, Artificial Intelligence in The Netherlands – Startup Report 2018, 2018.
7. https://nos.nl/artikel/2305235-kabinet-wil-kunstmatige-intelligentie-aanjagen-met-2-miljard-euro.html.
8. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf.
9. Articles 35 and 36 GDPR.
10. Article 22 GDPR.
11. District Court of the Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.
12. Dutch Minister of Internal Affairs and Kingdom Relations, letter to the Dutch House of Representatives, 8 October 2020 (reference number 26643, nr. 642) and *Donald Duck duikt in de digitale wereld*.
13. Dutch Minister of Internal Affairs and Kingdom Relations, letter to the Dutch House of Representatives, 8 October 2020 (reference number 26643, nr. 641).
14. Dutch Minister of Justice and Security, letter to the Dutch House of Representatives, 18 February 2020 (reference number 2829671).
15. https://www.politie.nl/nieuws/2019/januari/16/%E2%80%98kunstmatige-intelligentie-vergroot-onze-slagkracht.html.
16. B.W. Schermer, J.J. Oerlemans, *AI, strafrecht en het recht op een eerlijk proces*, Computerrecht 2020/3.
17. Dutch District Court of Amsterdam, 19 April 2018 (ECLI:NL:RBAMS:2018:2504).
18. Dutch Minister of Justice and Security, letter to the Dutch House of Representatives, 18 February 2020 (reference number 2717062).
19. *Consultatiedocument Wijzigingsbesluit financiële markten 2017* (Consultation document Financial Markets Amendment Decree 2017), https://www.internetconsultatie.nl/wijzigingsbesluitfm2017/document/2401.
20. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.06.2014).
21. Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014).
22. *Guidelines on certain aspects of the MiFID II suitability requirements*, Final Report, European Securities and Markets Authority, 28.5.2018 (ESMA35-43-869).
23. *Artificiële Intelligentie in de verzekeringssector - een verkenning*, De Nederlandsche Bank (Dutch Central Bank) & Autoriteit Financiële Markten (Financial Markets Authority), July 2019; an English version with the title "Artificial intelligence in the insurance sector - an exploratory study" was published in December 2019.
24. *General principles for the use of Artificial Intelligence in the financial sector*, De Nederlandsche Bank (Dutch Central Bank), 2019.

25. *Position Paper DNB t.b.v. hoorzitting/ rondetafelgesprek 'Wettelijk kader en toezicht' d.d. 17 februari 2020*, De Nederlandsche Bank (Dutch Central Bank), 13.2.2020 (A034-1175186779-161).
26. *Wet op de medische hulpmiddelen* (Medical Devices Act), *Staatsblad* (Official Gazette) 1970, 53.
27. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.07.1993).
28. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017).
29. 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, 04.05.2016; cor. OJ L 127, 23.5.2018).
30. *Uitvoeringswet Algemene verordening gegevensbescherming* (GDPR Implementation Act), *Staatsblad* (Official Gazette) 2018, 144.
31. *A European strategy for data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19.2.2020, COM(2020) 66 final.
32. Recital 11.
33. ECLI:NL:RBARN:2008:BD7578.
34. https://www.christies.com/features/A-collaboration-between-two-artists-one-human-one-a-machine-9332-1.aspx.
35. Dutch Supreme Court 4 January 1991 (ECLI:NL:HR:1991:ZC0104), Dutch Supreme Court 24 February 2006 (ECLI:NL:HR:2006:AU7508).
36. Dutch Supreme Court 30 May 2008 (ECLI:NL:HR:2008:BC2153).
37. Article 2 Dutch Patent Act 1995.
38. Blok, P.H. (2018). *Echte rechten voor kunstmatige creaties – moeten we octrooien blijven verlenen als slimme systemen het uitvindwerk overnemen?* Amsterdam: Delex.
39. Article 4 Dutch Patent Act 1995.
40. Article 6 Dutch Patent Act 1995.
41. Blok, P.H. (2018). *Echte rechten voor kunstmatige creaties - moeten we octrooien blijven verlenen als slimme systemen het uitvindwerk overnemen?* Amsterdam: Delex.
42. Article 8 Dutch Patent Act 1995.
43. Under the Databases Act of 1999, data (content) of an AI application could also be protected if it qualifies as (i) a collection of works, data or other independent elements, (ii) systematically or methodically arranged, and (iii) a substantial investment.
44. E.g. Facebook, LinkedIn, etc.
45. Dutch AI Action Plan.
46. Dutch AI Action Plan.
47. https://www.acm.nl/nl/organisatie/missie-en-strategie/onze-agenda/acm-agenda-2020-2021/digitale-economie.
48. https://www.acm.nl/nl/organisatie/missie-en-strategie/onze-agenda/acm-agenda-2020-2021/digitale-economie.
49. https://www.acm.nl/sites/default/files/documents/2020-01/werkzaamheden-acm-in-2020.pdf.
50. https://www.acm.nl/sites/default/files/documents/2020-02/acm-leidraad-bescherming-online-consument.pdf.

Louis Jonker
Tel: +31 20 6789 510 / Email: jonker@vandoorne.com

Louis Jonker is a leading expert in law and technology. Besides assisting clients in IT and Outsourcing projects, Louis focuses on legal issues and strategic partnerships concerning (disruptive) technologies and innovations in the financial industry (FinTech, Digital Payments) and healthcare industry (Digital Health, HealthTech).

Furthermore, Louis is engaged actively in addressing the legal issues and challenges in the areas of Cloud, Blockchain, Electronic Identification and Authentication, Artificial Intelligence and Robotisation, with regard to contracts as well as compliance issues.

Louis is a frequent speaker at national and international conferences and seminars, and he teaches at Tilburg University and Nyenrode Business University. Furthermore, Louis is very active in industry associations (e.g. Holland FinTech and Sourcing Netherlands).

Berber Bosch
Tel: +31 20 6789 235 / Email: bosch@vandoorne.com

Berber Bosch is a talented IT lawyer who drafts, advises and litigates on any type of agreement or other commercial arrangement, as long as there is a technology component to it. She especially likes to immerse herself in complex legal issues concerning innovative technologies, including in the areas of HealthTech, Blockchain and AI.

Berber holds a Bachelor's degree in Law from the University of Amsterdam and studied at the Freie Universität in Berlin. She obtained a Master's degree in Information Law at the Amsterdam Institute for Information Law (IViR) and undertook the Master's programme of Law & Technology at the Tilburg Institute for Law, Technology and Society (TILT).

Besides being a member of Van Doorne's IT Team, Berber was also a member of Van Doorne's Dispute Resolution & Insurance Law Team.

Lodewijk Heinsman
Tel: +31 20 6789 520 / Email: heinsman@vandoorne.com

Lodewijk Heinsman recently joined Van Doorne's IT Team, where he primarily assists clients with IT transactions, contracts and disputes in the broadest sense. During a previous internship with Van Doorne's Research & Development Team he was quite actively involved in developments in the area of LegalTech, including with moderating roundtables on this topic.

Lodewijk holds a Bachelor's degree in Law from Utrecht University and obtained his Master's degree in Law & Technology at the Tilburg Institute for Law, Technology and Society (TILT).

Van Doorne

Jachthavenweg 121, 1081KM Amsterdam, Netherlands
Tel: +31 20 6789 123 / URL: www.vandoorne.com

Portugal

Nuno da Silva Vieira & Daniela Guimarães
Antas da Cunha Ecija & Associados, Sociedade de Advogados, R.L.

Trends

Portugal has advanced significantly in the implementation of Artificial Intelligence (AI). In fact, this year, the Portuguese Government presented a plan for digital transition that aims to develop a structured approach to invest in innovation, seeking to put Portugal at the forefront of the fourth industrial revolution and enhance the positive impact that digitalisation and technology have in promoting social and economic progress. This Action Plan is the engine of the country's transformation, with the purpose of accelerating Portugal, without leaving anyone behind, and raising the status of the country in the world. To this end, it is based on three main pillars of action, developing in an integrated manner a set of measures that seek to articulate the various synergies and sectoral policies: training and digital inclusion of people; the digital transformation of the business fabric; and the digitisation of the State. It also implements the Portugal Digital Mission Structure, as the main structure to support the development and implementation of government policy in digital matters and establishes the general principles for the creation and regulation of Technological Free Zones that allow the elaboration of a legislative framework that promotes and facilitates the realisation of research, demonstration and testing activities, in the real environment, of technologies, products, services, innovative processes and models in Portugal.

At the same time, the country is still implementing the "National Strategy for Artificial Intelligence" – "AI Portugal 2030". Portugal is showing good results in some innovation indicators (including but not limited to AI), although in many of them we have been typically placed below the average of the European Union. Portuguese institutions are particularly well positioned in terms of international research collaborations, broadband penetration and product/process innovations in Small and Medium-sized Enterprises (SME). Portugal has been relatively successful as an innovation-friendly environment and has an attractive research system. By 2030, Portugal will have a knowledge-intensive labour market with a strong community of forefront companies producing and exporting AI technologies supported by an academia involved in high-level, fundamental and applied research. AI technologies will be easily available to promote the efficiency and quality of all activities, including SMEs, public services and every citizen. The labour force will be highly qualified, and Portugal will be at the forefront of AI education for all. AI will improve the quality of services and the efficiency of processes while guaranteeing fairness, wellbeing and quality of life. The country has strong players in some areas that may serve as inspiring examples and help drive innovation and research, such as: (1) Natural Language Processing; (2) Real Time Decision Making with AI; (3) AI for Software Development; and (4) AI for Edge-computing.

Ownership/protection

In the European Union, software is not protected by patent or by a special form of protection, as we sometimes hear in discussions on the subject. Much has been debated about these two possibilities. However, Directive 91/250/EEC of 14 May on the legal protection of computer programs has stated that Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works, which provides that the term 'computer program' shall include their preparatory design material. It should be noted that the discussion about the patentability of software remains in some countries (as is the case in the United States) and that there are exceptions. In Portugal, the INPI (*Instituto Nacional da Propriedade Intelectual*) admits, for example, the hypothesis of patent registration of a computer program if that software reveals itself to be strictly technical and essential to the execution of an invention.

Implementation of AI/big data/machine learning into businesses

Numbers from 2017 show that Portugal has a shortage of qualified human resources in advanced technological areas, mostly in terms of higher education (67% of the EU average in 2017) but also in lifelong learning (88.8%) and new PhDs (94%). Employment in knowledge-intensive activities is low (57%) but it is slightly above average in fast-growing enterprises (103.2%). Since 2017, things have improved and, every year, a larger number of qualified professionals have entered the professional market. As such, the slice of employment of fast-growing companies in the most innovative sectors has been improving. The R&D expenditure of the business sector has considerably improved since 2015 and represents about 52% of gross expenditure in R&D. SMEs are doing quite well in innovations in the product or the process (158.8%) and in marketing/organisation levels (112%). Things are improving as qualification and specialisation are the main keys to Portugal's strategy up to 2030.

Civil liability

Traditionally, the Portuguese justice system has been averse to the introduction of AI tools, machine learning or data collection tools. However, in Portugal we have seen a change in the last couple of years, especially in the areas of consumer protection and industrial property law. Concerning consumer protection, Portugal has, obviously, implemented Regulation (EU) 524/2013 of 21 May 2013, which creates a mechanism of online resolution of consumer disputes. The Online Dispute Resolution (ODR), as it is called, is a platform provided by the European Commission to allow consumers and traders in the EU or Norway, Iceland, and Liechtenstein to resolve disputes relating to online purchases of goods and services without going to court. Speaking of Industrial Property Law, most of the Portuguese private mediation centres use online platforms to solve the matters with which they are confronted. On the other hand, the country has also implemented the eIDAS Regulation (Regulation (EU) 910/2014) and 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.

Criminal issues

At this point, the most important use for AI and machine learning tools in the Portuguese criminal system concerns the fight against cybercrime. On this topic, there is special legislation – specifically Law 109/2009 of 15 September 2009 (Cybercrime Law), which sets out the activities of and punishments for informatic fraud, illegal access to information

systems, illegal data interference, informatic sabotage and illegal interception of data. Portugal also abides by Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. The Portuguese investigation authorities use the most sophisticated AI tools to collect specific data and proof in these matters.

National security and military

Portugal recognises the need to have modern Armed Forces, well-equipped, trained and ready to efficiently carry out their missions, whether in areas under sovereignty, jurisdiction or national responsibility, or beyond its borders. For that reason, Ministry of Defense Order No. 4101 of 2018 introduced a set of recommendations. In anticipation of all trends, the Portuguese Ministry of Defense will invest in new research and development projects to monitor the impact of digital evolution on military capabilities, giving a very clear priority to unmanned autonomous systems, robotics and AI which, at present, but especially in the foreseeable future, are revolutionising methods of combat. On the other hand, in the medium and long term, climate change will have an impact on the security and defence of States, and on protecting citizens, and must also be taken into account in the employment scenarios of the Armed Forces in light of what now begins to be designated as Green Defense.

Nuno da Silva Vieira
Tel: +351 926 850 733 / Email: nvieira@adcecija.pt

Nuno da Silva Vieira (born in 1980), Partner at Antas da Cunha Ecija & Associados, Sociedade de Advogados, R.L. Graduated in Law from the University of Minho Law School (2003). Member of the Portuguese Bar Association since 2006. In 2012, he founded Vieira Advogados, a law firm that introduced itself as a Legal Startup and operated from Braga until 2019, when it merged with Antas da Cunha Ecija & Associados. He has published several books devoting his time, also, to giving conferences, courses and lectures in the areas of commercial law, compliance and digital law. Attended an MBA (2016/2018) at AESE Business School, in partnership with the IESE Business School of the University of Navarra. In 2017 concluded the IESE – Business School Innovation and Entrepreneurship program in New York City, considered by the *Financial Times* that year to be the best executive-trained business school in the world. In 2018 he was considered one of the 40 most promising Portuguese leaders under the age of 40, an initiative of Expresso and the Forum of Business Managers and Administrators.

Daniela Guimarães
Tel: +351 915 279 009 / Email: dguimaraes@adcecija.pt

Daniela Guimarães (born in 1991), Senior Associate at Antas da Cunha Ecija & Associados, Sociedade de Advogados, R.L. since 2020. Daniela received her Law Degree from the School of Law of the University of Minho. Postgraduate in European Union Law from the same school and also in International and European Economic Criminal Law from the Faculty of Law of the University of Coimbra. She also attended courses in International Criminal Law at the University of Salzburg in Austria and Advanced European Law at King's College London in the United Kingdom. From 2013 to 2014, she was President of ELSA Portugal – The European Law Student's Association, a European association with presence in over 40 countries. She began her career at Magellan – European Affairs Consulting, with offices in Porto and Brussels, as a consultant. Collaborated with Vieira Advogados from 2015 to 2020. Since 2013 she has been a member of CEDU – Center for Studies in European Union Law at the University of Minho. Preferred practice areas are Financial Litigation, European and International Union Law, Regulation and Policy Making.

Antas da Cunha Ecija & Associados, Sociedade de Advogados, R.L.

Avenida Fontes Pereira de Melo, n.º 6, 2.º andar, 1050-121 Lisboa, Portugal
Tel: +351 213 192 080 / URL: https://adcecija.pt

Romania

Cristiana Fernbach & Cătălina Fînaru
KPMG – Toncescu și Asociații S.P.A.R.L.

Trends

As specific laws regarding artificial intelligence ("AI") have not yet been adopted, and all EU Member States have a large interest in AI and new technologies, such States are on their way to finding the right united approach to regulation and use.

Although AI technology has raised many concerns, it is a great innovation that may boost economies and bring many benefits to humankind.

The Romanian digital transformation landscape looks far more different this year. Besides the creation of a Romanian Association for Artificial Intelligence, over 13 Romanian Universities and research institutes work on AI-related topics. Regarding the ongoing projects of the Romanian academic ecosystem, it is worth mentioning: CoRoLa (reference electronic corpus of the contemporary Romanian language); CAMI (AI ecosystem for self-management and sustainable quality of life); UP Drive (researches automated urban parking and driving); and ROBIN (project that develops cognitive systems for personal robots and autonomous vehicles).[1]

AI is a field of interest not only for the Romanian Government and public institutions, but also for the private sector, where start-ups in the field are becoming more numerous and popular.

A national strategy for AI shall consider funding AI research in academia, the improvement of collaboration between companies and technological transfer on AI-related development, how to boost AI by national initiatives in industry and other economic sectors of the Government and how to create more places to grow skills and perform networking within industry.[2]

As things are evolving very fast in terms of technical development, the adoption of appropriate amendments to the existing legal framework (e.g. on consumer protection, on product liability) and of a new regulatory framework for AI on the national level is a matter of urgency. As of the resolution of the European Parliament of 12 February 2019[3] on a comprehensive European and industrial policy on AI and robotics, the Member States should follow five principles in developing a national legal framework: create an internal market for AI; respect personal data and privacy; provide rules for liability; consider consumer protection and empowerment; and provide specific provisions on IP rights in case of robotics. A further dimension to be taken into account in designing the new AI legal framework is ethics. Aspects such as the development of human-centric technology, embedded values in technology, decision-making – limits to the autonomy of artificial intelligence and robotics – and last but not least, transparency and algorithmic governance have to considered by the law makers.

Regarding the industry sectors most active in Romania in the adoption of AI for automation of business processes, we can name the retail, telecom, banking and insurance, healthcare and, as the rising star, transportation and logistics industries.

Ownership/protection

Not so long ago, human interaction and activities like playing chess could only be carried out by humans; but due to the evolution of AI, even more activities are now routinely performed by machines.

As we can see today, AI is not just for the tech, automotive, and transportation industries. Researchers are working on many more applications of AI which will revolutionise the ways in which we study, work and communicate. AI systems are already touching all industries and will actively contribute to the digitalisation of the modern world.

The rapid evolution of AI will lead to the development of AI that is capable of learning without being specifically programmed by a human. In this case, one could ask whether AI may be considered a legal person or a "new person".

From a legal perspective, one of the most challenging aspects of AI refers to the copyrights recognised by the law in regard to the AI algorithm, as well as in regard to the results of using AI. According to the law, intellectual property rights are the rights given to persons over their own creations, which give the creator an exclusive right over the use of the creation for a certain period of time.

Romanian Law no. 8/1996 regarding copyright ("Law no. 8/1996") recognises and guarantees copyright for the natural person who created the literary, artistic or scientific work or any similar work of intellectual creation. The same protection is guaranteed to the author of a computer program, which includes any expression of a program, application programs and operating systems expressed in any kind of language, whether in source code or object code, or the preparatory design material and manuals. In the case an AI algorithm is created by one or more employees in the course of their duties or on instructions from their employer, the economic rights in computer programs belong to the employer.

According to Law no. 8/1996, the author may conclude an agreement for the use of a computer program in which the user of such program is granted the non-exclusive right to use the program, but may not transfer the right to use the program to another person. The transfer of the right to use a computer program does not imply the transfer of the copyright related to it. In other words, if a company owning the economic rights to an AI algorithm concludes an agreement with another company for the use of the AI algorithm, the developer company still remains the owner of the copyright to the algorithm.

Moreover, the issues relating to ownership in the field of AI can become even more complex, as long as AI is able to engage in the act of creation or in creating innovative solutions that may be subject to patent law. For this specific type of AI, the important point to note is that the developer sets the parameters for the work generated by the AI.

In order to be protected by copyright law, creative works must be original. This requires the intervention of a human author. Romanian law, like in many other European jurisdictions, establishes that copyright law only regulates works created by a human author.

In this context, two scenarios may be realised: (i) copyright protection is denied for works that have been created by AI; or (ii) copyright protection for works that have been created by AI may be attributed to the developer or to the user of the AI.

In the first scenario, the works that have been created by AI may not be protected by copyright and could be freely used because they are not created by a human author. Moreover, the Court of Justice of the European Union ("CJEU") stated in its *Decision C-5/08 Infopaq International A/S v Danske Dagblades Forening* that copyright applies only to original works, and that originality shall reflect "the author's own intellectual creation".[4]

It is worth mentioning that the second scenario is recognised by United Kingdom legislation and other worldwide legislation.

Romanian legislation does not address this specific copyright ownership issue for works that have been created by AI, but it is clear about the fact that legislation must be adapted to the new digital environment, especially the legislation imposed by the Copyright Directive. It will be very interesting to see if Romanian legislation will adopt one of the scenarios mentioned above.

Another legal aspect which is not yet regulated by Romanian legislation regards the criteria to be followed in determining liability for copyright infringement by AI in the process of creation.

The legislation regarding liability will address this legal issue in detail, and will take into consideration the fact that the evolution of AI will likely result in a high degree of autonomy for AI, and that it will be very hard to identify the person responsible for an infringement by AI in the process of creation.

Even if Romanian law regulates the copyright of the author of a computer program in which an AI algorithm may be included, the fast evolution of AI imposes the need for new and more applied legislation, which should consider both the developer of AI and its user.

In the near future, Romanian legislation will be able to address the legal issues raised by creating and using AI. The first step in updating the Romanian legislation relating to IP is the harmonisation of the Copyright Directive into national legislation, addressing at least the following aspects:

- Who is the author of the creation resulting from the use of AI?
- Who is liable if AI infringes copyright in the creation process?

Antitrust/competition laws

The development of different types of AI and the extensive use of big data has started to shape a new view of the digital market, and directly influences competition law.

One of the most used applications of AI and which creates controversy is the pricing algorithm or pricing bots, whose sole purpose is to maximise profits by automatically setting the prices of one particular product or service. By using machine learning technology, this kind of algorithm can analyse large amounts of data and is able to optimise the pricing policies implementing continuous price changes, largely known as "dynamic pricing".

Dynamic pricing is considered to improve market efficiency by allowing companies to react instantaneously to changes in supply conditions as well as to fluctuations in market demand, but it is also considered to be challenging for non-algorithmic sellers that cannot compete. Moreover, dynamic pricing challenges consumers, because in order to make decisions under constant price fluctuations, they also need to use algorithms to facilitate decision-making.[5]

Using AI with price-setting algorithms could cause them to collude among themselves without any formal agreement or human interaction, to the detriment of consumers.[6] The problem in this particular case is that the applicable legislation does not cover the issue of what can be seen as evidence in order to prove the existence of collusion. If such case occurs, the competent authority must prove the so-called "meeting of minds" between the parties.

According to the CJEU's case law, an agreement within the meaning of Article 101 TFEU (which regards all agreements between undertakings, decisions by associations of undertakings and concerted practices) requires the existence of a concurrence of wills between competitors with the intention to restrict competition, and that the parties' need to

feel bound by the said agreement constitutes the faithful expression of the parties' intention.[7] In the case of algorithm collusion, it is very hard to prove a supposed agreement, because what would constitute evidence of collusive activity is unclear in an environment where algorithms are making autonomous decisions and there is no record of pricing decisions.

Even if the collusive activity is somehow proven, another issue is the one that addresses liability in such cases. Because the algorithms are designed by people, one can say that the creator is liable. In fact, the antitrust liability in the digital market field is more complicated than it seems. Firstly, there is no legal provision that establishes the criteria for the liable person: it can be the creator of the algorithm or the user of it. Secondly, there are circumstances that influence liability, such as: the ability to constrain AI; and the relationship between humans and computers. Thirdly, liability is influenced by the levels of technological development and use of computer algorithms. For example, if the algorithm uses deep learning technologies, where human intervention is not necessary, it is very hard to assign liability to a certain person.

Besides the issues of machine collusion, another important problem that needs to be considered is the impact of big data on the digital economy. Big data can provide a consistent market power to undertakings, and possibly to the one which has the dominant position to misuse it. Issues like abuse of dominance or merger control are constantly in the attention of the antitrust authorities worldwide.

Even considering the constantly changing legal framework, new technology has clear benefits. Businesses that use price algorithms may increase price transparency, which will help both businesses and consumers to buy products at the lowest cost.[8] Using big data will help consumers to have greater market transparency, by allowing them to more easily compare prices or characteristics of competing goods or services.

Fast technological developments, some of which are mentioned above, demand upcoming changes in Romanian antitrust law. Although it will take some time to update the current regulations, the Romanian Competition Council ("RCC") has already started to adjust to the new economic environment and to the digital market. For example, the RCC is implementing a big data information system with the objective of integrating and exploiting large volumes of data in order to support investigative activities, develop a preventive function, and detect and take action specific to the activity of the RCC.

The system will provide the RCC with a tool to assist the investigative process, using specialised tools to retrieve, visualise, analyse, collaborate, corroborate, alert and report. These new capabilities are meant to help in five areas of investigation and analysis, which are: fraudulent auctions; cartel screening; structural and trade links between enterprises; sector-specific inquiries; and economic concentration.

Besides the implementation of the aforementioned project, the RCC continued to develop an analytical tool indicator, the Aggregate Index of Competitive Pressure ("AICP"), a project which began around six years ago.

The AICP functions as a primary screening or diagnostic tool to show the extent to which the national industries reviewed are approaching an ideal situation which fully facilitates free competition. Also, using this screening indicator aligns the RCC with the popular trend among competition authorities to proactively tackle competition policy.

Board of directors/governance

The continuous development of AI and big data also influences companies' governance systems, which need to be updated in line with the latest technologies. The roles and

responsibilities of the Board members must adjust to the technologies that can be used to help such members carry out their duties.

Romanian law provides that a director's powers are established by the shareholders in the company's articles of incorporation. Their activity mainly consists of carrying out all acts which are necessary and useful in fulfilling the company's object of activity. In practice, this translates to the following tasks: reviewing and guiding corporate strategy; setting performance objectives; selecting, compensating, monitoring and, when necessary, replacing key executives; dealing with financial and operational control; and assuring compliance with the applicable legal provisions.

Regardless of the different types of tasks of the directors or managers, it is possible that some of this activity can be taken over by AI. Depending on the degree of autonomy, there are three different types or levels of AI roles: assisted AI; advisory AI; and autonomous AI.[9]

If companies decide to integrate AI and big data in their governance systems, they need to consider beforehand an assessment to analyse the impact and the expected result of such integration. It is recommended that a company should make audits or tests in order to verify if AI is accurately interpreting data.

After deciding to integrate AI, it is recommended that at least one ethical expert should be a member of the Board in order to supervise how the AI deals with its tasks, and to make sure that no ethical principles are being violated. This change itself requires the updating of the organisational chart and issuing policies and procedures that address AI integration.[10] Moreover, companies must take all necessary measures in order to secure the data used by AI systems and protect it from hackers.

In their activities, all Board members should act on a fully informed basis, in good faith, and with due diligence and care. In this respect, if they act based on the information provided by AI, they must check to see if the information is correct or at least not in contradiction with their expertise. At least a basic analysis must be made before acting upon the information provided by AI, because if AI makes a mistake, there is no legal framework that exempts Board members from being liable.

Romanian law confirms that one of the main obligations of the Board members is to act in the best interest of the company. From this principle, the two key elements of the fiduciary duty are the duty of care and the duty of loyalty. It is difficult to state that the fiduciary duties of the Board members are affected by implementing an AI system, as the problem is complex, and its solution depends on the type of AI used. Moreover, the reaction of the Board members to the information received from the AI is also relevant. For example, if the AI system used is an autonomous AI that is able to evaluate options and make decisions, it will be very hard to determine who is liable in the case of misconduct.

Until regulation is updated, at present, the liability of Board members is neither ruled out nor limited to some extent if an AI system is used.

Regulations/government intervention

In 2018, EU Member States adopted a common Declaration on Cooperation on Artificial Intelligence, which was signed by Romania and endorsed by the Council of the European Union. Following this, in February 2019, the Council adopted the Coordinated Plan on Artificial Intelligence, which states the main coordinates of the EU strategy when regulating and addressing AI and its challenges. Romania adopted the Plan in April 2019 through the Chamber of Deputies' decision, with recommendations to draft documents that can be used

by non-specialised persons and to have wide consultations with the business sector in order to identify the current needs and obstacles. It is worth mentioning that the EU is working hard to bring to light the pillars of the soon-to-come regulation by establishing high-level expert groups to address important aspects, such as the High-Level Expert Group on Artificial Intelligence, which recently drafted the Ethics Guidelines for Trustworthy AI.

As the European Coordinated Plan encourages Member States to develop their national AI strategy by mid-2019, Romania contributed in drawing the contours of a future digital policy by taking part in organising the Digital Assembly 2019. This forum is considered the most important European digital event of the year and took place on 13–15 June in Bucharest, Romania. The collaboration between the European Commission and the Romanian Presidency of the Council of the European Union gave the chance to high-level policy makers and stakeholders to have future-focused discussions and develop networking opportunities.[11]

Implementation of AI/big data/machine learning into businesses

Deciding to implement AI into a business is not an easy task. Before taking that decision, one should make a strong assessment regarding implementing AI into the business model or using it to facilitate the decision-making process. Either way, taking this step will be challenging because it involves issues regarding data privacy, employment, IP and competition, as well as consumers' rights and liability.

It is well known that AI is strongly connected to big data, and both need to comply with privacy and data protection regulations.

Generally speaking, the most important privacy principles of the GDPR applicable to AI concern: Notice; Consent; Access; Use; Transfer; and Disposal. The first two principles involve providing consumers with notice from the controller on its collection and processing activities which the consumers must consent to. Access concerns the right of Access, Rectification, Erasure, Right to Restriction of Processing, Right to Data Portability and Right to Object of the Data Subject. The Use of data concerns the identification of the data location and maintenance of the records for data processing activities, data categories, data retention schedules, and data transfers. Transfer imposes the obligation of the data controller to maintain records of personal data transfer to other countries and the obligation of the controller to implement an appropriate organisational and technological safeguard to protect against the risk of compromise. Disposal concerns the safe ways to erase personal data.[12] Therefore, AI systems must guarantee privacy and data protection beginning from the development phase, during deployment, and throughout utilisation. All information must be protected, starting with that provided by the user, and ending with the information generated about the user by the system following its use. This is why, when implementing an AI system, one must ensure that it is trustworthy; meaning that, among other things, the data must be handled ethically. According to the Ethics Guidelines for Trustworthy AI, there are four ethical principles in the context of AI systems: respect for human autonomy; prevention of harm; fairness; and explicability.[13] Each of these is grounded in fundamental human rights; but sometimes, depending on the case, they may be in conflict. In this type of situation, tensions between principles must be treated carefully, and trade-offs, if necessary, should be reasoned and based on evidence rather than intuition or past experiences. "In situations in which no ethically acceptable trade-offs can be identified, the development, deployment and use of the AI system should not proceed in that form."[14]

Two other important privacy and data protection issues are the freedom of choice and real informed consent. There are many cases where individuals cannot choose to use the same

product/service without the AI algorithm being involved. Also, consent is not always informed and freely given. For these reasons, freedom of choice over the use of AI and the right to a non-smart version of AI-equipped devices and services are now being taken into consideration.[15]

Public opinion on AI systems is also important and needs to be taken into consideration when one uses AI and big data, because of the social impact they create. In all areas of our lives, be it in education, work, care or entertainment, AI and big data may alter our conception of social agency or impact our social relationships and attachments. Therefore, the effects of these systems must be monitored and considered extremely carefully.[16]

When developing and implementing AI systems in their businesses, executives must ensure the quality and integrity of the data used over the performance of such data. Feeding malicious data into an AI system may change its behaviour, particularly with self-learning systems.[17]

Besides guaranteeing privacy and data protection, starting from the development phase, executives should be aware that AI systems ought to be designed in such a way that they operate without infringing copyright or any other legal regulations. The AI system should be developed in such a manner that complies by design with all applicable legislation and in consideration of legal persons' and natural persons' copyrights.

Another key issue that companies implementing these new technologies must be aware of is the implication of competition laws. We mentioned above the issues of machine collusion and the impact of big data in the digital economy. The lack of clear legal provisions that specifically regulate this field will be considered as a risk. Companies need consultants to continually monitor the applicable legislation and opinions of the competent authorities regarding antitrust activity in the digital market.

The digital market has an important impact on consumers. In the context of AI and big data, consumers' choices are used to drive sales. This impact has positive aspects, like the fact that consumers can benefit from buying products or services more relevant to their personal needs. However, it also has a negative aspect, in that their information is collected, combined and assigned to third parties. When a company markets its AI product or service, it must consider that, as in all other aforementioned fields, the legislation is not updated to the market reality and the current legislation provisions will be applied. In the EU, the legislation regulating electronic commerce, Directive 2011/83/EU on consumer rights, Directive 2006/114/EC concerning misleading and comparative advertising, Directive 2004/48/EC on the enforcement of intellectual property rights, along with the GDPR and the basic legislation concerning fundamental rights, might be considered. Non-compliant development and implementation of AI systems may lead to liability issues.

Civil liability

Civil liability when using AI technology is currently one of the hottest topics relating to AI, and raises many concerns and questions. Since there is no specific regulation in the field, we can only try to apply the current provisions in civil law by analogy. In Romania, we can rely on contractual provisions where they exist, or on general tort liability provided by the law when a contract was not concluded. Specific legislation pertaining to civil liability, from permitted means of evidence to be submitted in court trials to means of evaluating injury claims derived from the use of AI, have not yet been adopted in Romania.

The AI system should be documented in every phase of its life from its creation, and should be explainable, meaning that both the technical processes and the related human decisions

can be explained.[18] This could make the identification of the cause of an error made by AI easier, which should be linked to a human input.

According to Romanian Civil Code, each person has the duty to respect the rules of conduct required by the law or local custom, and he/she should not harm through actions or inactions the legitimate rights or interests of others; there being an obligation to fix the damages caused. Regarding tort liability conditions, Romanian civil law regulates that the one who causes damage to another by an unlawful act, committed with guilt, is obliged to fix it.

For tort liability, damage is the first condition, being a flexible concept taking into consideration that the victim's protected interest or right may be more or less significant, and the damage to such an interest or right may depend on specific situations. Thereby, this may have a major impact on the overall assessment of whether a tort liability claim may be justified in a specific case where an AI technology is involved.[19]

Considering the fact that AI technology has the ability to self-develop without human intervention, the application of tort liability shall be interpreted with precaution because the victim has to prove that the AI technology was at fault.[20]

In addition to the responsibility of the victim to prove that the AI technology was at fault, it shall prove the causal link between the damage and the AI technology's unlawful act. However, if the sequence of events is not evident, it will be more difficult for the victim to succeed in establishing and proving a causal link. This may be a first obstacle to pursuing a claim for compensation.[21]

Moreover, the Romanian Civil Code also regulates the responsibility of the principal for the conduct of the official in charge. In this regard, the principal is obliged to repair the damage caused by the official in charge whenever the unlawful act committed by the official in charge relates to the duties or purpose of the functions entrusted to the official in charge. In light of this specific legal provision, if someone can be held liable for the unlawful act of a human official in charge, it is likely that the principal shall be liable for the unlawful act of a non-human official in charge. Using the assistance of an AI technology official in charge may have the same legal regime, if such assistance leads to damage.[22]

The Romanian civil law imposes the obligation to repair the damage caused by the things found in the care of the person responsible, known as objective liability (not based on fault). For the victim, the advantage of objective liability is obvious, as it does not have to prove the AI technology's fault for the damage and the link between the damage and the unlawful act of the AI technology.[23]

According to the Romanian provision regarding prescription, the prescription of the right to action in the compensation of the damage caused by an unlawful act begins to run from the date when the victim knew or had to know both the damage and the person responsible for it. This legal approach raises the risk that the tort liability claim be cut off prematurely, before the AI technology may be identified as the source of the damage, because of the complexity of the AI technology.[24]

Alongside tort liability approach, responsibility can be transposed into a contract with very clear and comprehensive provisions on liability in different situations. In drafting contracts, companies should identify the impact of their AI systems from the very start, as well as the norms their AI system ought to comply with to avert negative impacts.[25] By knowing from the beginning what the risks are when implementing and using that AI system, companies will be able to draft a solid framework that can clearly identify the risk responsible in a certain situation. Moreover, this would help in drafting instructions for using AI, codes of practice and warnings when they are needed.

The best approach under the current legal framework is to avoid situations that may cause liability problems by being very responsible when developing and deploying AI systems. This means that human rights and ethical principles must be respected to the highest standard, addressing all the key issues that may arise in the most professional way.

* * *

Endnotes

1. *The European AI Landscape*, p. 21 available at http://adigaskell.org/wp-content/uploads/2018/04/ReportontheEuropeanAILandscapeworkshop.pdf.
2. *Ibid*., p. 21–22.
3. *Resolution of the European Parliament of 12 February 2019 on a comprehensive European and industrial policy on artificial intelligence and robotics*, p. 114–180 available at https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.pdf.
4. Court of Justice of the European Union, *Decision C-5/08 Infopaq International A/S v Danske Dagblades Forening*, paras 35, 37, available at http://curia.europa.eu/juris/document/document.jsf?docid=72482&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=3638175.
5. OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*, p. 18, available at http://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf.
6. Oxera Consulting LLP, *When algorithms set prices: winners and losers*, p. 5, available at https://www.regulation.org.uk/library/2017-Oxera-When_algorithms_set_prices-winners_and_losers.pdf.
7. *Case T-41/96, Bayer AG v Commission of the European Communities*, para. 69.
8. Microsoft Corporation, *The Future Computed. Artificial Intelligence and Its Role in Society*, p. 80, available at https://news.microsoft.com/futurecomputed/.
9. Petrin, Martin, *Corporate Management in the Age of AI* (March 4, 2019). UCL Working Paper Series, *Corporate Management in the Age of AI (No. 3/2019)*; Faculty of Laws University College London Law Research Paper No. 3/2019, p. 14, available at SSRN https://ssrn.com/abstract=3346722 or http://dx.doi.org/10.2139/ssrn.3346722.
10. Independent High-level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, p. 22, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
11. *Digital Assembly 2019*, available at https://ec.europa.eu/isa2/events/digital-assembly-2019-0_en.
12. Articles 7, 13, 15, 16, 18, 20, 21, 30 and 32 GDPR.
13. Independent High-level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, p. 12, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
14. *Ibid*., p. 20.
15. Mantelero, Alessandro, *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, p. 8, available at https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6.
16. Independent High-level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, p. 19, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
17. *Ibid*., p. 17.

18. *Ibid*., p. 18.
19. Expert Group on Liability and New Technologies – New Technology Formation set up by the European Commission, *Liability for Artificial Intelligence and other emerging digital technologies*, p. 19–20 available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.
20. *Ibid*., p. 23–24.
21. *Ibid*., p. 20–22.
22. *Ibid*., p. 24–25.
23. *Ibid*., p. 25–27.
24. *Ibid*., p. 29.
25. Independent High-level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, p. 21, available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

Cristiana Fernbach
Tel: +40 722 779 893 / Email: cfernbach@kpmg.com

Cristiana has 17 years of experience in business law, with a strong contract law and compliance & regulatory background. She strengthened her expertise in European technology and data privacy law in Bucharest and Berlin on matters ranging from regulatory, particularly for the banking and TMT sectors, to complex software licensing contract structuring, and to new technologies such as AI and blockchain. She was recognised in 2018 by *The Legal 500* for advising top-tier clients on data privacy.

Cristiana holds a law degree from the Nicolae Titulescu University in Bucharest, a Master's degree (LL.M.) from Freie Universität Berlin, and an MBA from Munich Business School. She holds a CIPP/E (European Certified Information Privacy Professional) from IAPP (the International Association of Privacy Professionals).

She is fluent in English and German.

Cătălina Fînaru
Tel: +40 721 195 771 / Email: catalinafinaru@kpmg.com

Catalina's areas of expertise comprise data protection, technology and e-commerce matters. Her attention to detail and practice-oriented view equally contribute to tailored legal solutions in tech law and data privacy projects across various industries, such as IT, banking, pharmaceuticals and advertising.

She holds a law degree from the University of Bucharest and started her legal career with internships at ANCOM (National Authority for Management and Regulation in Communications).

KPMG – Toncescu și Asociații S.P.A.R.L.

69–71 București – Ploiești Road, Bucharest, Romania
Tel: +40 741 800 800 / URL: www.kpmglegal.ro

Russia

Rustam Rafikov
Rafikov & Partners

Artificial intelligence / big data trends and considerations under Russian law

Businesses and the government actively use big data analysis in Russia. The first evangelists of big data in Russia were the telecommunication, internet and banking sectors. Today, we can see a wide application of big data technology by retailers, producers and governments. Big data technology, though, does not have a wide appeal in Russia; some changes have been made by legislators to make big data analysis easier. The main idea here is to make possible legally the transfer of big data between entities. The problem is that big data is viewed as being a part of personal data. As regulation on personal data and information technologies in Russia is very strict (there have been cases where LinkedIn was banned and penalties were imposed on Twitter with a risk of a ban of the service – which are examples of the strict regulation and necessity of legal compliance here), companies are still very cautious of processes which involve the transfer of big data. The government has promoted legal ways of entering into an agreement on big data transfer by way of an information service contract. The self-regulation of big data analytics and data analysis we see from businesses mainly takes place in the IT sector in Russia. Businesses need to have standards and ethical boundaries for big data self-regulation.

Artificial intelligence ("AI") regulation and use in Russia is at its peak. Some industries are actively searching for legal grounds for AI implementation: digital identities of citizens; face recognition; transaction analysis; deep analytics; and so on. Businesses have been lobbying for special regulations for AI and machine learning ("ML"). Adopting AI has become a new trend for businesses in Russia after the implementation of the government strategy for the development of AI. As a result, we have seen new investment flows and government spending into the AI/ML sector.

The purpose of this chapter is to establish an understanding of the issues concerning legal regulation, trends and considerations under Russian law. This chapter intends to provide business leaders and stockholders with a framework to adapt big data analysis and AI technologies.

Legal trends in the big data industry

We cannot ignore the hype connected to the idea of big data – that it will change everything. Statistical approaches were developed a long time ago and used by scientists to make conclusions about their research subjects. Big data allows predictions to be made on customers' behaviour and market tendency, and can be used to find discrepancies, similarities or even more – essentially, helping with decision-making. A study of successful companies that used big data shows us examples of gathering, storing and analysing data by new ways.

There is a prediction that every human will generate 1.7 megabytes every second by using devices, the internet, GPS systems, photos and videos.[1] Completely new approaches to analyse and store data make this process even faster. Specifically, cloud technologies and distributed computing tools could help to store and analyse data. Some modern algorithms, such as speech and photo recognition systems connected with AI and ML, create new possibilities to analyse data and make predictions. Big data itself could be characterised as a set of extracted information that could be analysed by special software (e.g. Hadoop, Tableau, Microsoft Azure, etc.). Big data is associated with the following key concepts: (i) *volume* (big data has a huge volume of information); (ii) *variety* (there are different data sets with structure or without it); and (iii) *velocity* (high speed of gathering data, analysing data and getting results from it).[2] These key features, with the possibility of using technology or software to analyse big data, allows us to create value.[3] Digital development provides us with a myriad of tools to gather and analyse data, so-called big data.

The Russian President in his instructions from the Presidential Address to the Federal Assembly[4] is intrusted by the Government and the State Duma with providing amendments to the legislation. The amendments should provide a framework for the regulation of big data analytics, taking into account human and civil rights and freedoms during the processing of personal data. The Ministry of Communications has already presented a new bill specifying the definition of big data analysis. The proposed amendments interpret big data analysis as analysis of non-personalised data. In addition, the government wants to create a register of operators processing big data. Businesses reacted negatively and proposed to remove the definition of big data and the idea of creating a register of processors of big data. Today, the regulation is still pending and discussed as a draft bill.

The self-regulation of big data in Russia is very active. Businesses engaged in processing personal data issued the Codex on Ethical Use of Personal Data. The Codex is a document intended to balance the interests of the government, businesses and citizens. The new Codex has been positively accepted by market players and many entities have adhered to its ethic principles. The Russian self-regulated Association of Big Data proposed a strategy for developing big data analytics, pointing out that each year the big data market in Russia grows by 12%. The ethical implications of big data analysis are widely accepted by key players.

A new law on regulating digital rights took effect on 1 October 2019. The law amended the Russian Civil Code with new provisions on: digital rights; possibilities to enter into an agreement or vote electronically; smart contracts; and information services agreements. Article 783.1 of the Civil Code also establishesd a new form of agreement, as aforementioned: information services agreements. The specified form of the contract provides that parties can enter into an information services agreement with the condition that the customer acquiring information may oblige a contractor to refrain from actions that may cause unauthorised disclosure of the information to third parties. The terms and conditions of service to provide big data is now defined in the Civil Code. As the Russian law system is a continental system, having a so-called statutorily defined contract is obvious. Before the amendment, market players were at risk of breaching legislation on personal data for businesses due to legal uncertainties. Big data is the impersonalised information; however, in order to gather it you sometimes need to process the data. Upon gathering and processing the data, it is usually transmitted to another party for analysis. In this case, there was a debate on whether we need to notify a person (get consent) or other third parties while processing and analysing the data. In this respect, the new amendment seems like a kind of signal to the market that was uncertain. The amendment now allows businesses to enter into an information service contract and exchange big data. The next step in the development of the regulation is to define legally the term big data in Russian law to set it apart from personal data.

The Russian government actively uses big data analytics for national security, economic research, urban planning and even tax policy. The Russian tax authorities introduced the automated control system VAT-2 which analyses information gathered from value-added tax declarations in order to find tax evasion schemes. The system facilitates the discovery of tax evasion schemes and creates obstacles for breach of law connected with false VAT declarations submitted by taxpayers. The Russian government is also gathering data for analysing and identifying the productivity of its bodies. The government's data is available on an Open Source[5] website and on a new digital analytical platform for statistical data.

Big data considerations for transactions

Big data is recognised by practitioners as impersonalised data. However, personal data regulation is very strict in Russia. At the end of 2019, penalties for breach of personal data law were increased. Specifically, these penalties were connected with a breach of law on the localisation of personal data. Russian law requires the localisation of personal data on Russian citizens on servers situated in the Russian jurisdiction. Any breach of this provision may lead to a penalty and ban in Russia. LinkedIn failed to comply with the regulation and was banned upon a court decision. In 2019–2020, the Russian authority Roskomnadzor (Federal Supervision Agency for Information Technologies and Communications) started court proceedings against Twitter and Facebook. Upon the court decision, a penalty was imposed on both Twitter and Facebook. Twitter appealed to the court but was unsuccessful. Failure to comply with laws on personal data may lead to a ban of service in Russia. LinkedIn was banned and lost the entire Russian market and is today almost unknown in the region. It is advisable to have a legal compliance team and to cooperate with Russian authorities.

The main difficulties for big data deals is personal data regulation. Today, the regulation is very broad and personal data-processing rules apply. However, we have seen a common practice which involves many market players asking customers to consent to the processing of personal data that includes big data analytics (data anonymisation and transfer of data). Gathering big data in compliance with personal data regulation is a good policy for companies. Due to legal uncertainties concerning the definition of big data, the best way to process and acquire personal data would be to proceed in compliance with the personal data law in Russia.

Legal trends in AI and ML

AI development, investments and legal regulation nowadays has gained a lot of attention. The Russian President introduced a decree on the strategy for the Development of Artificial Intelligence in Russia.[6] The decree is a part of a national strategy, "Digital Economy", that is intended to foster the development of digital technology. This strategy is connected with providing investments, increasing government spending on AI and ML, as well as creating measures for security of human and civil rights and freedoms. The main telecom, internet and media companies entered into an alliance for the development of AI and ML. This alliance will provide principles and methods of using AI, ML, robotics technologies and decisions for introducing them in industries.

Businesses are actively lobbying the government to pass several amendments for the development of AI and ML. For example, banks are active players in this process. Their interest concerns automatically performed face recognition and digital ID. Russia still uses hard copies of IDs without biometrical data. As a result, the current IDs cannot be used in identification processes through the internet. Many banks are searching for solutions for

the identification of persons through the internet. This could be helpful for providing bank products to the market, and using AI technologies for identification and bank compliance. Telecommunication operators initiated a draft bill for selling SIM cards via the internet. The proposal is concerned with the idea of creating a link with a telephone number and the citizen's ID. The government uses e-signatory and identification methods for accessing government services. However, government identification takes time, and for businesses this time is crucial for acquiring customers. The idea of face recognition, voice recognition and ML application tools is to create an autonomous customer recognition system.

The local government of Moscow actively uses AI for urban planning and traffic management. Yandex as an operator of a navigation platform and map service entered into an agreement with the Moscow government regarding traffic management. By using AI, the navigation platform provides solutions for users to escape traffic jams: when the system recognises a traffic jam, it provides information for users of alternative routes. The change of routes for users is mostly intended to avoid the backup of cars in one place. The local government in Russia actively uses traffic cameras, recognition systems and traffic planning solutions. Several startups were acquired by the Russian government to provide face recognition services. We view these changes as a trend and expect new developments of AI/ML technologies to be used by the government.

AI/ML considerations for transactions

The main source for defining AI and ML in Russia is the Presidential Decree on the strategy for the Development of Artificial Intelligence in Russia. While there is no specific regulation for AI and ML technologies, the source for the legal definitions of AI is in said decree. Meanwhile, many AI and ML systems are operating based on own internal regulation. There are several legal debates on intellectual property for works created by AI. Most debates are concerned with the point that AI work is work made for hire. This type of work is regulated by the Civil Code and requires drafting bylaws for transferring intellectual property on work made for hire. Some of the debates concern the responsibility of the AI. For example, development of self-driving cars requires a legal framework of liability for the operator. According to Article 1079 of the Civil Code, persons "whose activity is associated with increased hazard for people around (the use of transport vehicles, mechanisms, high voltage electric power, atomic power, explosives, potent poisons, etc.; building and other related activity, etc.) shall be obliged to redress the injury inflicted by a source of special danger, unless they prove that injury has been inflicted in consequence of force majeure or the intent of the injured person […] The obligation of redressing injury shall be imposed on the legal entity or the individual who possess the source of special danger by right of ownership, the right of economic or operative management or on any other lawful ground (by right of lease, by procuration for the right to drive a transport vehicle, by decision of the corresponding body on the transfer of the source of special danger, etc.)". Thus, any operation of the AI machine or program is under the responsibility of such person.

Transfer of software with AI is subject to the Civil Code regulation related to intellectual property. Russia is a part of the Berne Convention, thus copyrighted works, including computer software is under the protection of the law. A new trend concerning software regulation in Russia is a requirement to install local software for mobile devices and Smart TV products. An incentive for passing such law was a measure to help Russian software producers. Therefore, it is better to enter into the Russian market with a software product through a joint venture or Russian entity.

Regulatory sandboxes are new ways of testing legal regulation on the digital economy. The Russian government introduced regulatory sandboxes for AI and ML technologies. The same was carried out by the Central Bank with regards to e-payment and fintech startups. A company may submit an application and develop a product in such environment without any regulatory framework by a special decree.

Future perspective of legal regulation of big data, AI and ML

Russian businesses are actively engaged in new technologies and intend to develop them. Meanwhile, the government has provided regulations on increasing spending, investments and development of such technologies. The main issues with regards to new technologies are the privacy of people, localisation and security of data in Russia. Many laws that have been passed have had negative feedback from businesses. However, such laws are related to government security and privacy. Obviously, there is always room for disputes and finding the necessary balance.

Nowadays, the government and businesses are in dialogue with regards to future business regulation. Participation in working groups of experts with the government creates a future framework for legal regulation. This conclusion has been made from our firm's experience and participation in working groups as experts organised by local and federal government. We expect that legal regulation towards big data, AI and ML will rapidly grow along with the development of new technologies.

* * *

Endnotes

1. Marr, B., Big data in practice: how 45 successful companies used big data analytics to deliver extraordinary results. John Wiley & Sons. New York. 2016. P. 113.
2. Doug, L., 3D data management: Controlling data volume, velocity and variety. META Group Research Note. 6 (70). 2001. Retrieved from: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.
3. De Mauro, A., Greco, M., Grimaldi, M., A formal definition of big data based on its essential features. Library Review. 65 (3). 2016. P. 122–135.
4. List of instructions from the Presidential Address to the Federal Assembly, 15 February 2020 [Perechen' Porucheniy po realisatsii Poslaniya Prezidenta Federalnomy Sobraniyu]. Retrieved from: http://kremlin.ru/acts/assignments/orders/62673.
5. Open Data Portal Russia. Retrieved from: https://data.gov.ru.
6. Presidential Decree on Development of Artificial Intelligence in the Russian Federation, 11 October 2019 [Ukaz Prezidenta o Razvitii Iskustvennogo Intellekta v Rossiyskoy Federacii]. Retrieved from: http://publication.pravo.gov.ru/Document/View/0001201910110003.

Rustam Rafikov
Tel: +7 926 758 82 40 / Email: r.rafikov@rafikovlawpartners.com

Rustam Rafikov is a managing partner of Rafikov & Partners based in Moscow and Saint Petersburg. Rafikov & Partners was ranked as a leader firm in the Russian market on digital economy and related transactions by the Pravo 300 ranking. Rustam is a recommended lawyer in digital economy, fintech and TMT according to the business journal KommersantЪ and the Pravo 300 ranking. Rustam is an expert of the Moscow City Council within the working group of blockchain technologies regulation. His practice areas include M&A, venture investments, private equity, transactions with intellectual property, and telecom, media and technologies. Rustam graduated from the University of Manchester (LL.M.) and is currently finishing his MBA classes in the Maastricht School of Management.

Rafikov & Partners

Bolshaya Pochtovaya str., 26B bld.2, Moscow, 105082, Russia
Tel: +7 495 201 1534 / URL: www.rafikovlawpartners.com

Singapore

Lim Chong Kin
Drew & Napier LLC

Trends

Artificial intelligence ("**AI**"), big data, and machine learning have been the subject of tremendous interest in Singapore in recent years. Advances in mobile computing and increasingly widespread Internet and social media usage, amongst other things, have contributed to the availability of large volumes of data, which are increasingly being analysed by machine learning algorithms to make predictions or decisions.

The Government aims to position Singapore as not only a hub for big data but also a world leader in the adoption and use of AI technologies to drive economic growth and improve the life of its citizens. The Smart Nation initiative, launched by the Prime Minister Lee Hsien Loong in 2014, is a Government-led nationwide effort which seeks to transform Singapore into a "Smart Nation" by harnessing digital technologies across all segments of society, and to provide a competitive advantage for businesses through innovation.

Notably, AI has been identified by the Government as one of the four frontier technologies which are essential to growing Singapore's Digital Economy, alongside Cybersecurity, Immersive Media and the Internet of Things. To this end, the Government has launched a slew of initiatives to promote the adoption and development of these new technologies in Singapore across the public and private sectors, to build AI capabilities, and to create a highly conducive environment for businesses to thrive in these fields.

Some of the initiatives that have been launched in Singapore in recent years include:

a) the establishment of the Smart Nation and Digital Government Office ("**SNDGO**") under the Prime Minister's Office ("**PMO**") to lead the digital transformation efforts. The SNDGO plans and prioritises key Smart Nation projects, drives the digital transformation of Government, builds long-term capabilities for the public sector, and promotes adoption and participation from the public and industry;
b) the establishment of the Government Technology Agency ("**GovTech**"), a statutory body that serves as the implementing agency of the Smart Nation initiative. GovTech's roles include transforming the delivery of Government digital services and building Smart Nation infrastructure;
c) the establishment of SGInnovate, a Government-owned company which invests in and develops Deep Tech start-ups in Singapore. SGInnovate comes under the purview of the National Research Foundation ("**NRF**"), a department within the PMO which sets the national direction for research and development;
d) the launch of AI Singapore, a national AI programme by NRF, to build AI capabilities, grow local talent, build an AI ecosystem, and put Singapore on the world map. Its activities include seeding and providing support for AI research, accelerating the adoption of AI by Singapore-based organisations, and AI talent development;

e) the formation of the Advisory Council on the Ethical Use of AI and Data, chaired by former Attorney-General V K Rajah SC, to tackle ethical questions raised by the growing use of AI, in order to develop a trusted AI ecosystem. The 11 council members are drawn from a range of backgrounds and comprise international leaders in AI such as Google, Microsoft and Alibaba, advocates of social and consumer interests, and leaders of local companies keen to make use of AI;
f) the launch of the Future Law Innovation Programme by the Singapore Academy of Law, aimed at encouraging the adoption and invention of new technology amongst law firms, legal departments and legal tech start-ups;
g) the establishment of a new National AI Office to facilitate the commercialisation of AI research and act as a link between the private and public sectors;
h) the launch of a National AI strategy, which involves five "National AI" projects in the high socio-economic impact sectors of border security, logistics, healthcare, education management and estate management, aimed at delivering tangible benefits to citizens and businesses; and
i) the provision of Government grants and incentives, such as the AI and Data Analytics ("**AIDA**") Grant offered by the Monetary Authority of Singapore ("**MAS**"), which aims to promote the adoption and integration of AIDA in financial institutions.

Various governmental and regulatory agencies have also issued policy papers setting out their views on matters relating to AI and big data, and have invited stakeholder feedback on certain policy issues and proposals by way of consultation exercises. Recent examples include:

a) the Personal Data Protection Commission's ("**PDPC**") Proposed Model AI Governance Framework ("**Model AI Framework**"). The Model AI Framework is the first in Asia and is intended to provide detailed and readily implementable guidance to private sector organisations to address key ethical and governance issues when deploying AI solutions;
b) a research paper titled "*Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights*", published by the Competition & Consumer Commission of Singapore ("**CCCS**", formerly the Competition Commission of Singapore) in collaboration with the Intellectual Property Office of Singapore ("**IPOS**");
c) a Discussion Paper on Data Portability issued by the PDPC in collaboration with the CCCS, setting out the findings of a study on the potential introduction of a data portability requirement and discussing the impact and benefits of such a requirement. The PDPC has since issued a Public Consultation Paper on the proposed introduction of a new data portability obligation (see below);
d) MAS's "*Principles to Promote Fairness, Ethics, Accountability and Transparency* ("**FEAT**") *in the Use of AI and Data Analytics in the Financial Sector*"; and
e) MAS's Veritas framework, which will enable financial institutions to evaluate their AIDA solutions against the principles of FEAT.

The Singapore courts have also had the opportunity to address issues raised by AI in the context of cryptocurrencies. In the case of *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17 ("***B2C2 v Quoine***"), the Singapore International Commercial Court ("**SICC**") had to decide on how legal principles were to be applied to a cryptocurrency exchange on which the trades were made by a computer, i.e. through the operation of algorithmic trading and not consciously entered by a human being.

While the algorithmic program in *B2C2 v Quoine* was found by the SICC to be "deterministic" in nature, with "*no mind of [its] own*" and "*mere machines carrying out actions which in another age would have been carried out by a suitably trained human*", the SICC (per Simon

Thorley IJ) opined that the ascertainment of knowledge in cases where computers have replaced human actions will develop in the future as disputes arise as a result of such action, particularly in cases where the computer in question is "*creating artificial intelligence*" and can be said to have "*a mind of its own*" (*B2C2 v Quoine* at [206] to [209]).

Ownership/protection

The Singapore Government has sought to facilitate the protection of intellectual property ("**IP**") rights in AI technologies, in order to support innovative enterprises to bring their AI products to market faster.

Notably, on 26 April 2019, the IPOS launched an Accelerated Initiative for Artificial Intelligence ("**AI²**") scheme, which will accelerate the grant of AI-related patent applications to six months, compared to the typical period of two years or more. The scheme is limited to the first 50 applications filed, subject to the IPOS's discretion to adjust the cap and/or criteria subsequently.

The IPOS's circular on the AI² scheme defines AI as follows:

> *"AI refers to a set of technologies that seek to simulate human traits like: sense, comprehend, act and learn to achieve specific tasks. AI inventions are commonly associated with, but not limited to, machine learning. Machine learning is the form of AI that uses algorithms and statistical models to enable computers to make decisions without having to be explicitly programmed to perform a particular task…"*

Eligibility for the AI² scheme is subject to compliance with the following criteria:

(a) the application is an AI invention (e.g., image recognition, speech/voice recognition, natural language processing, and autonomous systems);
(b) the application has to be first filed in Singapore;
(c) Form PF1: Request for Grant of Patent, and Form PF11: Request for Search and Examination Report have to be filed on the same day;
(d) the application contains 20 or fewer claims;
(e) the applicant must respond within two weeks from the date of receipt of a Formalities Examination Adverse Report;
(f) the applicant must respond within two months from the date of receipt of a written opinion; and
(g) a supporting document tagged as a Fast Track document stating that the application is an AI invention must be furnished during the submission of Form PF11.

Under section 13 of the Patents Act (Cap. 221), for an invention to be patentable, it must satisfy three conditions:

(a) the invention is new;
(b) it involves an inventive step; and
(c) it is capable of industrial application.

Companies considering the possibility of patent protection for AI inventions may wish to note that potential issues may arise in light of the principle that a mathematical method *per se* is not a patentable invention. In this regard, the IPOS has stated in its circular on the AI² scheme that a claim to an AI method characterised by the mathematical steps of an algorithm would be considered a mathematical method *per se*, and therefore not an invention. Furthermore, where the said AI method is defined to be implemented on a generic computer or using conventional computer hardware, the mere recitation of said generic hardware in the claim is unlikely to be enough for the actual contribution of the claim to be considered anything more than the underlying mathematical method.

That said, the IPOS's circular also states that a claim to an AI method implemented on a computer and directed to solving a specific problem, such as a machine learning method implemented on a computer for speech or image recognition or natural language processing, would likely be considered as an AI invention in the patent application.

Apart from protection of AI solutions under patent law, the source code of a computer program may also be protected by copyright. Section 7A(1)(b) of the Copyright Act (Cap. 63) ("**Copyright Act**") expressly provides that "literary work" includes a "computer program" for the purposes of the Copyright Act.

In the context of AI, a couple of further issues may become increasingly relevant. These are: (i) rights in relation to data; and (ii) rights in relation to works generated by AI.

Protection of data under IP laws

The ability of IP laws to protect data may become an increasingly relevant issue in cases involving analytical applications or algorithms which derive their value from the underlying datasets.

In general, data *per se* is not protected under copyright law. Under the Copyright Act, a compilation of data may be protected as a literary work if it constitutes an intellectual creation by reason of the selection or arrangement of its contents.[1] In this regard, the Singapore courts have held that, for copyright to subsist in any literary work, there must be an authorial creation that is causally connected with the engagement of the human intellect. In the context of compilations, the compiler must have exercised sufficient creativity in selecting or arranging the material within the compilation to cloak the original expression with copyright.[2] Thus, it has been held by the Singapore courts in a case involving two publishers of phone directories that such data is not protected by copyright law (see *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185). It remains to be seen, in the context of AI datasets, what level of creativity is necessary for a selection or arrangement of facts or data to be deserving of copyright protection.

Singapore copyright law does not provide for a *sui generis* database right such as the one recognised in the European Union.[3]

As an alternative, data may be subject to protection under the common law of confidence if three elements are fulfilled:[4]

(a) the data has the necessary quality of confidence about it; i.e., it cannot be available to the public at large;
(b) the data must have been imparted in circumstances importing an obligation of confidence; and
(c) there is an unauthorised use of the data to the detriment of the party communicating it.

Where the aforementioned three elements are fulfilled, the owner of the confidential information may be able to bring an action for breach of confidence.

Proposed new exception for text and data mining

The Singapore Government has observed, in the Singapore Copyright Review Report (issued 17 January 2019), that text and data mining and its applications are crucial elements that fuel economic growth and support Singapore's drive to catalyse innovation in the digital economy. Text and data mining refer to the use of automated techniques to analyse text, data and other content to generate insights and information that may not have been possible to obtain through manual effort.

It is acknowledged that the economic and social impact of the insights obtained through text and data mining is far-reaching and growing. However, those involved in such activities risk

infringing copyright as the initial phase of the work typically involves incidentally extracting or copying data from large quantities of material, which may be protected by copyright.

In this light, the Ministry of Law and IPOS are proposing to amend the Copyright Act to allow the copying of copyrighted materials for the purpose of data analysis, provided that the user has lawful access to the materials that are copied and that the user cannot distribute the works to those without lawful access to the works. The proposed exception does not distinguish between commercial and non-commercial use.

Protection of AI-generated works

At this juncture, it remains to be seen whether and how current IP laws may be applied to protect AI-generated works. Under the present IP legal framework, a number of issues are likely to arise with respect to the protection of AI-generated works. Programs capable of generating such works already exist and are in use. For instance, certain news outlets currently use AI to automate repetitive news reports; e.g., financial reports or sports results.[5]

The Singapore courts have recognised that, under existing Singapore copyright law, only natural persons may be considered authors of works, although legal persons like companies may own the copyright in works. It is therefore necessary to be able to attribute the creative elements of a work to a natural person in order for copyright to vest.[6] Under the present statutory regime, the courts have further observed that "in cases involving a high degree of automation, there will be no original work produced for the simple reason that there are no identifiable human authors",[7] authorship being the exercise of independent original or creative intellectual effort.[8]

Antitrust/competition laws

The Competition Act (Cap. 50B) ("**Competition Act**") establishes a general competition law in Singapore. The Competition Act generally prohibits:

(a) anti-competitive agreements (the section 34 prohibition);[9]
(b) the abuse of a dominant position (the section 47 prohibition);[10] and
(c) mergers and acquisitions that substantially, or may be expected to substantially, lessen competition within any market in Singapore (the section 54 prohibition).[11]

The CCCS is the statutory authority responsible for administering and enforcing the Competition Act.

Competition issues pertaining to AI and big data have been the subject of various studies[12] by the CCCS.

Anti-competitive agreements and concerted practices facilitated by algorithms

Amongst the topics discussed in one of the CCCS's papers[13] is that of anti-competitive agreements and concerted practices facilitated by algorithms.

In its paper, the CCCS recognised the need to balance efficiency gains against the increased risk of collusion. In this regard, the CCCS has identified a couple of concerns in relation to algorithms providing new and enhanced means of fostering collusion. First, monitoring algorithms may enhance market transparency and organisations may be able to automatically extract and evaluate real-time information concerning the prices, business decisions and market data of competitors. Second, algorithms increase the frequency of interaction between organisations and the ease of price adjustments, as automated pricing algorithms may be able to automate the decision process of colluding organisations so that prices react simultaneously and immediately to changes to market conditions.[14]

In terms of applying competition enforcement to algorithms, the CCCS has observed that, where the use of algorithms is in furtherance of, or to support or facilitate any pre-existing or

intended anti-competitive agreements or concerted practice, such cases fall squarely within the existing enforcement framework. For example, where algorithms are used to assist in the implementation of an anti-competitive agreement and are ancillary to the main infringement, liability for breaching the section 34 prohibition may be established based on evidence of the underlying agreement or concerted practice. As another example, where a common third-party pricing algorithm is used by competitors to coordinate prices (i.e. "hub-and-spoke" scenarios), such activity may be caught by the section 34 prohibition.[15]

The CCCS has identified certain concerns about whether the existing competition enforcement framework is adequately equipped to deal with future developments involving algorithms. The main concern identified by the CCCS lies in how algorithms may lead to greater instances of tacitly collusive equilibriums which may fall outside the current scope of competition enforcement. Other concerns relate to how an organisation's independent and rational business justifications for using a third-party pricing algorithm may be weighed against any anti-competitive effect that may result from such use, and how liability may be established for any autonomous decision-making that results in collusive outcomes in situations involving self-learning algorithms. The CCCS has noted that, while its current analytical framework is equipped to assess anti-competitive conduct involving algorithms, there are no settled positions on the aforementioned concerns. As such, this remains an evolving field.

Data portability

Another recent development is the issuance by the PDPC of a consultation paper on the proposed introduction of a new data portability obligation in the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**").

Subject to certain prescribed exemptions and conditions, the proposed data portability requirement would allow individuals to request from an organisation a copy of their data that is in the organisation's possession or under its control, to another organisation in a commonly-used machine-readable format.[16] From a competition perspective, data portability may lead to efficiencies for organisations, as they may find it easier to gain access to more varied datasets. Data portability may also lead to a reduction of switching costs, as customers can request for their data to be transferred to a competitor without having to re-enter that information, ultimately enhancing competition. For organisations that rely on data as an important or essential input, a data portability requirement may facilitate access to this input and lower the barriers to entry and expansion, thereby enhancing competition.

Board of directors/governance

On 23 January 2019, the PDPC published the first edition of its Model AI Framework for public consultation, pilot adoption and feedback.[17] The Model AI Framework is the result of efforts by policy makers and regulators in Singapore to articulate a common AI governance approach and a set of consistent definitions and principles relating to the responsible use of AI. It also represents Singapore's attempt to contribute to the global discussion on the ethics of AI by providing a framework that helps translate ethical principles into pragmatic measures that businesses can adopt. Adoption of the Model AI Framework is on a voluntary basis.

The Model AI Framework comprises guidance on four key areas, including organisations' internal governance structures and measures. The Model AI Framework also expressly recognises that "*[t]he sponsorship, support, and participation of the organisation's top management and its Board in the organisation's AI governance are crucial*". One of the suggested practices also includes establishing a coordinating body having relevant expertise and proper representation from across the organisation to oversee the ethical deployment of AI.

Briefly, the principles set out in the Model AI Framework across the four key areas include the following:

(a) Internal governance structures and measures: organisations should ensure that there are clear roles and responsibilities in place for the ethical deployment of AI, and that there are risk management and internal controls in place.
(b) Determining AI decision-making models: organisations should consider the risks of using a particular AI model based on the probability and severity of harm, and determining what degree of human oversight would be appropriate based on the expected probability and severity of harm.
(c) Operations management: organisations should take steps to understand the lineage and provenance of data, the quality of their data, as well as the transparency of the algorithms chosen.
(d) Customer relationship management: organisations should take steps to build trust and maintain open relationships with individuals regarding the use of AI, including such steps as general disclosure, increased transparency, policy explanations, and careful design of human-AI interfaces.

Regulations/government intervention

Protection of personal data

Aside from the obvious issues arising from the collection of large amounts of personal data for the purposes of big data analytics, the use of datasets in conjunction with AI applications also has the potential to raise data protection ("**DP**") issues especially where such datasets comprise personal data.

The PDPA sets out the general DP framework which governs the collection, use and disclosure of personal data by private sector organisations in Singapore. It operates alongside sectoral laws and regulations, for instance those issued by the MAS for the financial sector.

Under the PDPA's general DP framework, there are nine main obligations. Since the enactment of the PDPA, the general DP framework has been substantially a consent-based regime. In this regard, the "consent obligation" under the PDPA requires an organisation to obtain an individual's consent before the collection, use or disclosure of the individual's personal data, unless an exception applies.[18]

In 2017, the PDPC issued a public consultation paper in which it recognised that the existing consent-based approach to DP[19] may present challenges in the new digital economy. For example, it may not be possible for organisations to always anticipate all the purposes for using or disclosing personal data at first instance.

Given the state of technological advances and global developments, the PDPC therefore undertook a review of other bases for collecting, using and disclosing personal data under the PDPA. It proposed to introduce "notification of purpose" as a basis for the collection, use and disclosure of personal data, subject to the following conditions.[20] In this regard, it has been proposed that an organisation would only be able to rely on notification of purpose as a basis when it is impractical for the organisation to obtain consent, and the collection, use or disclosure of personal data is not expected to have any adverse impact on the individual.[21]

The PDPC has also proposed to introduce provisions for data innovation under the PDPA, which allow organisations to use personal data for certain business innovation purposes. Under this proposed provision, organisations can use personal data (collected in compliance with the PDPA) for the purposes of: (i) operational efficiency and service improvements; (ii) product and service development; or (iii) knowing customers better. It remains to be

seen how the proposed provisions would be formally implemented. At the time of writing, legislative changes to the PDPA have yet to be tabled.

A further issue that may be of relevance to organisations using large datasets is whether anonymised data may nevertheless be regarded as personal data for the purposes of the PDPA.

Technological advancements may increase the risk that a dataset that was previously anonymised may be de-anonymised, and thereby be considered personal data.[22] In this regard, the use of algorithms and/or machine learning technologies that are able to draw inferences about certain personal identifiers of individuals from voluminous datasets may increase the risk of data which is assumed to be anonymised to constitute personal data. Companies which intend to engage in such operations should therefore exercise diligence in order to ensure that they do not inadvertently collect, use and/or disclose personal data without fulfilling the requisite requirements, thereby infringing the obligations under the PDPA.

Trusted Data Sharing Framework & Data Regulatory Sandbox

The Info-communications Media Development Authority ("**IMDA**"), which is the current designated PDPC, has also developed a Trusted Data Sharing Framework by helping companies by establishing a baseline "common data sharing language" and systematic approach to understanding the broad considerations for establishing trusted data sharing partnerships.[23]

Under this Trusted Data Sharing Framework, the IMDA has introduced a Data Sharing Sandbox to encourage innovation in the use of personal data to offer new products or services, under circumstances where: (i) sharing of data is not likely to have an adverse impact on individuals; or (ii) where there is a need to protect legitimate interests, and benefits for the public outweigh adverse impacts on individuals, to be tested on the market.[24] Interested organisations may approach the PDPC to submit an application. If approved, the Data Sharing Sandbox will be effected by way of an exemption for the relevant organisation from provisions of the PDPA, subject to specified terms and conditions.

In recognition that a key obstacle to data sharing is the difficulty in assessing the value of the data assets, the IMDA has also issued, amongst other documents, the Guide to Data Valuation for Data Sharing to help organisations assess and value their data.

IMDA's Data Collaborative Programme also offers a Data Regulatory Sandbox to businesses and their data partners to explore and pilot innovative use of data in a safe "environment" in consultation with IMDA and PDPC. Some of the key considerations for organisations seeking to leverage Data Regulatory Sandbox include the following:

(a) Innovative: the use case should demonstrate how data can be used to derive new value or creation of new products, which would not be possible under the current regulation.
(b) Benefit to the public: the use case should likely not have any adverse impact on the consumers.
(c) Ready and concrete use case: the use case should not be hypothetical. It should have sufficient interest from the relevant stakeholders and have clear outcomes.
(d) Risk assessment and mitigation: The risks and impact should be assessed and mitigated, and there should be reasonable effort to protect the interest of the individual.

Cybersecurity Act 2018

The Cybersecurity Act 2018 (No. 9 of 2018) ("**Cybersecurity Act**") establishes the framework for the oversight and maintenance of national cybersecurity in Singapore and imposes duties and obligations on computer systems designated as critical information infrastructure (CII).

The Cybersecurity Act operates alongside the Computer Misuse Act (Cap. 50A) which criminalises certain cyber activities such as hacking, denial-of-service attacks, infection of computer systems with malware, and other sector-specific regulatory frameworks.

Protection from Online Falsehoods and Manipulation Act 2019

The Singapore Government is one of many jurisdictions to have enacted laws to deal with fake news and misinformation. The Protection from Online Falsehoods and Manipulation Act 2019 (No. 18 of 2019) ("**POFMA**") which came into effect on 2 October 2019 seeks to, amongst others, prevent the electronic communication in Singapore of false statements of fact. In particular, it is an offence under POFMA for a person to make or alter an automated computer program (i.e. a "bot") with the intention of using the bot to communicate a false statement of fact in Singapore.

Regulation of autonomous motor vehicles

The Singapore Government has also recognised the potential benefits that AI may bring to the transportation sector, and has sought to facilitate trials involving autonomous vehicles. In 2017, the Road Traffic Act (Cap. 276) was amended to include specific definitions relating to autonomous vehicles. For example, the term "autonomous motor vehicle" means "*a motor vehicle equipped wholly or substantially with an autonomous system (also commonly known as a driverless vehicle), and includes a trailer drawn by such a motor vehicle*".

The term "autonomous system" is defined to mean "*a system that enables the operation of the motor vehicle without the active physical control of, or monitoring by, a human operator*". Meanwhile, the term "automated vehicle technology" means "*any particular technology that (a) relates to the design, construction or use of autonomous motor vehicles; or (b) otherwise relates to advances in the design or construction of autonomous motor vehicles*".

Furthermore, the Road Traffic (Autonomous Motor Vehicles) Rules 2017 ("**Autonomous Vehicles Rules**") was introduced to regulate the trials of autonomous vehicles. Most significantly, there is a general prohibition against the trial or use of an autonomous motor vehicle on any road unless the person has specific authorisation.

The framework established under the Autonomous Vehicles Rules sets out that parties interested in conducting trials of autonomous vehicles must submit an application to the Land Transport Authority ("**LTA**"). The application to the LTA must include, amongst others, the objectives of the trial, the type of autonomous vehicle to be used and how the autonomous vehicle is intended to be used. In granting a party the authorisation to conduct such trials, the LTA retains the discretion to impose conditions, such as a condition for an autonomous vehicle to be accompanied by a safety driver that has been trained to take over full control of the autonomous vehicle when required, and to state the geographical area in which the trial may be conducted.

In 2018, in response to queries raised in Parliament in respect of the safety measures that are currently in place for the conducting of trials of autonomous vehicles, the Senior Minister of State for Transport stated that to ensure the safety of all road users, trials must fulfil stringent requirements. For instance, an autonomous vehicle must pass a safety assessment to demonstrate that it can adequately handle basic manoeuvres and safely stop upon the detection of an obstacle. An autonomous vehicle must also have a vehicle fault alert system that will alert the safety driver of any faults, and allow the control of the autonomous vehicle to be immediately transferred to the safety driver.

In January 2019, Enterprise Singapore published Technical Reference 68, a set of provisional national standards to guide the industry in the development and deployment of fully

autonomous vehicles. Technical Reference 68 promotes the safe deployment of fully autonomous vehicles in Singapore and contains standards with respect to vehicle behaviour, vehicle safety, cybersecurity and data formats. As a provisional standard, Technical Reference 68 will continue to undergo refinement as autonomous vehicle technologies mature.

* * *

Endnotes

1. Section 7A of the Copyright Act.
2. *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [24].
3. *Ibid.* at [34]–[35].
4. *Obegi Melissa and Others v Vestwin Trading Pte Ltd* [2008] 2 SLR(R) 540.
5. The New York Times, *The Rise of the Robot Reporter* (5 February 2019), accessible at https://www.nytimes.com/2019/02/05/business/media/artificial-intelligence-journalism-robots.html.
6. *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 at [41], [72].
7. *Ibid.* at [81].
8. *Ibid.* at [75].
9. Section 34 of the Competition Act.
10. Section 47 of the Competition Act.
11. Section 54 of the Competition Act.
12. *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (16 August 2017) by CCCS (in collaboration with the IPOS and the PDPC); *Discussion Paper on Data Portability* (25 February 2019) by PDPC (in collaboration with CCCS).
13. CCCS, *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (16 August 2017).
14. *Ibid.* at pages 66 to 68.
15. *Ibid.* at pages 69 and 70.
16. PDPC (in collaboration with the CCCS), *Discussion Paper on Data Portability* (25 February 2019), at page 3.
17. The AI Framework was recognised as a top award in the "Ethical Dimensions of the Information Society" category by the World Summit on the Information Society Prizes.
18. Section 13 of the PDPA.
19. PDPC, *Public Consultation on Managing Personal Data in the Digital Economy* (27 July 2017), at page 4.
20. PDPC, *Public Consultation on Managing Personal Data in the Digital Economy* (27 July 2017), at page 6.
21. PDPC, *Public Consultation on Managing Personal Data in the Digital Economy* (27 July 2017), at page 7.
22. PDPC, *Advisory Guidelines on the PDPA for Selected Topics* (revised 31 August 2018), at page 14.
23. IMDA, Trusted Data Sharing Framework, https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf.
24. IMDA, Data Sharing Sandbox, https://www.imda.gov.sg/-/media/imda/files/industry-development/innovation/guide-to-data-sharing-powerpoint.pdf?la=en.

Lim Chong Kin
Tel: +65 6531 4110 / Email: chongkin.lim@drewnapier.com

Chong Kin is a Director with Drew & Napier LLC. He heads both the Competition, Consumer and Regulatory, and the Technology, Media and Telecommunications ("**TMT**") Practice Groups, and is also the co-head of the firm's Data Protection, Privacy & Cyber-security Practice Group.

Chong Kin has experience in advising the sectoral competition regulators on liberalisation matters since 1999, including drafting, implementing and enforcing the competition law framework for the telecom, media and postal sectors, before moving on to the general Competition Act.

He continues to advise both regulators and industry on competition matters under various sectoral competition codes and is widely acknowledged by peers, clients and rivals as a leading competition lawyer in Singapore.

Chambers 2019 lists him as a band 1 Competition and TMT lawyer, noting, "[Chong Kin] commands a leading reputation in the TMT sector and is especially noted for his regulatory expertise"; and: "He attracts praise for both his 'knowledge and responsiveness' as well as for offering 'clarity in his advice' to clients. He is adept at advising corporations on a range of competition mandates, including compliance, transaction reviews and filings both in Singapore and across the ASEAN region."

Drew & Napier LLC

10 Collyer Quay, 10th Floor Ocean Financial Centre, Singapore 049315
Tel: +65 6531 4110 / URL: www.drewnapier.com

South Africa

Fatima Ameer-Mia, Christoff Pienaar & Nikita Kekana
Cliffe Dekker Hofmeyr Inc.

Trends

Terminology

"AI" or "artificial intelligence" is a computer or software system that uses algorithms to make it possible for machines to learn from experience, adjust to new inputs and perform or simulate human-like behaviour or tasks.

"Machine learning" is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Computer Business Review (online) defines "big data" as large sets of data that are so large and complex that traditional data processing cannot be used to analyse them. The data sets can be both structured or unstructured and, typically, "big data" analysis finds ways to analyse and extract information computationally to reveal patterns, trends and associations, often relating to human behaviour and patterns.

Trends in South Africa

In many industries in South Africa, there has been a drive towards incorporating big data analysis, artificial intelligence and machine learning into businesses and products to streamline operations, analyse user behaviour and determine or predict potential purchasing behaviour. Below we discuss some key trends within South Africa.

FinTech and InsurTech

In the banking industry, financial institutions are increasingly using big data sets (through AI-enabled software) to improve their analysis of clients' credit scores and subsequent risk profiles for loan considerations, to create value-added services and to improve on existing service offerings. AI software is now able to use big data from a variety of online sources linked to a client, including social media accounts, to build risk profiles and better understand which clients may benefit from or be interested in certain products.

Insurance companies have also been using AI and big data analysis to better analyse their clients' behaviours, better predict risk exposure and create insurance models that address concerns that many clients have had with the industry's lack of transparency and large premiums. A South African-based InsurTech start-up uses AI software with photographic recognition to analyse photographs of items which end-users wish to insure and have submitted via the app. The app is able to identify the item from the photograph and offers the end-user insurance for the identified item.

HealthTech

AI is enabling medical professionals to make faster and more accurate diagnoses and to help more patients in remote, far-to-reach locations in South Africa. South Africa's major medical

insurers are experimenting with big data analytical tools and "chatbots" (that utilise machine learning) to create a more client-centric business model that allows its members to connect information about their healthy habits, such as gym workouts and healthy food purchases, in order to get points and receive rewards, such as discounts on flights. In South Africa, there are also a number of entrepreneurial companies using AI and big data to assist the lifestyle management of certain types of diabetes and conduct genetics analytics. A digital health company in South Africa is using a technology platform that uses AI and machine learning to analyse big sets of data of its public and private sector clients, which then allows these clients to implement and manage their healthcare programs.

AgriTech

In the agricultural sector, a few companies are using drones that use artificial intelligence, machine learning and big data analysis to provide imagery to farmers of their crops, and interpret these images and other related data to provide an analysis about the health of the crops.

Other Technology Trends

There are a number of South African AI start-ups which successfully use AI technology and machine learning. For example, one such start-up focuses on developing AI which helps people work more effectively, rather than replacing them with AI systems. As an example, it provides non-coding businesses with the opportunity to develop "Virtual Adviser Apps", which can provide a business' clients with detailed information about the products that that business offers and can also be developed to assist staff in taking decisions particular to their unique business.

Another successful start-up uses artificial intelligence to assist companies within the manufacturing sector to eliminate defects in their factories and improve yield in the production process, and is the first African machine learning specialist company which provides AI solutions for businesses across the globe.

Whilst South Africa is taking big strides in the AI industry, it is not without challenges. In the South African economy, where unemployment is rife, businesses looking to implement AI systems should be mindful of AI replacing human jobs so as not to negatively affect the economy. AI systems are also expensive to implement, and cost is therefore a challenge (and often a barrier) to many businesses.

Ethical AI

A particularly topical trend at present is ethical AI and how we define what a "good outcome" is when it comes to algorithms. The Centre for Artificial Intelligence Research ("CAIR"), which primarily consists of a collaboration of South African universities research groups, was established with the aim of building world-class AI research capacity in South Africa. The CAIR is tasked with, amongst other things, investigating ethical use of AI. In the absence of any policy or regulatory standards regarding ethical AI, it is up to the coders and creators to act ethically and to self-regulate (as such).

Ownership/protection

When a company creates an AI algorithm, who is the owner?

An AI algorithm, or more specifically the written code, encompassing both the program's source code and object code would be categorised as a "computer program" in South Africa and is protected by the law of copyright. The point of departure in the law of copyright is that ownership of original work shall vest in the author, or in the case of joint authorship, in the co-authors of the work. It is therefore critical to identify who the author is. In respect of

a computer program, the Copyright Act 98 of 1978 ("Copyright Act") states that the author is the person who exercised control over the making of the computer program. Where the work is created in the course and scope of employment (whether under a contract of service or apprenticeship), the employer will hold the copyright. Where a computer program has been commissioned, the person commissioning the work would be the author; i.e., where a company has commissioned a developer to create an AI algorithm, the author and therefore owner of the copyright would be the company that commissioned the work, and not the developer (unless stated otherwise in an agreement). See also the section below on copyright.

A more interesting legal question is: who owns the work that an AI machine may create?

In South Africa, the Copyright Act defines an "author" in relation to various works as "the person". The only exception is in respect of a "published edition" which refers to the "publisher" as the author (and does not explicitly refer to a "person"). Considering that all the other definitions refer to "the person", we do not think that it was the drafter's intention to treat the authors of published editions differently to other works and that this is likely just a result of poor drafting. A "person" is not defined in the Copyright Act, and as such we must revert to the rules of statutory interpretation which suggest that a purposive interpretation should follow when a literal interpretation is not possible. The ordinary literal dictionary meaning of a "person" is "a human being regarded as an individual" (*Oxford English Dictionary*). However, both natural and juristic persons are eligible for ownership rights in copyright, so a literal interpretation does not assist us in this instance. Upon a purposive interpretation, we are of the view that the intention of the legislature when drafting the Copyright Act was for legal persons (including both natural and juristic persons) to receive protection under the Act – however, it is unlikely that the legislature anticipated the concept and technology in respect of AI when drafting such provisions, and therefore it is unlikely that the intention of the legislature was for a machine to enjoy copyright protection and ownership.

If the machine is truly autonomous, the work is technically "original" (and not commissioned) as the work would be machine-learned from a series of data inputs. In some instances, the company and/or person feeding the data (inputs) may not know what the output will be – work could therefore be an incidental creation. However, in other instances, the work may be "commissioned" and the copyright vests with the person who commissions such work.

Policy and laws have yet to keep up with the rapidly changing technology landscape. This ownership conundrum is another legal lacuna to which there is no exact answer and would largely depend on the facts and circumstances at hand.

What intellectual property issues may arise regarding ownership?

Ownership issues which may arise include conflicting claims in situations where intellectual property is unregistered. For example, technology may be developed simultaneously but by separate parties or co-developed; and once brought to market, issues around where ownership rights are attached could be of concern.

How are companies protecting their technology and data?

Depending on the type and form of technology, there are various ways to protect one's intellectual proprietary interests in South Africa, including: non-disclosure agreements ("NDAs"); copyright; trade marks; and patent protection.

NDAs

Confidentiality agreements (or NDAs) are almost standard practice in respect of any technology services arrangements and are often concluded as standalone agreements well in advance prior to any technology services agreement being concluded. The purpose of

an NDA is to protect the proprietary and confidential information of the disclosing party. Companies may require developers, employees and third-party suppliers to sign such NDAs prior to having access to such information.

Copyright

Copyright in South Africa is regulated by the Copyright Act and automatically subsists in original works, eligible for protection, created by a qualified person or which were first published in South Africa or another country to which protection is extended. Under the Copyright Act and for a work to be eligible for copyright, it must (i) fall within one of the recognised types of work, (ii) be original, and (iii) be captured in a material form. As stated above, an AI algorithm would be categorised as a "computer program" in South Africa and is protected by the law of copyright.

It is important to note that copyright is territorial in nature. If the work is first published in South Africa, or any one of the owners (authors) is a South African citizen or is domiciled or resident in South Africa (in the case of an individual), or, in the case of a juristic person, is incorporated in South Africa, then the Copyright Act and common law rules afford protection.

However, where a work was first published outside of South Africa or the owners (authors) are not South African citizens, residents or domiciled or incorporated within South Africa, then the work would need to qualify for protection on the basis of the protection being extended to the relevant country by virtue of public international law. South Africa is a signatory to the Berne Convention for the Protection of Literary and Artistic Works of 6 September 1886 ("Berne Convention"). The Berne Convention provides that works must be afforded equal protection in the signatory state as its own copyrighted works. Although a signatory to the Berne Convention, South Africa is, however, not a signatory to the World Intellectual Property Organisation Copyright Treaty of 20 December 1996, which essentially extends the protection of literary and artistic works under the Berne Convention to computer programs. Consequently, copyrights in "internationally created" computer programs are not explicitly recognised in South African law.

Moral rights

Additionally, and separate from an author's copyright, moral rights exist in South Africa to protect certain categories of works. Moral rights include the right to paternity (i.e., the right to claim authorship of the work) and the right to integrity (i.e., the right to object to any distortion or modification of the work where such is derogatory, prejudicial or may cause prejudice to the author). Moral rights are personal rights which attach to the author and exist to protect the integrity and ownership of their work. Moral rights cannot be assigned due to their personal nature, but can be waivered, and should be done so in writing. It is important to bear in mind that a moral right can only subsist in a work if such work enjoys copyright protection in South Africa in the first place.

Trade marks

A trade mark is a word, symbol, phrase or device which identifies the services or goods of one person and distinguishes it from the goods and services of another. It has become popular to give AI software human-like names (e.g., Sophia and Robot Lawyer Lisa), catchy, easy-to-remember names or easily identifiable symbols. To obtain trade mark protection, the mark must: (i) be distinguishable; (ii) not confuse consumers about the relationship between one party and another; and (iii) not otherwise deceive consumers with respect to the qualities of the product.

Trade marks can be registered or unregistered. Unregistered trade marks are protected under common law, in particular the law of delict (tort). Registered trade marks are regulated and

protected by the Trade Marks Act 194 of 1993 ("Trade Marks Act"). It is worth noting that ownership of a registered trade mark is established on a first-to-use basis rather than first-to-file. Registration of a trade mark is not mandatory to establish rights, but a registered trade mark makes proof of ownership easier in the case of infringement. Registration under the Trade Mark Act is *prima facie* proof of ownership and validity. A registered trade mark can be protected forever, provided that it is renewed every 10 years.

Unregistered trade marks are protected under the common law and an applicant would claim for "passing off" under the law of delict for the infringement of its goodwill. The delict of passing off consists of a representation, direct or indirect, by a manufacturer or supplier that his business or goods (or both) are those of a rival manufacturer or supplier. This is often more difficult to prove, as an applicant must show that: (i) the name, get-up or mark used by the applicant has become distinctive of his goods or services; and (ii) the name, get-up or mark used by the respondent is such or is so used as to cause the public to be confused or deceived into believing that the respondent's goods or services emanate from the applicant.

It is important to note that trade mark protection is territorial and that trade marks registered in other jurisdictions are only recognised insofar as they constitute "well-known marks" under the Trade Marks Act.

Well-known marks are protected under the Paris Convention on the Protection of Industrial Property of 20 March 1883 ("Paris Convention") and section 35 of the Trade Marks Act. Whether a mark is "well-known" or not will depend on the knowledge of the trade mark in the relevant sector of the public, including the knowledge which has been obtained as a result of the promotion of the trade mark. If a trade mark is determined to be "well-known", it will receive protection only if the owner is a resident of a nation, domiciled or has real and effective industrial or commercial establishment in a country which is a Paris Convention signatory.

Patents

A patent is a certificate in a prescribed form to the effect that a patent for an invention has been granted in the Republic. Patent protection is granted for a limited period of 20 years. The Patents Act 57 of 1978 ("Patents Act") defines the scope of patentable inventions and explicitly states what cannot be patented. Presently, the Patents Act explicitly excludes a "program for a computer" from the definition of invention and thus from being patentable. It may be in the future that, as in other jurisdictions, the law is developed to accommodate software patents. However, the hardware design that complements the software can be patented as an industrial design.

What are the applicable laws with respect to data ownership, security and information privacy?

Data ownership

Data is arguably one of the most valuable assets in today's world. Data is an intangible asset capable of being commoditised, owned and sold. Ownerships depends on from where it originates and the form it takes. Certain data constitutes personal information and shall be regulated by data protection laws including the Protection of Personal Information Act 4 of 2013 ("POPI").

Information privacy

The right to privacy is enshrined in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed". In order to give effect to the right to privacy, POPI

was promulgated. POPI is data protection legislation primarily modelled on the European Union general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions, including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of POPI. It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable, technical and organisational measures to prevent unlawful access. Whilst POPI has been promulgated into law, the substantive provisions of POPI are not yet in effect (only the provisions relating to the establishment of the Information Regulator and procedure for making regulations are currently in effect). The commencement date of these provisions of POPI will need to be determined by the President, but this is likely to be later in 2020. Once POPI comes into effect, parties shall have a one-year grace period to comply with it.

Not all data processed in an artificial intelligence or big data context involves personal information and human interaction, but a large spectrum of it does, and this has a direct impact on individuals and their rights with regard to the processing of personal information. Typical AI applications make it possible to collect and analyse large amounts of data in order to identify attitude patterns and predict behaviours of groups and communities. The risks related to the use of data in this context is also to be considered. For example, POPI, as does the GDPR, also requires responsible parties (data controllers) to clearly disclose the purpose for which collected data will be used. The use of AI potentially exposes data subjects to different risks or greater risks than those contemplated initially, and this could be considered as a case of further processing personal information in an unexpected manner. AI produces profiles and decisions that are based not just on data that a data subject has consensually submitted, but on data sometimes obtained without the knowledge or consent of a data subject.

Information security

At present, the current legal framework relating to cybercrime and cybersecurity in South Africa is a hybrid of different pieces of legislation and the common law, which has not kept up with the dynamic nature of technology and international standards. This prompted the drafting of the Cybercrimes Bill [B6-2017] ("Cybercrimes Bill") which will, *inter alia,* consolidate and codify numerous existing offences relating to cybercrimes, as well as create a variety of new offences which do not currently exist in South African law. Before the Cybercrimes Bill becomes law, it will need to be passed by both houses of parliament, undergo a public participation process and receive presidential assent. At the time of writing (March 2020), the Cybercrimes Bill remains with the selection committee in one of the houses of parliament which is processing responses to public submissions made to it.

However, until the Cybercrimes Bill becomes law, most cyber-related crimes, such as hacking and phishing, are regulated under the Electronic Communications and Transactions Act 25 of 2002 ("ECT Act"). It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the ECT Act relating to cybercrime offences and cybersecurity.

Antitrust/competition laws

Internet access is a critical aspect to enable growth in big data analytics, artificial intelligence and machine learning. Currently in South Africa, a significant portion of internet traffic in South Africa is through mobile data. The cost of mobile data in South Africa has been historically high when compared to other countries. Cable.co.uk ranks South Africa 143rd in the world in terms of mobile data costs. However, this is likely to soon change as the South

African Competition Commission conducted a formal market inquiry into data services and ordered two of South Africa's biggest mobile operators to drastically reduce their data prices and has also been conducting a formal market inquiry into data services. The decrease in mobile data costs will help bolster the amount of data available for big data analytics within South Africa and increase the customer base for apps using AI and machine learning.

As seen above, competition law is well established in South Africa. The South African Competition Commission is very proactive in enforcing the Competition Act 89 of 1998 ("Competition Act") and trying to facilitate market growth and fairness in South Africa. Competition law is well established in South Africa, and the South African Competition Commission is very proactive in enforcing the Competition Act. For instance, according to its annual report for the financial year 2018/2019, the Competition Commission levied administrative penalties to the value of 333 million Rand (approximately €18.24 million).

The Competition Act prohibits certain activities amongst competitors (horizontal relationships) and amongst a firm and its suppliers and/or its customers (vertical relationships).

For horizontal relationships, activities such as price-fixing, collusive tendering and market division between competitors are prohibited. More broadly, any agreement or concerted practice by firms or an association of firms that have the effect of substantially preventing, or lessening, competition in a market are prohibited, unless a party to the agreement, concerted practice, or decision can prove that any technological, efficiency or other pro-competitive gain resulting from it outweighs that effect.

For vertical relationships, any agreement between parties is prohibited if it has the effect of substantially preventing or lessening competition in a market, unless a party to the agreement can prove that any technological, efficiency or other pro-competitive gain resulting from that agreement outweighs that effect. This includes a supplier of goods imposing a minimum resale price to firms purchasing and on-selling their goods and/or services.

What happens when machines collude?

Machine collusion will mainly arise in horizontal relationships and could arise in a number of different contexts.

For instance, two competitors may both utilise software that uses price algorithms to determine the price of a particular type of good or service; e.g., a new camera. If the software is given the capabilities to interact with each other, or, if they have a sophisticated program through which, using machine learning, they can develop these capabilities, then it is theoretically possible that they may "collude" and simultaneously increase the price of the camera in order to ensure that both firms make a greater profit without the risk of losing business to their competitor.

Currently, the Competition Act does not expressly deal with machine collusion. However, the Competition Act does state that a firm is held directly liable for prohibited activities where its employees, staff and directors are involved in prohibited activities on its behalf. Thus, we are of the view that where machines, owned and under the control of and/or instructed by a company, engage in prohibited and anti-competitive activities, our law shall similarly hold the company/companies directly responsible and liable.

What antitrust (competition law) concerns arise from big data?

With the ever-increasing analysis capabilities of big data, firms can successfully utilise data that was previously too large and unrefined to come up with strategies to improve their business model and analyse the market in which they operate in more depth.

This has the potential to have positive effects by increasing the level of competition in a particular industry and allow market disruption with new entrants. Smaller firms and new

entrants can use big data analysis to successfully analyse gaps in the market. Businesses can also, through big data analysis, address consumer dissatisfaction and obtain information previously unknown to both the customer and the business.

For example, in South Africa, one of the newer banks was able to gain significant market strides in the banking sector by successfully identifying a gap in the market; i.e., because customers with lower incomes were not opening bank accounts because the monthly bank fees were too expensive, the bank then came up with a price-per-transaction model that encouraged these customers to open an account.

Companies need to also be conscious of the data analysis and even raw big data that they share with others within the same industry. This is because the Competition Act prohibits the sharing of information between competitors if it has the effect of substantially preventing or lessening competition in a market (unless its technological, efficiency or other pro-competitive gains resulting from such sharing outweighs that effect).

For example, if different companies are all members of an industry body, and at one of these industry body meetings, commercially sensitive information of the competitors (even if it is only large volumes of raw data) is shared, then these companies run the risk of violating anti-competitive laws.

Board of directors/governance

What governance issued do companies need to be aware of, specific to AI and big data?

Companies, more particularly the board of directors of the company, need to ensure effective and secure data management when implementing AI and utilising big data sets. Directors owe certain fiduciary duties to the company and must understand and ensure data is lawfully obtained, stored and used within a specified purpose. Companies will adopt and rely on AI-enabled technology to improve decision-making and management, but it is critical to note that the ultimate responsibility and oversight duties still reside with the board and individual directors. Unless the Companies Act 71 of 2008 ("Companies Act") or common law is developed to provide otherwise, AI and big data will play a supporting function for more effective governance.

The King IV Report on Corporate Governance for South Africa – 2016 ("King IV") is a set of voluntary principles in the area of corporate governance. Companies listed on the Johannesburg Stock Exchange are required to comply with King IV by law. In particular, King IV has a specific focus on the oversight of information and technology management. The board of the company is specifically tasked to make sure it proactively monitors cyber incidents and ensure that it has systems and processes in place from a cybersecurity perspective. Failure by a company to prevent, mitigate, manage or respond to an incident amounts to a breach of directors' duties, both under the common law and the Companies Act.

Under the common law, a breach of fiduciary duties may apply, and the director can be held liable for any losses, damages or costs. Section 76 of the Companies Act sets out standards of directors' conduct, and that a director must always act in good faith, for a proper purpose, in the best interest of the company and with a degree of reasonable care, skill and diligence. Failure to prevent, mitigate, manage or respond to an incident may amount to a breach of directors' duties under the Companies Act.

How does AI and big data affect the due diligence process for boards of directors?

AI has the capability to reduce the workload of a director and make working and decision-making more efficient, quicker and arguably cost-effective. For example, AI-enabled technology can scan, process and organise large data sets in a due diligence exercise and

highlight possible risks more quickly than a human would be able to. The director or professional can then interpret those risks and make a judgment call accordingly. Some AI technologies are capable of highlighting risks and offer solutions based on machine learning, which may remove the need for ultimate judgment from a human entirely. However, as discussed above, a director still retains certain duties to the company and would be ultimately responsible for any decision made by a computer program.

How do AI and big data affect a board's fiduciary duties?

The Companies Act imposes a positive duty on directors to manage the business and affairs of the company. As previously discussed, directors have certain duties which they owe to the company, which include common law duties and duties created under the Companies Act: more specifically, the duty to act in good faith and for a proper purpose in the best interests of the company; and also acting with due care, skill and diligence. Directors may, however, delegate all or any of its management powers and authority to some other person and in those matters involving skills or expertise within the delegatee's competence. However, as in the case of delegating to a human, the ultimate duty remains with the instructing director who cannot shirk his or her fiduciary duty through delegation. Directors will retain the ultimate management function even where a power has been delegated.

AI will certainly permeate the board room, but it is unlikely that South Africa will witness robo-director appointments anytime soon. Only natural persons may serve on the board of directors of a company. Therefore, it is not possible for a robo-director (or AI program) to be appointed to the board.

Regulations/government intervention

Specific laws relating to AI, big data or machine learning in South Africa

AI and machine learning

Unlike other jurisdictions, South African regulators have not yet caught up with the rapid pace of AI technology. South Africa has not yet formalised any policy documents or entered bills to parliament for the regulation of AI. However, the President has appointed members to the Presidential Commission on the Fourth Industrial Revolution ("4IR Commission"), which will assist the government in taking advantage of the opportunities presented by the digital industrial revolution. The task of the 4IR Commission, which will be chaired by the President, is to identify relevant policies, strategies and action plans that will position South Africa as a competitive global player. In late 2019, the 4IR Commission submitted a draft diagnostic report to the President regarding South Africa's 4IR plan and identified available opportunities. The final report is expected to be presented to cabinet in 2020.

Although AI and machine learning are not yet specifically regulated, there are signals that government is building the groundwork for implementation across various industries. For example, in late 2019 the South African regulator responsible for, among other things, the licensing of spectrum surprised the telecommunications industry by publishing a memorandum on the licensing of those parts of the spectrum required to enable 5G. The memorandum invited interested parties to submit their views of the licensing for radio frequency in the ranges of 700MHz and 800MHz, 2.3GHz, 2.6GHz and 3.5GHz by the end of January 2020. Access to 5G technology will allow for industries to explore further AI capabilities and we anticipate interesting new business opportunities shall arise as a result.

Big data

"Big data" as a concept is not specifically regulated, but to the extent that a party wishes

to analyse data sets which include personal information, POPI will be applicable (once commenced). POPI imposes various conditions which must be complied with in respect of the lawful processing of personal information. Personal information can only be processed if, *inter alia*, the data subject consents to the processing, processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party, or processing is necessary for pursuing the legitimate interest of the responsible party. Therefore, a party wishes to use process personal information will need to consider what the implications are from a data protection perspective.

Implementation of AI/big data/machine learning into businesses

What are the key legal issues that companies need to be aware of?

To keep abreast of the trends in their industries, maximise revenue and better understand their consumers, most businesses are increasing their use of AI, big data and machine learning.

When utilising these technologies, one of the most critical legal issues that all businesses should consider is data protection law, which is primarily covered by POPI. As mentioned above, personal information may only be processed for a specific, explicitly defined and lawful purpose (such as where a data subject's consent has been obtained).

Often, businesses wish to utilise big data analysis and AI to further process personal information. An example of this is where a financial provider utilises AI software to analyse which of its customers have mortgage bonds, and then offers such customers its household insurance. This would not be in line with the original purpose for which this information was provided (i.e., so that the customer can take out a home loan); therefore, this further process must be legally justifiable under one of the recognised grounds under POPI.

Businesses are encouraged to review their policies and agreements with customers and their suppliers to ensure that they comply with POPI.

POPI also requires businesses to secure the integrity of personal information in their possession or under their control with appropriate and reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information. With businesses storing more big data than ever before, a data breach can have devastating consequences and expose a business to significant civil liability as well as administrative penalties. Thus, it is important that businesses ensure that they have in place proper security measures which adhere to international best practice.

Civil liability

What are liability considerations when using AI technology? Where does the liability fall when AI fails?

In South Africa, civil liability can be divided into contractual and delictual (tort) liability. Currently, AI is not recognised as having its own civil liability.

In order for a plaintiff to establish a civil liability claim, such plaintiff must establish that the defendant acted negligently or with intention. An exception to this is strict liability, a common example of which is vicarious liability in employment relationships. In these instances, an employer (often a legal entity) is held liable for its employees' acts (or omissions) that are performed in the course and scope of their employment, which result in delict being committed; e.g., where a construction worker negligently drops a pile of bricks on someone passing the construction site, seriously injuring them.

We are of the view that persons utilising AI technology will similarly remain responsible even in the absence of fault (strict liability) for delicts and their lack of fulfilment of their contractual obligations due to the AI technology.

In South Africa, it is customary for information technology ("IT") contracts that include a service or the licensing of certain software to contain the following warranties that the service provider shall perform:

- their obligations in a professional manner; and
- in accordance with the relevant service levels.

Service levels are targets used to measure or to track the performance of a system and/or service. Service levels in a contract are usually accompanied by service credits. Service credits are deductions from the amount that a client shall pay to a service provider under a contract due to a failure to meet a service level. Thus, if a service level is not met regardless of whether or not AI technology was used, the relevant service credit shall apply and the service provider shall remain contractually liable. Similarly, where a service provider has indemnified a client for a loss due to using its services/system, then it shall remain contractually liable to that indemnity even if AI technology is used.

Sometimes, a service provider may not be the creator or developer of the AI technology. In such instances, where the AI technology fails, it may be possible for a service provider to claim for damages/losses from the developer where its contractual agreement with the developer has warranties or indemnities similar to those in the preceding paragraphs or other liability provisions.

Where the client is a natural person or a small juristic person (consumer), they may also be able to hold both the service provider and developer liable under the Consumer Protection Act 68 of 2008 ("CPA") where the AI technology is considered unsafe, defective or of a poor quality. This is because the producer, importer, distributor and retailer are all deemed to include an implied warranty of quality under the CPA. The CPA also contains a similar right to quality services for a consumer. This is, however, confined to the supplier (i.e., service provider).

What impact does AI have on negligence and malpractice?

It is also likely that in malpractice suits, a person that used AI technology, even where such software is unsupervised, will not readily escape liability as a court is likely to find them negligent (i.e., having not acted in accordance with the reasonable person standard or failing to perform a duty of care or adhere to a professional standard) on the basis that they used the technology without the proper level of care and oversight expected by a reasonable person in their position, or that a reasonable person would not have found the technology appropriate and/or of the acceptable standard for the task that it was used for. In professions such as healthcare and law, whilst AI technology can greatly assist in the generation of faster results, the results would still need to be interpreted by the relevant healthcare practitioner or legal practitioner and cannot be relied on in isolation. Failure to exercise this level of oversight by the relevant practitioner may be a breach of a professional duty, and liability would then attach to the relevant practitioner.

Criminal issues

What if an AI robot or system commits a crime directly?

CR Snyman (2015) Criminal Law, 6th Ed. identifies that most crimes in South Africa have a few essential requirements, namely:

- conduct;
- causation;

- unlawfulness;
- capacity; and
- fault (either intention or negligence).

Where a machine has "committed" a crime such as fraud, under current South African law, that machine shall not itself be found guilty of the crime. This is because current law only recognises conduct that was carried out by human beings as crimes.

Machines also cannot be found guilty of committing a crime, because, like animals and inanimate objects, they are not deemed to have the legal capacity to commit any crime. Where the fault requirement is intention, South African law has not yet developed to recognise a machine, that would likewise not be considered able to act with a direction of its will, as having committed a crime.

Even the Cybercrimes Bill (not yet in effect in South Africa), which seeks to revolutionise the criminal law landscape in South Africa by creating crimes such as cyber fraud and cyber extortion, does not provide for instances where AI (and not a human) is "responsible" for a crime.

Consequently, we are of the view that until South African law is developed to specifically allow for machines to be held directly liable for their crimes, the person who controls and/or instructs the machine would be held responsible for the crime. This view is strengthened by the fact that currently, where an animal is incited by a human to attack another human, it is the human who incited the animal who will be found guilty of committing a crime of assault or murder.

What is not yet clear is how our law shall deal with machines and software that have such sophisticated systems that they are able to independently develop, through machine learning, the capabilities to "commit" crimes without any input from their developers or owners.

What if AI causes others to commit a crime?

It is also possible that AI robots shall cause others to commit crimes.

Renowned author and biochemist Isaac Asimov provides a classic example of this in his book, *The Naked Sun* (1957). A robot unprompted by the perpetrator hands its detachable metallic arm to an enraged but unarmed woman, who in a blind rage strikes and kills a man with the metallic arm.

While we have not yet developed humanoid AI robots to such a level of generalised artificial intelligence and mobility, it is not impossible to imagine instances where AI could enable others to commit crimes. For instance, a piece of AI software could be developed to hack into a website containing financially sensitive information, and then make this information publicly accessible on social media platforms. Persons could then use this information to steal money and unlawfully access other persons' accounts.

For the reasons above, the persons committing the crime and instructing/supervising the machine in its hacking of the website (once the Cybercrimes Bill comes into effect and hacking is a recognised crime) would be held responsible for the crimes.

Discrimination and bias

What laws apply to AI or machine learning systems that produce biased results?

AI is not perfect or impartial. It is possible that biases will exist in the data that AI programs as, in reality, it is a human-built algorithm which will reflect such human bias. For instance, if the training data used in machine learning and/or development in AI programs contains inherent biases this could in turn affect the effectiveness and neutrality of the AI program.

Depending on the context in which such data is used, various anti-discrimination laws may apply, including but not limited to:

- the Constitution, which promotes equality as a central and inalienable right. Unfair discrimination on one of the listed grounds in section 9 is unconstitutional;
- the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 was promulgated to give effect to section 9 of the Constitution, and to prevent and prohibit unfair discrimination and harassment, promote equality and prevent hate speech;
- the Employment Equity Act 55 of 1998 provides, *inter alia*, that no person may unfairly discriminate, directly or indirectly, against an employee on one or more of the listed grounds; and
- the Competition Act prohibits a dominant firm from discriminating between purchasers of like goods/services in terms of prices charged, if that discrimination leads to an anti-competitive effect. However, conduct involving differential treatment of purchasers is not prohibited if the dominant firm can establish that the differential price makes only reasonable allowance for the difference in costs results from the different method of supply/distribution.

Given South Africa's discriminatory past under apartheid, if South African society is to embrace AI to its full potential, there needs to be trust in the AI programs and the AI solutions produced. An important element of this trust is widespread reliability and a belief in the fairness and authenticity in the results produced using AI and machine learning.

Acknowledgment

The authors would like to thank Lee Shacksnovis, an Associate in the Technology, Media & Telecommunications practice of Cliffe Dekker Hofmeyr, for her contribution to the preparation of this chapter. Lee specialises in commercial, information technology, intellectual property, data protection law and telecommunication law. She has experience in drafting a broad range of information technology and sourcing agreements and regularly advises clients on compliance with privacy laws and data protection regulation in South Africa. Lee has worked in a variety of industries and sectors, both locally and internationally but her interests lie in the financial services and healthcare industry.

Tel: +27 21 481 6453 / Email: lee.shacksnovis@cdhlegal.com

Fatima Ameer-Mia
Tel: +27 11 562 1898 / Email: fatima.ameermia@cdhlegal.com

Fatima Ameer-Mia is a Director in the Technology, Media & Telecommunications practice in Johannesburg. Fatima specialises in commercial, information technology, telecommunications, intellectual property and data protection law. She also has a special interest in the fields of e-commerce, fintech and matters relating to cybercrime and information security. Fatima advises clients, both locally and internationally, on general commercial matters and transactions with a technology related focus – such as software development, licensing, outsourcing, and a wide range of managed services. Her expertise extends to fintech, health-tech, insure-tech and data protection across a diverse range of industry sectors, especially financial services, retail and healthcare.

She regularly advises on data protection and information security, including providing training, seminars, risk assessments and governance frameworks on cybersecurity and data protection laws.

Christoff Pienaar
Tel: +27 21 481 6350 / Email: christoff.pienaar@cdhlegal.com

Christoff Pienaar is a Director and National Head of our Technology, Media & Telecommunications practice. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions.

Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Nikita Kekana
Tel: +27 21 481 6334 / Email: nikita.kekana@cdhlegal.com

Nikita Kekana is an Associate in our Technology, Media & Telecommunications practice. Nikita specialises in commercial, information technology, intellectual property and data protection law. Nikita also has a keen interest in artificial intelligence, machine learning and privacy law. Nikita completed her LL.B. at the University of Cape Town in 2016.

Cliffe Dekker Hofmeyr Inc.

11 Buitengracht Street, Cape Town, 8001, South Africa
Tel: +27 21 481 6350 / URL: www.cliffedekkerhofmeyr.com

Spain

Sönke Lund
Grupo Gispert Abogados & Ecomistas

Trends

Spain still faces a serious delay in relation to artificial intelligence and robotics, technologies which need urgent development in Spain. Such development needs adaptation in basically two fields: financing and legislation.

Between 2009 and 2015, the investment destined to R&D&I was reduced by half in Spain, to the extent that Spain in innovation rankings was placed alongside countries like Croatia, Poland, Latvia, Hungary, Greece, Slovakia, Cyprus, Italy, Malta, Lithuania, Estonia, Portugal and the Czech Republic, with only one group below that, which included Bulgaria and Romania. In the ranking, Spain places 17th out of 28, well below its economic weight. According to the EU Commission, between 2010 and 2016, performance has even worsened, hampered by a lack of funding and public support, low SME contribution, low entrepreneurship, lack of venture capital funds to invest, no private funding for public projects, or few large foreign-controlled companies, among others.

While other countries designate relevant funds for research on artificial intelligence, the Spanish government is still studying how to address this problem.

As for legislation, even being within the legal framework of the European Union, where studies for new positions have been ongoing since the beginning of 2017, Spain is far behind, as these initiatives are basic and influential in terms of financing.

On behalf of the European Union, important terms are already mentioned, such as "electronic person". This term brings with it other new considerations, such as a new ethical code or even a basic income. In this way, this electronic person will contribute in some way to the development of the country in which it is situated. Another strong question studied is the establishment of a clear legal responsibility for the acts of this person. The main idea, after ruling out possible liability of the manufacturer, is the creation of a fund or compensation insurance. This fund would be responsible for taking legal costs if, for example, an autonomous car is involved in a traffic accident.

However, there are two initiatives, as part of the Digital Agenda for Spain, that promote investment in artificial intelligence and robotics. This same Digital Agenda has as one of its main objectives to promote R&D&I in the industries of the future, although theoretical and with little real action. These two initiatives were included in the Agenda in 2015 in order to support the development of these sectors, and are specifically: the National Plan for Smart Cities; and the Plan to Promote Language Technologies.

This National Plan for Smart Cities, designed in 2015, has been relieved by the Smart Territories Strategy, with the idea of continuing the work carried out by the previous Plan. In this context, the MOBILus project has to be mentioned. MOBILus is headed by Barcelona

and consists of a partnership of 48 members from 15 countries, and has been chosen by the European Institute of Innovation and Technology (EIT) to lead its Knowledge and Innovation Community. The work of the consortium focuses on moving people, connecting communities, supporting the business fabric and reimagining public spaces.

More recently, the Ministry of Science, Innovation and Universities (MCIU), in line with the 2018 Communication from the European Commission to the European Parliament, the European Council, the Council and the Economic and Social Committee on AI for Europe, and the subsequent Coordinated Plan on AI, has worked on a Spanish R&D Strategy in Artificial Intelligence. The MCIU created in November 2018 the Working Group Artificial Intelligence, which is dedicated to the design of this Strategy. The Strategy for AI in R&D&I in Spain establishes a series of Priorities that will be framed in the new Spanish Strategy for Science, Technology and Innovation (EECTI) 2021–2028 and that will have to be developed in initiatives and activities defined and financed through the State Plans for Science, Technology and Innovation (PECTI), mobilising the synergies between the different levels of public administration and through the co-development of the public and private sectors. A condition in the development of technologies and applications of AI linked to this Strategy will be to avoid the negative bias and prejudices of society, such as in relation to gender, race or other forms of discrimination, and from which AI decision-making systems must be freed.

Situation in 2020

What the year 2020 will bring for the next decade and the future for Spain is currently uncertain, as the consequences of SARS-CoV-2 (COVID-19) on the development of artificial intelligence, machine learning and big data may be extremely different, without it being possible to make predictions at this stage. Already at the end of 2019 and the beginning of 2020, there were tendencies that were strongly focused on the sector of "remote medicine", which should have a positive effect on, among other things, medical care in sparsely populated areas, the exchange of anamnesis data in diagnostics and the relief of hospitals. Whether autonomous driving will remain a trend in 2020, as expected, because machine learning tests will increase or automation will be raised from level 2 (partial automation through assistance systems) to level 3 (operator automation) or even to level 4 (high automation) is in the stars. The expected boom in robotics and the associated general artificial intelligence, the use of digital assistants in the work area for routine activities, chatbots, etc. is also influenced by current conditions.

Ownership/protection

In Spain, the most complex algorithms, despite the fact that they are often the result of research, design and programming by a subject or entity, and the importance they have in the business model of more and more companies, still do not receive the necessary attention and protection.

They have no place in industrial property rights, and their inclusion in copyright may be insufficient and forced. However, a possible solution for this normative vacuum could be found in the analogical application of Article 133.1 of the Royal Legislative Decree 1/1996 of April 12, 1996, approving the consolidated text of the Law on Intellectual Property, which protects databases not for their originality, but for the simple existence of a substantial investment at an economic level, use of time or effort. Another situation is given regarding the most complex algorithms which are usually written in computer code which turns the algorithm into software.

Regarding the ownership of such complex algorithms, according to the law of intellectual property, the exploitation rights of the algorithms carried out in the scope of an employment relationship are assigned to the employer, differentiating two assumptions. On the one hand,

when they are carried out as a result of the employee's habitual activity; and on the other hand, when the algorithms are carried out outside the employee's normal functions.

With respect to the first assumption, the regulation simply attributes to the employer the results of the employee's work. This is a logical question derived from the fact that the worker was hired precisely to carry out the particular algorithm, so there is no doubt that the worker's salary is sufficient justification for the employer to appropriate the result of the work.

In the second case, in case of creation of an algorithm outside of the usual functions of the worker, Intellectual Property Law *ex lege* gives the employer the exploitation rights to the computer program created by the worker, without having to pay any compensation.

The Supreme Court and doctrine have come to understand the application of this assumption exceptionally and only when there is no doubt that the requirements – the express instructions of the entrepreneur – have been met.

This regulation – regarding the computer programs created by employees – launches a "wager" of all or nothing. If the employer can prove that he gave precise instructions to the worker to create the concrete algorithm, the worker will have no economic right over him, even if he performed it outside of his usual functions or for what he was hired to do in the company. On the contrary, if the company cannot prove it, the worker will have all the economic rights over the algorithm, without the company being able to do anything.

In short, if the algorithm is created following specific instructions from the employer, he will be the owner of the algorithm; if, on the contrary, the worker creates the algorithm on his own – with the company's computers or with his own computers, in his working hours or leisure time – he will be the owner of the algorithm.

In fact, the only means available to companies to protect this valuable intangible asset is the figure of trade secrets.

With the publication of the new Directive for the protection of trade secrets, and the resulting transposition rule in Spain – Law 1/2019 on Commercial Secrets – the protection of trade secrets, and therefore of the algorithms that may be included in this category, has been significantly extended, recognising protection measures that will allow companies to protect these valuable intangible assets against third parties; and from now on, this type of protection has some legal certainty, although in some cases it is not yet sufficient.

Antitrust/competition laws

The use of data is not a new phenomenon regarding antitrust and data advantage issues – in non-digital markets maintaining customer databases, conducting consumer surveys and market research have long been business activities. However, digitisation of the economy has had an enormous effect on the nature, sources, applications and the volume of data. Actually, the risk of foreclosure associated with the concentration of data is being looked at in the context of merger control, which does not exclude the use of antitrust enforcement tools to tackle behaviour related to artificial intelligence and big data activities, as exclusionary or exploitative "big data" conduct could lead to enforcement action. Nevertheless, theories of harm underlying the prohibition of illicit conduct are premised on the capacity for a company to obtain market power from its data, unmatched by its competitors. Before it can be determined whether data contributes to the strengthening of a market position, the context of the reality and extent of such "data advantage", the features found in online markets as network effects, multi-homing, and market dynamics, conducive to the market or not, have to be considered from the beginning. Two aspects appear to be of relevance here: the scarcity *vs.* replicability of data; and the scale of the data trove.

Access to data by an operator does not automatically preclude access by other operators. Multi-homing by customers or the diversification of services offered by a single source opens opportunities for the collection of user data. Access to data may be conditioned on the company's capacities to build a large database on personal or non-personal data. This, in turn, depends on the extent to which network and experience parameters as well as scale economies act as entry barriers. The availability of third parties' data, i.e. coming from data brokers, may cancel out big data accessibility concerns, but the availability and impact of external sourcing depends very much on the nature of the data concerned and the applicable rules – from personal data protection, trade secrets and intellectual property in general.

In terms of scale (and scope) of data, their strategic relevance and foreclosure opportunities must be verified. These two points depend on which level a company may gain economic benefit, and beyond which data volume those benefits decrease or cease to exist as a whole. The scope of data may also be as relevant as scale, depending on the market conditions of each case.

Among other possible problematic uses of data, the following stand out:

Collusive agreements: An algorithm can facilitate an agreement between competitors that limits competition, i.e. by means of the automation of the pricing process which facilitates monitoring and coordination between competitors. The ability to obtain price information in real time can encourage automated price coordination; for example, when retailers sell competing products on sales platforms and, instead of competing independently, agree not to lower their prices to improve each other's offer, using monitoring and repricing tools.

Algorithms and barriers to entry: An algorithm may also be used to limit entry into a particular market or it may be used to exclude a competitor from a particular platform or to favour its own services or products or services of other companies (*Google* case).

These and other behaviours are being monitored and analysed by the various competition authorities and international bodies aware of the new scenarios and the limits of current regulations. In fact, the debate on competition law, big data and algorithmic fairness is generating great response among different interest groups, as the use of artificial intelligence favours the formation of cartels and strengthens their stability.

Respect for the rules protecting free competition is not only the responsibility of companies operating in a given market, but is also the responsibility of companies that do not operate in the market affected by the illegal conduct. Therefore, a programmer who is approached by two companies or a single company in order to design an algorithm that can be used to break the rules of the game may be sanctioned.

The ECJ confirmed in the *AC-Treuhand* case that a consultancy company "may be held liable for an infringement of Article 81 EC (Article 101(1) TFEU) where that company contributes actively and with full knowledge of the facts to the setting up or maintenance of a cartel between producers operating in a market different from that in which that firm operates". The rules protecting free competition, and in particular Article 101 TFEU and Article 1 of the Spanish Antitrust Law, prohibit all types of agreements and concerted practices which distort competition irrespective of the market in which the parties operate and of the fact that only the commercial behaviour of one of them is affected by the conduct.

Board of directors/governance

What governance issues do companies need to be aware of, specific to AI and big data?
Companies need to be aware that the organisational challenges associated with AI occur at multiple levels: collaboration and work modes; resources; and strategic forecasting, combined

with big data, entail tailored governance. When data enters into automated systems that are capable of learning, deduction, suggestion, diagnostics and even prediction, governance should take into account the more specific and multi-scale evolution of data AI.

The effects of big data and AI on internal communication, education and awareness benefit from the support of the top management. AI can provide a strategy of process optimisation thanks to automation and the development of predictive analyses (maintenance, fraud, loss of customers) and service personalisation.

To get big data and AI well established, a company needs the resources to create a big data trove, a mature plan for data upstream, the process of skills building and opening up an ecosystem for its teams, and to familiarise its teams and management with the technology. In order to archive satisfactory results, companies must inventory data, create governance units, define roles and responsibilities and decide who would own the data.

How do AI and big data affect the due diligence process for boards of directors?

Due to the pervasiveness of electronically stored information and search and retrieval technologies, discovery has changed rapidly. The due diligence process is getting more and more automated, leading to cheaper, faster transactions with better risk management. Random indexing programs already offer an efficient solution to the challenge of classifying, organising, prioritising and highlighting corporate documents. Thanks in large part to advances in e-discovery, M&A due diligence tasks are ripe for automation and significant gains may be realised.

How do AI and big data affect a board's fiduciary duties?

As machine learning algorithms become more advanced, we should expect to see more of them employed in innovative ways in governance issues. Robot-advisers on due diligence and fiduciary duties are merely another example of these algorithms replacing a traditionally "human" role, which may encourage a partially new approach to the "business judgment rule" which was enshrined in Spanish law by the Reform Bill of the Spanish Companies Law (*Ley de Sociedades de Capital*) to improve corporate governance (passed on November 17, 2014). The question of how a machine algorithm could possibly comply with this rule may be addressed with the fact that robot-advisers are no less likely to meet this rule than human advisers. Robot-advisory firms can design their programs to mitigate the concerns that have given rise to fiduciary duties. Accordingly, the fiduciary duty rule may provide an adequate liability scheme for current robot-advisers, ensuring that victims of algorithms falling short of the standard can recover from the registered investment adviser who can best shoulder the cost; that is, the firm. As machine algorithms grow in sophistication, the law and even more the courts will consistently face questions of who should be held at fault for increasingly more independent and truly autonomous decisionmakers. The EU is actually designing a legal regime for autonomous machines. Alternate liability regimes, like implementing a compensation fund, should ensure that victims of autonomous machines receive relief. These schemes could also provide some protection to manufacturers and developers by providing limited liability in return for payments to the fund. Thus, companies should take steps to create an appropriate corporate framework, like an insurance or compensation scheme, and adopt changes that can handle this increasingly complex issue, thereby paving the way for a legal and corporate regime with the capacity to handle truly autonomous technology.

How are AI and big data affecting communication plans to shareholders, vendors, etc.?

Generally speaking, the effects of AI on communication plans are mainly on the capacity to analyse the digital landscape of networks, to report on exact insights and real-time updates,

and to deliver information to even the smallest target audiences in innovative ways using virtual and augmented reality applications. Further, shareholders will be able to virtually join a conference from their offices and experience a briefing or information session. In addition, the delivery of faster responses to crises, following pre-set parameters as part of human-centric contingency plans and the ability to prevent corporate communications from inconsistencies, discrepancies, conflicts and predictions of oncoming issues, will increase the reputation of the company. AI will also help expose false information and identify deception.

Regulations/government intervention

Spain does not have any specific laws relating to AI, big data or machine learning, nor is the Spanish legislator considering specific laws. But as machines are increasingly likely to replace positions occupied by humans and new technologies are turning to the spheres of robotics, which may prompt calls for the improvement of regulation, and faced with the avalanche of applications of artificial intelligence, the European Union has already made proposals for laws to frame the various controversies that may occur. Besides that, we have already mentioned the Spanish strategy paper above.

In February 2017, the European Parliament Resolution of recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) was adopted.

Parliament's Resolution calls on the Commission to establish a common legal framework throughout the EU in the field of robotics and artificial intelligence, so as to be able to anticipate the regulatory projects on the subject in certain countries.

Some of the axes of this proposal are the need to establish ethical standards, to determine liability in the case of autonomous vehicles – proposing the existence of compulsory insurance and supplementary funds for possible victims of accidents involving these vehicles – or the creation of a specific legal personality for robots to clarify the determination of liability in the event of causing damage.

Accordingly, Parliament called on the Commission, on the basis of Article 225 TFEU, to present a proposal for a directive, on the basis of Article 114 TFEU, on the rules of civil law in the field of robotics, on the basis of a series of recommendations grouped into the areas, amongst others, of:

- General principles concerning the development of robotics and artificial intelligence for civil use.
- Research programmes on the possible risks and opportunities of artificial intelligence and robotics in the long term.
- Ethical principles, in view of the potential for empowerment of the use of robotics, in the light of human health and safety, freedom, privacy, integrity and dignity, self-determination and non-discrimination, and the protection of personal data, reflecting the complexity of the field of robotics and its social, medical and bioethical implications on the development, design, production, use and modification of robots.
- Personal data and the flow of personal data, to ensure that civil legislation in the field of robotics complies with the General Data Protection Regulation and the principles of necessity and proportionality for the proper use of robotics and to avoid possible security breaches.
- Autonomous transport (all forms of remotely piloted, automated, connected and autonomous road, rail, inland waterway and air transport, including vehicles, trains, vessels, ferries, aircraft and drones, as well as all future forms resulting from development and innovation in this sector) is the area which most urgently needs EU and global

rules to ensure the cross-border development of autonomous and automated vehicles, as it will have an impact on aspects such as civil liability (liability and insurance), road safety, all environmental issues (e.g. energy efficiency, use of renewable technologies and energy sources), data issues (e.g. access to data, protection of personal data and privacy, exchange of data), ICT infrastructure issues (e.g. high density of efficient and reliable communications) and employment (e.g. creation and loss of jobs, training of drivers of heavy vehicles for the use of automated vehicles).

- Care and medical robots that allow medical and care staff to devote more time to diagnosis and better planned treatment options, improve mobility and integration of disabled or elderly people, etc.
- Civil liability regime for damages caused by robots, pointing out that the risk management approach does not focus on the person "who acted negligently" as personally responsible, but on the person or persons capable of minimising the risks and managing the negative impact, imputed proportionally to the actual level of instructions given to the robots and their degree of autonomy – so that the greater the learning capacity or autonomy and the longer the robot's "training", the greater the responsibility of the trainer.
- Access to source code, input data and robot construction details which should be available when necessary, to investigate both accidents and damage caused by "intelligent robots" and to ensure their continued operation, availability, reliability, safety and security.

Another noteworthy initiative refers to the setup of standards for artificial intelligence.

The European Commission has issued a Communication COM(2018) 237 Artificial Intelligence for Europe, marking a European initiative on artificial intelligence. This initiative is considered essential for the future of the European economy and the leadership of national industry in a competitive global market. It recognises the role of standardisation as a response to the challenges posed by this key technology, especially in terms of safety, reliability and ethical considerations. CEN and CENELEC standards support compliance with European legislation through harmonised standards. The European Commission foresees that the application of artificial intelligence will impact on compliance with several European directives, for which there is a solid normative body.

Artificial intelligence is advancing continuously and is widely affecting industries such as automation, data management and integration of intelligent technologies. Society is also impacted as artificial intelligence changes the way business works, production is optimised and new worker profiles are needed. Thus, AI affects a multitude of sectors in which standardisation has great relevance: intelligent manufacturing; robotics; autonomous vehicles; virtual reality; health; visual recognition; data manipulation and analysis; domestic appliances; and cybersecurity. In all these sectors there are currently essential standards that must be updated to incorporate this new technology.

The European standardisation system is essential to avoid the fragmentation of the European Single Market and to guarantee a people-centred approach to artificial intelligence, ensuring that society benefits. The European standardisation bodies, CEN and CENELEC, constitute a trusted environment for the development of artificial intelligence, as European standards deal with aspects of reliability, privacy and security. In addition, they work together with the international organisations ISO and IEC, where the ISO/IEC JTC 1 SC 42 Standardisation Committee on Artificial Intelligence has just been created, which is already developing the first two international standards on terminology and reference framework for these systems using machine learning.

Sönke Lund
Tel: +34 934 594 071 / Email: sonke.lund@grupogispert.com

Sönke Lund has a degree in Law from the University of Hamburg, and was admitted to the Hamburg Bar in 1991 and to the Barcelona Bar in 1997. He is specialised in Intellectual Property Law, Private International Law, Consumer Law, Distribution and International Sales, IT and TMT.

Amongst others, he is a member of:

- the IBA (International Bar Association) where he is the former Chair of the International Sales Committee, Vice-Chair of the Alternative and New Law Business Solutions Committee and Member of the Advisory Board of the Agricultural Law Section. Sönke also has experience in the: Dispute Resolution Section; Energy, Environment, Natural Resources and Infrastructure Law Section; and Intellectual Property, Communications and Technology Section;
- the ALAI/ALADDA (*Association Littéraire et Artistique Internationale*/ *Asociación Literaria y Artística para la Defensa del Derecho de Autor*);
- the GRUR (German Association for Protection of Intellectual Property – Special Committee on Data Law – International Development Section);
- the Academic Association of Cartel Law (*Studienvereinigung Kartellrecht*); and
- German Association of Lawyers – Working Group of International Economic Law (*Deutscher Anwaltverein – Arbeitsgemeinschaft Internationales Wirtschaftsrecht*).

Sönke was also a contributor to the Spain chapter of *The ICLG to: Telecoms, Media & Internet Laws & Regulations 2018*.

Grupo Gispert Abogados & Ecomistas

Avinguda Diagonal, 416, pral 1ª, Barcelona 08037, Spain
Tel: +34 934 594 071 / URL: www.grupogispert.com

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.[1] 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.[2]

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.[3] 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.[4]

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 11th 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.[5]

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*[6] 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.[7] 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.[8] 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.[9]

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.[10] 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.[11] 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.[12] 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),[13] 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.[14]

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.[15]

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/rapporter/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

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

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

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

Switzerland

Clara-Ann Gordon & Dr. András Gurovits
Niederer Kraft Frey Ltd.

Trends

In Switzerland, the use of artificial intelligence (AI), machine learning and big data continues to increase. It is a fact that digitalisation plays a key role in our daily life, and indirectly puts pressure on all economic stakeholders to follow development.

AI as a whole raises a lot of questions. Therefore, in Switzerland, different institutions are conducting studies to answer questions regarding topics such as ethics and the risks and opportunities of AI innovation.[1]

In addition, the Swiss federal government has funded research programmes on the effective and appropriate use of big data, and has incorporated a new federal working group specialised in AI.[2] On behalf of the Federal Council, this working group examined the challenges of AI and need for action. Although, there is still room for improvement in a number of areas, the report (published in December 2019) shows that Switzerland is well-positioned for the application and challenges of AI.[3] The legal framework in Switzerland is generally sufficient to meet the new challenges posed by AI and there is currently no need for fundamental adjustments.[4] Nevertheless, applications for AI that challenge the legal system in certain areas are emerging.[5] Strategic guidelines for the Federal Council are to be derived from the report by spring 2020.[6]

According to the latest AI research, the majority of companies are not yet prepared for implementing AI into their businesses, nor do they know how to maximise the use of AI.[7] However, there are some leading tech/telecom companies headquartered in Switzerland that have already started implementing and developing their own AI. For example, a leading Swiss telecom company is using chatbots in its customer support service, and is offering support for other businesses to implement the use of AI, in order to maximise income and respond to market demand.[8] Moreover, many companies already use intelligent wearables in order to help facilitate their employees' work and improve their results.

Hence, from a pragmatic point of view, the use of AI is trending; whereas from a regulatory perspective, there are still questions left unanswered. When dealing with new and innovative digital technologies, Switzerland follows the following principles:

- Bottom up-approach: Switzerland wants to provide an optimal, innovation-friendly environment for the development of new technologies, while leaving the choice of specific technologies to individual actors.
- Application perspective: When assessing new technologies, the focus is on application and its effects. Regulation with regard to AI should not be based on the technology itself; it only starts where there are gaps or risks to the fundamental rights of the data subjects.
- Technology neutrality: Switzerland pursues a technology-neutral legislative and regulatory approach. Rules should be as competition-neutral as possible. The legal

framework should not be geared to individual technologies, but should treat comparable activities and risk – whenever possible – equally.
- Market failure: If there is no market failure and the use of AI lies within the framework of private sector activities, regulation should generally be avoided.
- Legal admissibility: The use of AI *per se* does not justify any need for government action or regulation. The regulatory question only arises when AI affects fundamental rights or causes market failures.
- Special attention to fundamental rights: If fundamental rights are affected by AI or if the current legal system proved inadequate, there is a need for regulatory action.
- Necessary legal basis for government action: The state (administration) and judiciary may in principle use AI as a tool, even if this concerns the legal position of persons, provided that the necessary legal basis exists.[9]

Ownership/protection

Copyright. Under Swiss copyright law, only works that are considered an intellectual creation with an individual character are protected by copyright (art. 2 para. 1 of the Swiss Copyright Act (CopA)). AI as software generally meets these requirements. However, works created by AI cannot be considered intellectual creations as they are not made by humans. These works currently cannot be copyrighted and the author cannot acquire copyright derivatively.

It must be clarified how copyright law is to deal with the fact that many forms of AI require enormous amounts of data for the training process, which are at least partially protected by copyright. The data usually has to be duplicated for use by AI, which is basically a copyright infringement. This could represent a considerable hurdle for the development of AI.[10]

Copyrighted works are protected for 70 years after the death of the author (or 50 years in the case of computer programs; art. 29 para. 1 of the CopA).

Patents. Under Swiss law, patents are granted for new innovations applicable in industry. Anything that is obvious having regard to the state of the art is not patentable (art. 1 para. 1 and 2 of the Swiss Patents Act). AI may be patentable under Swiss law; however, there are issues regarding results created by AI. The assessment of whether these results are obvious, and therefore patentable, should be carried out from a machine's viewpoint and not a human's one. Moreover, AI cannot be named the inventor, but it also does not act as a mere tool in order for its operator to be named inventor. Furthermore, according to prevailing opinion, patent law in Switzerland only permits natural persons as inventors in the legal sense (or legal persons, depending on the interpretation). The recognition of AI systems is, however, excluded due to their lack of legal capacity.[11]

Data ownership. Under Swiss law, there are no property rights (in the sense of the Swiss Civil Code) to data, since data is intangible. The Federal Act on Data Protection (FADP) does not convey ownership to data either, as it only regulates protection against unlawful data processing.[12] Protection of and factual ownership to data could therefore, e.g., come from intellectual property rights such as copyright. As a rule, data can be protected by copyright only if it is considered an intellectual creation with an individual character (see above). However, data generated by machines does not fall under the protection of Swiss copyright law, as it is not recognised as an intellectual creation (art. 2 para. 1 CopA).[13] On a more positive note, databases may be protected by copyright as collected works (art. 4 para. 1 CopA).

As part of the ongoing revision of the FADP, not only will the right to formational self-determination in the use of information and communication technology be increased, but the

transparency of data processing by information and communication technology users will also be improved. In addition, the control of data subjects over their data and the powers of the Federal Data Protection and Information Commissioner will be strengthened.[14]

As decisions based on AI systems are often not comprehensible, precautions must be taken to ensure transparency. A form of explainability is therefore also provided for in the draft of the new FADP: The data controller must inform the data subject of any decision taken exclusively on the basis of automated processing of personal data that has legal effects on or significantly affects the data subject (art. 19 para. 1 of the new FADP). The data subject may request that the decisions are reviewed by a natural person (art. 19 para. 2 of the new FADP). Where data subjects exercise their right to information, the data controller must state that an automated individual decision has been taken and on what logic this decision is based on (art. 23 para. 2 let. f). Art. 19 and 23 of the new FADP are not applicable where humans interfere in the decision-making process and where AI merely served as a decision-making aid. Special traceability requirements also exist for non-automated individual decisions of authorities that are made with the help of AI and concern the legal status of a person. If an authority therefore bases its decision on AI, it is essential that the system provides information about the information and criteria it takes into account, the assumptions it makes, and the relevant reasons for the result.[15]

Another challenge arises when companies use AI in their interaction with customers, e.g. via chatbots. These can be used in a variety of ways to answer consumer questions. Since it is possible to talk to a chatbot like a human being, the consumer may not be able to tell that it is a machine. If consumers were not informed in advance about the interaction with AI systems, the Swiss Federal Act against Unfair Competition could be applied in Switzerland.[16]

De lege ferenda, in doctrine various solutions have been debated for this problem. One solution could be the qualification of data as "*lex digitalis*".[17] Data would then fall under traditional ownership and possession rules, thus would be assigned to an owner who would benefit from all the proprietary rights. The second solution proposes the introduction of ownership protection specifically for data, whereas the last thesis proposes a new intellectual property for data.[18]

Antitrust/competition laws

Algorithms and big data. In Switzerland, protection against unfair competition is assured by the Competition Commission (ComCO) using the legal instruments provided by the Swiss Cartel Act (CartA). Swiss competition law does not contain specific provisions on algorithm-driven behaviour, ergo its general rules apply.

Thus, if, or when, machines collude, under Swiss law only explicit collusion is considered unlawful, unless there is tacit collusion as part of an abuse of market power.[19] Collusion (be it explicit or tacit) requires the subjective component of the "concurrence of will" or "consensus". This component distinguishes unintended mistakes of the algorithm from unlawful intended collusive restrictions of competition.

Under art. 5 para. 3 (a) CartA, agreements between companies on the same level of the production and distribution chain which directly or indirectly fix prices are presumed to eliminate effective competition and are thus prohibited. The same interdiction applies in the case of agreements between undertakings at different levels of the production and distribution chain (art. 5 para. 4 CartA). Therefore, if competitors agree to fix prices using algorithms, or even AI, these agreements are unlawful (i.e. hub and spoke cartel). However, if an algorithm is faulty and makes an unintended mistake, there is no consensus between competitors and there should be no sanction for the company.

Any abuse of a dominant position is unlawful, pursuant to art. 7 CartA. Because algorithmic computer programs can now store, collect and process a large amount of data, antitrust concerns relating to big data also have to be considered. Big data can put companies in dominant positions on the market. The Essential Facilities Doctrine is an example of how big data issues can relate to the abuse of a dominant position. Is data an essential facility to which the owner has to grant its competitors access?

Board of directors/governance

There are no AI- and big data-specific guidelines of which the board should be aware. In general, Swiss companies need to be aware of the Swiss Code of Best Practices for Corporate Governance when they perform their corporate governance.

The board of a Swiss company (company limited by share or a limited liability company) is responsible for the overall supervision and management, with its duties listed in art. 716a CO. The members of the board of directors are jointly and severally liable for any damages caused by an intentional or negligent breach of those duties.

Regulations/government intervention

There are no specific regulations in relation to AI, machine learning or big data. To our knowledge, so far, the Swiss federal government has founded research programmes and established specialised institutions in these fields, but no current or upcoming regulations have been announced.

However, based on a recent study[20] conducted by the Federal Office of Communications, a three-point strategy was proposed which, first, suggests the creation and maintenance of a national data infrastructure that would enable a nationally coordinated and internationally networked infrastructure. Second, the Office calls for stricter privacy and competition law rules for the internet sector specifically. And, thirdly, the implementation of the principle of personal data sovereignty is required as a long-term solution in order to empower data subjects to have better control over their data.

Implementation of AI/machine learning/big data into businesses

AI creates immense opportunities for businesses. However, there is also a great risk of the abusive use of AI.

Legal difficulties which companies would face when implementing AI/big data into their businesses are, in particular, data protection and financial trading rules, as well as regulating liability. Businesses need to plan for a budget for legal structuring of the use of AI/big data, as well as compliance. They should also implement a chapter on AI/big data into their codes of conduct.

Data protection. Big data and AI go hand in hand. On the one hand, AI needs a great amount of data to function and learn. On the other hand, big data techniques use AI to extract value from huge sets of data. Swiss data protection law, however, was not created with AI or big data in mind.[21] The FADP is only applicable to the processing of personal data. In particular, factual data and geo data do not fall within the scope of application. Data that is anonymised (meaning that no connection to a person can be established) does not fall under the FADP, either. However, since big data facilitates the identification of persons through the inclusion of huge amounts of data, Swiss data protection rules can become applicable even though the processed data was anonymised at some point.[22] Differential Privacy, a

method to avoid re-identification of data subjects by adding "randomness" to a data set, can be implemented to avoid this. As soon as the FADP becomes applicable, however, the processing has to be in line with the general principles of data processing set out in art. 4 *et seq.* FADP, *inter alia*, the principles of lawful processing, good faith, proportionality, purpose limitation, etc. Compliance with the transparency prerequisite and obtaining consent for data processing can be a challenge when big data is concerned, as it is hard to keep track of the processing. The purpose of the data collection also needs to be clearly defined, which can be problematic. The principle of data minimisation is an inherent contradiction to how big data works, as big data only functions by processing huge amounts of data over a long period of time. The same is true for the limitation of the retention period for data.[23]

Financial trading. Market manipulation by AI/algorithms has to be avoided pursuant to art. 143 of the Financial Market Infrastructure Act. Therefore, it is prohibited to use algorithmic trading to give out false or misleading signals regarding the supply of, demand for or market price of securities. Supervised institutions that engage in algorithmic trading must employ effective systems and risk controls to ensure the avoidance of such misleading signals.[24] Art. 31 of the Swiss Financial Market Infrastructure Ordinance (FMIO) then requires market participants that pursue algorithmic trading to record all orders and cancellations, and to possess effective precautions and risk controls that ensure that their systems do not cause or contribute to any disruptions in the trading venue.

Liability. As the situation regarding liability can be unclear (see below), businesses are advised to contractually regulate responsibility and liability for any damages caused by AI/big data.

Other legal issues/examples. As businesses implement AI/big data into their daily business, they need to ensure that they are compliant with the law. For example, big data is nowadays often used in the hiring process ("hiring by algorithm"). Therefore, labour law provisions also have to be adhered to. When algorithms make hiring decisions, the person responsible has to ensure that the algorithm does not discriminate against anyone (i.e. based on age, sex, nationality, etc.). According to the general prohibition of discrimination under labour law in art. 328 CO, algorithms are not allowed to be programmed in such a way that they discriminate directly. They must also not discriminate indirectly, i.e. in spite of neutral regulation they may have disadvantageous effects for different groups of employees (based on race, age, sex, nationality, etc.), unless this is objectively justified and proportionate. However, there are hardly any deterrent sanctions against discriminatory behaviour. It was not until May 2016 that the Federal Council established that there are gaps in the protection against discrimination in private law. The general prohibition of discrimination under labour law is supplemented by special statutory prohibitions of discrimination, which, however, offer only very selective protection: For example, the Gender Equality Act prohibits any direct or indirect discrimination based on sex (art. 3). The Disability Discrimination Act only applies to federal employment relationships, but excludes the area of private-law employment relationships. The general prohibition of discrimination under labour law (art. 328 CO) does not provide a satisfactory solution to address the problem of possible discrimination by algorithms.[25] Data-related rights of employees, pursuant to art. 328b CO, also play a key role. The provision sets forth that the employer may only handle data to the extent that such data concerns the employee's suitability for the job, and are necessary for the performance of the employment contract.[26] It is questionable whether the professional element required by art. 328b CO is given if the algorithm takes into account data whose information content lies in the correlation between non-work-related data and work performance.[27]

Civil liability

There are no specific provisions under which an employer could be held liable for damages caused by artificially intelligent machinery. General civil liability rules are applicable.

Contractual. Contractual liability plays a key role, as many AI services will be provided under agency contracts pursuant to art. 394 *et seq.* CO. In this context, as well as generally, Swiss doctrine is discussing the widening of the concept of "faithful performance", which includes human supervision of AI. It is, however, unclear how far this supervision should go. Regarding sales contract liability, it is the seller that is liable for any hardware errors of an AI robot (art. 197 CO).[28] Moreover, doctrine is debating the possibility of disclaiming liability for subcontractors such as software suppliers in general terms and conditions.[29]

Non-contractual. Art. 41 CO generally regulates civil liability for damages incurred not in relation to contracts. The person who causes the loss or damage is obliged to provide compensation. The proof of burden for any such loss or damage lies with the injured party. Art. 55 CO regulates the liability of employers for any loss or damage caused by employees or ancillary staff in the performance of their work. Furthermore, the Swiss Product Liability Act regulates liability specifically for damages incurred by faulty products. Software as a product can fall under the provisions of the Product Liability Act.

If AI causes damages in Switzerland, we need to distinguish whether such damages were caused by a faulty product, mistakes the AI made on its own, or through wilful programming.

In the case that the AI makes a mistake on its own, the producer is not liable because he cannot be held responsible for the "decisions" of the product. Liability for the operation of autonomous information systems must always be linked to the act or omission of an offender. In addition, machines do not act intentionally (i.e. with knowledge and will), negligently (i.e. without taking into account the consequences of their lack of caution) or culpably (i.e. personally accusable), nor do they develop judgement (i.e. subjective insight, ability to form wills and ability to implement wills).[30] If, however, damages are incurred due to product defects of the AI (i.e. faulty programming), the producer is liable under the Product Liability Act or art. 55 CO. Product safety liability should also be considered. The injured party can, therefore, file claims against the producer and seek compensation.[31]

Moreover, it is important to take into account whether the manufacturer of the software and the producer of the end-product are different entities. In this case, the manufacturer cannot be held responsible for the damages caused by the end-product.

Specifically, liability for accidents caused by self-driving cars can be allocated to the driver as well as the owner, according to art. 58 of the Swiss Road Traffic Act. The owner's liability is a liability for the consequences, and is not dependent on any culpability on the part of the owner.[32]

Each case is different; for example, factors like when the product was released on the market could play a role when assigning civil liability, therefore a case-by-case analysis is recommended. The Federal Council currently considers the existing regulations to be sufficient. So far, the application to robots has not resulted in any gaps in responsibility. However, this assessment does not exclude the possibility that sooner or later the question of specific regulatory requirements will arise. In other cases, the legislator has reacted by introducing a strict liability. Damage caused by the new technology is therefore attributed to a person who will then be responsible for the damage regardless of fault. Anyone who benefits from the new technology should also assume the risks associated with it.[33]

Criminal issues

Under the Swiss Criminal Code, there are no specific provisions regarding felonies or misdemeanours committed by AI. General Swiss criminal law applies. The Federal Council currently also considers the existing provisions in criminal law to be sufficient. In fact, offences committed using robots can be prosecuted like any other crime committed by a person using an object. Thus, as things stand at present, there is no legal loophole that the legislator would have to fill.[34]

Swiss criminal law requires the personal culpability of the offender. If an AI robot or system commits a criminal act, it cannot be criminally liable under the current and traditional Swiss criminal law doctrine. The same is true if AI causes someone to commit a crime. Therefore, attribution of the criminal act to the creator/programmer or the user of the AI robot or system should be considered. If an AI robot or system was intentionally programmed to commit a criminal act, the creator or programmer is criminally liable. If it was programmed correctly but intentionally used in a way that resulted in the committing of a criminal act, the user is criminally liable. The creator/programmer as well as the user can only be punished for the negligent commission of a criminal offence if negligence is also explicitly punishable for such criminal offence.[35]

Under art. 102 of the Swiss Criminal Code, it is even possible to assign criminal liability to a corporation if the activity cannot be attributed to a natural person, and if the criminal offence was committed in the exercise of commercial activities in accordance with the object of the undertaking. The undertaking can be fined up to CHF 5 million for such liability. If AI commits a felony or misdemeanour and the requirements mentioned above are met, the corporation using the AI can be held liable.

Discrimination and bias

Under Swiss law, there are no applicable regulations in relation to discrimination and bias of machines. The logic discussed above may apply accordingly.

National security and military

In Switzerland, AI is being used by the military, but so far there are no specific laws relating to AI, machine learning or big data.

* * *

Endnotes

1. SECO press release "*The pros and cons of artificial intelligence*", https://www.seco.admin.ch/seco/en/home/seco/nsb-news.msg-id-71639.html.
2. The Swiss Confederation on "*The Swiss Digital Action Plan*", 5 September 2018; also see The Swiss Confederation on "*Digital Switzerland Strategy*", September 2018.
3. https://www.sbfi.admin.ch/sbfi/de/home/das-sbfi/digitalisierung/kuenstliche-intelligenz.html.
4. https://www.sbfi.admin.ch/sbfi/de/home/aktuell/medienmitteilungen/news-anzeige-nsb.msg-id-77514.html.
5. https://www.sbfi.admin.ch/sbfi/de/home/das-sbfi/digitalisierung/kuenstliche-intelligenz.html.
6. https://www.sbfi.admin.ch/sbfi/de/home/aktuell/medienmitteilungen/news-anzeige-nsb.msg-id-77514.html.

7. Philipp A. Ziegler "*MSM Research AG - Research at a glance – Artificial Intelligence*", November 2018.
8. Joachim Hackmann "*Trends for 2019: How companies can use data better*", Teknowlogy Group, January 2019, commissioned by Swisscom and Teknowlogy/PAC.
9. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz'* an den Bundesrat", December 2019, 34–36.
10. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 40.
11. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 40.
12. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 634.
13. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 630.
14. Bundesamt für Kommunikation BAKOM, Geschäftsstelle Digitale Schweiz GDS, Aktionsplan, Digitale Schweiz, November 2019, 38.
15. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 37–38.
16. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 38.
17. Dr. Martin Eckert, LL.M. on "*Daten als Wirtschaftsgut – wem gehören digitale Daten*", 2016.
18. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 631.
19. Peter Georg Picht and Benedikt Freund on "*Wettbewerbsrecht auf algorithmischen Märkten*", sic!, November 2018, 669.
20. Prof. Thomas Jarchow and Beat Estermann on "*Big Data: Opportunities, risks and need for action by the Confederation*" – results of a study commissioned by the Federal Office of Communications.
21. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
22. Astrid Epiney on "*Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?*", Jusletter IT, 21 May 2015.
23. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
24. FINMA Circular 2013/8 on "*Market conduct rules*".
25. Isabelle Wildhaber/Melinda F. Lohmann/Gabriel Kaspar on "*Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädikativer Analytik am Arbeitsplatz*", ZSR vol. 138 (2019) I issue 5, 459, 470–471.
26. Isabelle Wildhaber on "*Robotik am Arbeitsplatz: Robo-Kollegen und Robo Bosse*", AJP 2017, 215 *et seq.*
27. Isabelle Wildhaber/Melinda F. Lohmann/Gabriel Kaspar on "*Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädikativer Analytik am Arbeitsplatz*", ZSR vol. 138 (2019) I issue 5, 459, 479.16.

28. Melinda F. Lohmann on "*Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse*", AJP 2/2017, 157.
29. Mario J. Minder on "*Artificial Intelligence: Eine Bestandesaufnahme im Jahr 2018*", sic!, 2019, 51.
30. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36.
31. Silvio Hänsenberger on "*Die Haftung für Produkte mit lernfähigen Algoritmen*", Jusletter, November 2018.
32. Dr. Martin Eckert and Luca Hitz on "*Selbstfahrende Autos: Zulässigkeit, Haftung und Datenschutz*", https://www.mme.ch/de/magazin/selbstfahrende_autos_zulaessigkeit_haftung_und_datenschutz/.
33. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36–37.
34. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36–37.
35. Nora Markwalder and Monika Simmler on "*Roboterstrafrecht*", AJP 2/2017, 173 *et seq*.

Clara-Ann Gordon
Tel: +41 58 800 80 00 / Email: clara-ann.gordon@nkf.ch

Clara-Ann Gordon is specialised in the areas of TMT/outsourcing, data privacy, internal investigations/e-discovery and compliance. She regularly advises clients in the above areas on contractual, governance/compliance and other legal matters, represents clients in transactions and before the competent regulatory and investigating authorities as well as before state courts, arbitral tribunals and in mediation proceedings, and renders opinions on critical regulatory and contract law topics in the said industry-specific areas.

She has advised on and negotiated a broad range of national and international IT, software and outsourcing transactions (also in regulated markets), has represented clients in technology-related court proceedings and international arbitration, and is experienced in data protection and secrecy laws, white-collar investigations and e-discovery, telecom regulations (including lawful interception), e-commerce and IT law.

Ms. Gordon regularly publishes in the field of technology (ICT) and frequently speaks at national and international conferences on emerging legal issues in technology law.

Dr. András Gurovits
Tel: +41 58 800 80 00 / Email: andras.gurovits@nkf.ch

András Gurovits specialises in technology (IT, telecoms, manufacturing, regulatory) transactions (including acquisitions, outsourcing, development, procurement, distribution), data protection, corporate, dispute resolution (incl. administrative proceedings) and sports.

He regularly advises clients on contractual, compliance, governance, disputes and other legal matters in the above areas.

He, thus, not only advises in these areas, but also represents clients before the competent regulatory and investigating authorities, state courts and arbitral tribunals.

Dr. Gurovits is distinguished as a leading lawyer by various directories such as *Chambers* and *The Legal 500*. Dr. Gurovits has been a lecturer at the University of Zurich for more than a decade. Presently, he is a listed arbitrator with the Court of Arbitration for Sport CAS/TAS in Lausanne and member of the Legal Committee of the International Ice Hockey Federation. He is also a member of the board of directors of Grasshopper Fussball AG.

Niederer Kraft Frey Ltd.

Bahnhofstrasse 53, 8001 Zurich, Switzerland
Tel: +41 58 800 80 00 / URL: www.nkf.ch

Taiwan

Robin Chang & Eddie Hsiung
Lee and Li, Attorneys-at-Law

Trends

Vision and government view

Taiwan's well-known information and communications technology ("ICT") and semiconductor industry has established a good foundation for intelligent technology development. According to the "Digital Nation and Innovative Economic Development Plan" and the "Taiwan AI Action Plan" announced by the Executive Yuan (i.e., the Cabinet of Taiwan) in 2016 and 2018 respectively, Taiwan has been seeking to develop world-leading AI infrastructure for device solutions and to establish a sound ecosystem that creates a niche market. Taiwan intends to become an important partner in the value chain of global AI technology and intelligence systems and will leverage the advantages in hardware and software techniques to promote AI technology among industries with, among others, test fields, regulations, and data-sharing environments. According to the Taiwan AI Action Plan, the government's view is that Taiwan is well positioned to take advantage of the opportunities in developing AI-related industries: (i) the industry leadership position in the manufacturing of ICT hardware; (ii) the vitality of Taiwan's small and medium-sized enterprises; (iii) vertical application of technology by government authorities and industries; and (iv) transparency of government data.

In addition to the above, the Ministry of Science and Technology under the Executive Yuan (i.e., the Cabinet of Taiwan) further announced the "AI Technology R&D Guidelines" in September 2019 to demonstrate the Taiwan government's commitment to improve Taiwan's AI R&D environment. Considering AI developments may bring changes to various aspects of human existence, the Taiwan government expects the participants to always be aware of such factors when conducting relevant activities and endeavouring to build an AI-embedded society with three core values, which are "Human-centred Values", "Sustainable Developments" and "Diversity and Inclusion". Deriving from the three core values, eight guidelines were published under the AI Technology R&D Guidelines for the guidance of AI participants, so that a solid AI R&D environment and society that connect to the global AI trends may be established. The eight guidelines are "Common Good and Well-being", "Fairness and Non-discrimination", "Autonomy and Control", "Safety", "Privacy and Data Governance", "Transparency and Traceability", "Explainability" and "Accountability and Communication".

AI is also expected by the Taiwan government to play an important role in the "5+2 Industrial Innovation Plan" ("5+2 Plan") as declared by the Taiwan government in 2018. The 5+2 Plan (which mainly focuses on seven industries, including smart machinery and the "Asia Silicon Valley" Project) is considered the core generator for Taiwan's next generation of industrial development. To facilitate the 5+2 Plan, the government has launched the "AI Talent Program", which aims to (i) cultivate 1,000 high-calibre talented persons in intelligent

technologies, (ii) train 5,000 talented persons in practical intelligent technologies, and (iii) attract foreign professionals by the year 2021. The "Act for the Recruitment and Employment of Foreign Professionals", as enacted in 2017, aims to attract foreign talent to increase Taiwan's competitiveness, which, according to the Taiwan AI Action Plan, would include AI development.

Key issues

With the developments in AI, machine learning and big data trends, it is generally observed that the more widely discussed legal topics in Taiwan are copyrights and intellectual property rights, legal liabilities and the impact on the existing regulatory regime in Taiwan. As of the date of this chapter, while to our understanding there still exists no court decision specifically addressing such issues yet, two laws have been promulgated in 2018 to cope with these new trends – these are: the law for a fintech regulatory sandbox (i.e., the "Financial Technology Development and Innovative Experimentation Act"); and the law for autonomous vehicles (i.e., the "Unmanned Vehicle Technology Innovation and Experiment Act"). The latter is considered one that may provide a more friendly environment for testing the application of AI and Internet of Things ("IoT") technology in transportation. Please refer to the "Regulations/government intervention" section for more details.

In addition to the above-mentioned legal issues, there have also been some discussions regarding the legal profession, such as how AI may impact the legal profession (e.g., whether AI will replace some of the jobs that lawyers do), whether AI-powered software/data analytics may be used as a tool or methodology in any legal cases (e.g., (for lawyers) to predict the outcomes of legal proceedings, and (for judges) to render a basis for making judgments with the assistance of algorithms and data).

Ownership/protection

AI and IP protection

When an AI technology is created, the first issue would be whether such technology can be protected by intellectual property rights, such as a copyright or patent.

Under Taiwan's Copyright Act, there are no registration or filing requirements for a copyright to be protected by law. However, there are certain features that qualify a copyright, such as "originality" and "expression". Therefore, while there is a type of copyright called a "computer program copyright" under Taiwan's Copyright Act, whether an AI is copyrightable would still depend on whether the subject AI has the required components (like the features described above) – especially the feature "expression" (instead of simply an "abstract idea"). Please note that there is a general view that an algorithm itself might not constitute a copyrightable work under the Copyright Act, but it would still depend on whether the AI has the required components. As to a new copyright developed by an employee of a company during the course of employment, where a work is completed by an employee within the scope of employment, the employee is the author of the work while the economic rights to such work will be enjoyed by the employer unless otherwise agreed by the parties.

As to patents, an inventor may file an application with Taiwan's Intellectual Property Office, and the patent right will be obtained once approved. According to the Patent Act of Taiwan, the subject to a patent right is "invention" and an invention means the "creation of technical ideas, utilising the laws of nature". As for a software-implemented invention, if it coordinates the software and hardware to process the information, and there is a technical effect in its operation, it might become patentable. Given that, whether an AI/algorithm is patentable would depend on whether it has the required components. As to a new patent developed

by an employee of a company during the course of employment, the right of an invention made by an employee during the course of performing his or her duties under employment will be vested in his or her employer, and the employer should pay the employee reasonable remuneration unless otherwise agreed by the parties.

IP rights arising from AI

How to determine the owner of the intellectual property of an AI-created work is expected to be a legal issue that will be widely discussed with the developments in AI. Currently, no intellectual property related laws or regulations have been specifically promulgated or amended to address this issue.

Before addressing this question, it is worth mentioning that, according to the view of many experts and scholars, AI development can be generally divided into the following three phases, and we are currently in phase 2:

(i) Phase 1: all intrinsic knowledge/information of AI is given by humans, and AI simply functions as a tool to respond to human query inputs. AI does not have the ability to learn or think.
(ii) Phase 2: AI learns through computer software designed by humans, which is called "deep learning". In addition to responding to human query inputs, AI is able to use its limited intrinsic perception and logic to help its users make decisions.
(iii) Phase 3: AI has evolved to have the ability to think for itself and act sufficiently like a human (i.e., it may have perceptions and emotions). That is, AI has a self-training ability, and the ability to evaluate, determine and solve questions.

With respect to phase 1, as AI merely functions as a tool utilised by humans to create a work or invention, the human (user of the AI) should be the owner of intellectual property (copyright or patent).

In phase 2, AI already has the ability of deep learning, and it is not merely a tool of humans. However, there would be issues as to whether AI has the ability to create an "original expression" under copyright law or to be an "inventor" under patent law, and if not, whether the human using the AI can be considered as the one who actually creates the "expression" or the invention. Such issues would be more important and cannot be ignored in phase 3, when AI has evolved to have the ability of independent thinking and can create an "expression" and make an invention like a human. Our preliminary view is that such issues might not be solved under the current IP regime in Taiwan; it is really a challenge faced by and needs to be addressed by the government, legislators, representatives of the court system and other legal practitioners in the future along with the development of AI.

Personal data protection

In Taiwan, personal information is protected by Taiwan's Personal Data Protection Act ("PDPA"); the collection, processing and use of any personal data are generally subject to notice and consent requirements under the PDPA. Pursuant to the PDPA, "personal data" is defined broadly as the: name; date of birth; I.D. card number; passport number; characteristics; fingerprints; marital status; family information; education; occupation; medical record, medical treatment and health examination information; genetic information; sexual life information; criminal record; contact information; financial conditions; social activities; and other information which may directly or indirectly identify an individual.

Under the PDPA, unless otherwise specified under law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of said individual's personal information,

subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area and persons authorised to use the data, etc.

Given the above, if a company wishes to collect, process and/or use any personal data for the purpose regarding AI and/or big data, it will be subject to the obligations under the PDPA as advised above.

Antitrust/competition laws

Under Taiwan's antitrust/unfair completion laws (i.e., the Fair Trade Act ("FTA") and its related regulations), the offender's "mental state" would be considered to determine the constituent elements of relevant types of violation. Take "concerted action" (i.e., so-called cartels), for example. Under Article 14 of the FTA, a "concerted action" generally means that "competing enterprises" at the same production and/or marketing stage, by means of "contract, agreement or any other form of mutual understanding", jointly determine the price, technology, products, facilities, trading counterparts, or trading territory with respect to goods or services, or any other behaviour that restricts each other's business activities, resulting in an impact on the market function with respect to production, trade in goods or supply and demand of services. The FTA further provides that: (i) the term "any other form of mutual understanding" means "a meeting of minds", whether legally binding or not, which would in effect lead to joint actions; and (ii) the "mutual understanding" of the concerted action may be presumed by considerable factors, such as market condition, characteristics of the good or service, cost and profit considerations, and economic rationalisation of the business conducts.

If the competing enterprises' actions are taken by the AI, there could be an issue of whether the actions are indeed led by "any other form of mutual understanding" among the enterprises in case no explicit contract or agreement exists among the firms. In such case, we think whether the firms really have a "meeting of minds" could be an issue when discussing and debating in court.

Board of directors/governance

The director's fiduciary duty and the obligation to act in good faith are set forth in Taiwan's Company Act. Pursuant to Article 23 of the Company Act, a director of a company shall be loyal and shall exercise the due care of a good administrator in conducting the business operations of the company. In case a director breaches such duty, he/she/it shall be liable for the loss or damage therefore sustained by the company.

As to the standards of "loyalty" and "due care of a good administrator" in conducting the business operations of a company, these are not explicitly stated in the Company Act or other relevant laws and regulations, and the general principle should be that the determination by the court in any given case should be based on the actual circumstances by objective and socially recognised criteria. Generally speaking, when discussing a contemplated proposal involving mergers and acquisitions or otherwise making an investment or a significant procurement plan that may involve a relatively huge amount of the company's expenditure, the board of directors may wish to have the company engage outside advisors or counsels (such as certified public accountants, lawyers, securities firms/investment bankers, real estate appraiser or other experts) to conduct due diligence and/or to provide their professional view(s) and/or opinion(s) on, for example, the fairness and/or reasonableness of the terms and conditions with respect to the contemplated transactions. By referencing and relying on experts' views and opinions, the directors may have a more solid basis to make decisions, so as to reduce the risk of potential breach of fiduciary duty claims.

We believe that the same principle applies in cases that involve AI-related issues. Despite the fact that there is no explicit court precedent and ruling in this regard as of the time of writing, we would say that in the case where the directors are not experts in such fields, in addition to the existing outside counsels, the directors/company would need to engage an AI expert for further advice during the due diligence process, as well as other decision-making processes if it involves any AI-related issues. The engagement of outside AI expert(s) should not only be a demonstration of fulfilling the fiduciary duty of the directors, but also a solid basis to support the legitimacy of the decision that is made.

Regulations/government intervention

Laws newly promulgated

According to our observation, Taiwan's government sector is aware of such AI trends and has proceeded to explore whether any existing laws and regulations, especially relevant legal restrictions, need to be adjusted accordingly. In early 2018, to promote fintech services and companies, the legislators in Taiwan promulgated a law for the fintech regulatory sandbox, the Financial Technology Development and Innovative Experimentation Act ("FinTech Sandbox Act"). The FinTech Sandbox Act was enacted to enable fintech businesses to test their financial technologies in a controlled regulatory environment. Although the FinTech Sandbox Act is not specifically designed for AI, machine learning or big data, the creators of new financial-related business models with AI or big data technology may test their new ideas and applications under such mechanism while enjoying exemptions from certain laws and regulations.

By referencing the similar spirit of the FinTech Sandbox Act, the legislators in Taiwan promulgated another law for a regulatory sandbox for autonomous vehicles/self-driving vehicles, the Unmanned Vehicle Technology Innovation and Experiment Act ("Unmanned Vehicle Sandbox Act") in late 2018, while the effective date is to be further determined. The Act is to provide a friendlier environment for testing the application of AI and IoT technology in transportation. The term "vehicle" under this Act not only covers cars, but also aircraft, ships/boats, and any combination thereof.

The rationale and the spirit behind the above two regulatory sandbox laws are similar. As mentioned above, these regulatory sandbox laws were enacted to enable the relevant businesses to test their new ideas and technologies within a safe harbour or sandbox scope permitted by such laws. An applicant needs to obtain approval from the relevant competent authority before entering the sandbox. Once the experiment begins, the experimental activities may enjoy exemptions from certain laws and regulations (such as certain licensing requirements and legal liabilities).

After completion of the approved experiments, the relevant competent authority will analyse the result of the experiment. If the result is positive, the relevant competent authority (the Financial Supervisory Commission for fintech sandboxes, or the Ministry of Economic Affairs for unmanned vehicles) will actively examine the existing laws and regulations to explore the possibility of amending them, after which the business models or activities previously tested in the sandbox could become feasible under law. Please note, however, that the sandbox applicant might still be required to apply for the relevant licence or approval from the relevant competent authority in order to formally conduct the activities as previously tested in the sandbox.

We would like to draw your attention to the fact that one of the most critical prerequisites for entering the sandbox is that the idea and technology must be "innovative". As of the

time of writing, the regulatory sandbox for unmanned vehicles has not taken effect and, to our understanding, though several fintech applications have been filed with the Financial Supervisory Commission (the competent authority of the fintech regulatory sandbox), no experiment has completed the process. Therefore, it is still unclear which type of idea and technology would be considered "innovative" by the relevant competent authority and the impact the regulatory sandbox might bring to the existing regulatory framework. AI is evolving and subject to further observation.

Laws under review by the government

According to the Taiwan AI Action Plan, the Taiwan government is still evaluating the following issues so as to further determine whether any laws need to be enacted or amended to address AI development:

(1) The impact on employment and the labour market.
(2) The rights and obligations derived from the application of AI technology (e.g., whether AI should be considered a "person" from the perspective of certain legal fields, whether there will be intellectual property rights in an AI-created work, etc.).
(3) Applying AI in the government.
(4) Open data.
(5) Consumer protection for AI applications.
(6) Restrictions on AI applications.
(7) The legal system of the regulatory sandbox.
(8) The applications of telecommunications spectrum resources.
(9) Government procurement (e.g., the outsourcing concerning AI issues).
(10) Industry regulatory challenges and approach to AI.

In addition to the above, some legislators proposed the draft 'Basic Act for Developments of Artificial Intelligence' in 2019, which is intended to set out some fundamental principles for AI developments, to request the government to promote the developments of AI technologies, etc. The draft is still under review by the Legislative Yuan (the congress), and whether this draft will be passed is uncertain.

Civil liability

Currently, no laws or regulations have been specifically promulgated or amended to address the developments in AI. Current Taiwan laws do not recognise AI as a legal person, so it should not be deemed as a "person" from the perspective of the Civil Code; and from a Taiwan law perspective, it is still generally considered that AI cannot yet be responsible for civil liability.

As there have been no specific laws or regulations governing civil liability with regard to AI, the Civil Code and general legal principles in Taiwan should apply.

Contractual liability

Taiwan's Civil Code provides claims and remedies for breach of contract (unless otherwise agreed upon by the contractual parties). Since AI itself cannot be a "person" liable for contractual obligations, when a purchaser purchases an AI product which performs the contractual obligations using AI technology, but the AI fails to perform as agreed under the contract, the purchaser may claim against the other contracting party (seller) based on certain grounds provided by the Civil Code, such as "incomplete performance" and/or "warranties against defects", etc. Under such circumstances, the remedies available to the purchaser at the current stage include, among others, requesting the seller to repair the product, to replace the defective product with a faultless one, to reduce the purchase price, and/or to compensate for the damages, depending on the facts of the individual case.

Tort liability

As advised above, under current law, AI itself cannot yet be responsible for any civil liability. Therefore, in case of tort liability arising from the use of AI technology, the injured party would still need to prove that the torts fall within any of the specific types of tort under the Civil Code and/or the Consumer Protection Act ("CPA"). Said types of tort include, without limitation, the following:

(1) Article 184 of the Civil Code: A person who, intentionally or negligently, has wrongfully infringed the rights of another person should compensate such person for any damages arising therefrom. The prevailing view among the courts and scholars is that there should also be causation between the tortious conduct and the injury.
(2) Article 191 of the Civil Code: The injury, which is caused by a building or other works on privately-owned land, shall be compensated by the owner of such building or works, unless there is no defective construction or insufficient maintenance in such building or works, or the injury was not caused by the defectiveness or insufficiency, or the owner has exercised reasonable care to prevent such injury.
(3) Article 191-2 of the Civil Code: If an automobile, motorcycle or other motor vehicle which does not need to be driven on tracks while in use has caused injury to another person, the driver shall be liable for the damages arising therefrom, unless he has exercised reasonable care to prevent the damages.
(4) Article 7 of the CPA: A manufacturer shall be liable for any damage caused by its products, unless it can prove that the products have met and complied with the applicable technical and professional standards of reasonably expected safety requirements before such products are released on to the market.

Take self-driving cars (i.e., autonomous vehicles), for instance. If the AI embedded in the self-driving system causes injury, the injured person may wish to prove and convince the judge that the self-driving car falls within the meaning of "automobile" and the user should be considered the "driver" for the purpose of Article 191-2 of the Civil Code. If the injured person wishes to establish a claim under Article 184 of the Civil Code, he/she should prove that the "user" was negligent when using the self-driving car. Also, the manufacturer of such self-driving car may be held liable under Article 7 of the CPA if the court considers that it is unable to prove that the car has met and complied with the contemporary technical and professional standards of reasonably expected safety requirements before such car was released on to the market.

Based on the above, it may be inferred that it does not seem to be easy to establish a tort solely based on how AI "behaves" or "acts". As AI becomes more sophisticated and can become independent, it will be more difficult to establish and determine civil liability in the future. Given that, we believe that the relevant laws should be re-examined to determine how to establish civil liability arising from human activities involving AI and to address liability and risk allocation of AI.

Criminal issues

Under Taiwan law, criminal liability generally requires a person's mental state of "intention" or "negligence", depending on the types of criminal offences explicitly specified in the relevant laws. Currently, no criminal-related laws have been specifically promulgated or amended to address the developments in AI. Therefore, although there have not been many legal scholars' views on relevant issues in Taiwan, we believe that, under current law, AI would not be able to have the required "mental state" as mentioned above and therefore AI

itself cannot commit a criminal offence. Also, in principle, under the current Taiwan legal regime, only natural persons (i.e., individuals) are capable of committing crimes, save for certain exceptional circumstances where legal persons may be subject to criminal fines.

Given that, similar to the discussion on tort liability, with regards to the issue of determining whether a criminal offence has been committed, one would need to prove the required conditions of criminal liability, such as "intention" or "negligence" and "causation" on the part of the person "using" or "behind" the AI. Again, for instance, taking self-driving cars (i.e., autonomous vehicles), the prosecutor may need to prove that the "user" of the car really acted negligently, while the user may assert that the result was simply the "behaviour" or "act" of the AI, so there was neither negligence on the user's part nor causation between any act of the user and the result. Furthermore, it is generally considered that under Taiwan law and practice, the burden of proof is generally higher in criminal cases – which may make it even more difficult to establish a criminal offence. Therefore, with respect to criminal liability, legislators in Taiwan may need to consider and propose some amendments to the current criminal laws in order to address particular circumstances and criminal justice when facing challenges from developments in AI.

Discrimination and bias

In Taiwan, currently no court decisions have addressed the issues of discrimination and bias that may be caused by the use of AI algorithms and big data analytics. Also, no specific laws or regulations have been promulgated or amended to address such issues.

In this regard, we believe that more and more discussions will emerge in legal fields such as labour/employment law (with respect to sex, race, religion or belief, political views, etc.), privacy law, antitrust, and any other area where "equality" or "fairness" would be an important factor with respect to social life and economic activity. This would be a developing area in both the legal profession and court proceedings.

Robin Chang
Tel: +886 2 2763 8000 ext.2208 / Email: robinchang@leeandli.com

Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on banking, IPO, capital markets, M&A, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan, including providing advice on compliance and regulatory issues, setting up a banking branch or bank subsidiary in Taiwan and customer complaints. He has been involved in many M&A transactions of financial institutions. He has also been involved in government projects in e-payment regulations in Taiwan.

Eddie Hsiung
Tel: +886 2 2763 8000 ext.2162 / Email: eddiehsiung@leeandli.com

Eddie Hsiung is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State, USA. His practice focuses on M&A, securities and financial services, cross-border investments, general corporate and commercial, startups, etc. He is familiar with legal issues regarding the application of new technologies such as fintech (e-payment, digital financial services, regulatory sandboxes), blockchain (ICOs, cryptocurrencies, platform operators) and AI, and is often invited to participate in public hearings, seminars, and panel discussions in these areas.

He has participated in many corporate transactions (e.g., M&A, IPO) spanning a broad range of industries (tech, information, media, cable, private equity, bio-tech). He regularly advises leading banks, securities firms, payment service companies, etc. on transactional, licensing and regulatory/compliance matters as well as internal investigations. His practice also includes data protection.

Lee and Li, Attorneys-at-Law

8F, No. 555, Sec. 4, Zhongxiao E. Rd., Taipei, Taiwan
Tel: +886 2 2763 8000 / URL: www.leeandli.com

United Arab Emirates

Nadim Bardawil
BSA Ahmad Bin Hezeem & Associates LLP

Trends

Artificial intelligence ("**AI**") is the ability of machines to undertake day-to-day activities requiring a certain level of intelligence as opposed to natural intelligence observed in humans and animals.

The United Arab Emirates ("**UAE**") has not enacted any specific laws addressing the area of AI. However, the UAE government has already displayed a strong commitment to integrating AI in day-to-day government operations as displayed by the growing Smart Government initiatives.

A little less than three years ago, the UAE Strategy for Artificial Intelligence was launched, which is a unique government-led initiative to boost the inclusion of AI across nine different sectors: health; space; water; technology; education; environment; traffic; transport; and renewable energy. The AI Strategy was immediately followed by the UAE appointing the first ever Minister of Artificial Intelligence, responsible for overseeing the UAE's adoption of AI and future government projects.

One of the major initiatives of the Ministry of AI has been the launch of Think AI which enables discussions between the public and private sector for the most efficient and responsible adoption of AI in the UAE. The UAE has also launched AI Strategy 2031 with the goal of positioning the UAE as a global leader in AI by 2031.

Ownership/protection

As in most other jurisdictions, the protection of unique and novel technology as well as data is an important part of any company's continued success. IP creators in the UAE have access to the same types of protection mechanisms that are commonly used through the UAE's current IP laws consisting of UAE Federal Law No. 37 of 1992 on Trademarks, UAE Federal No. 7 of 2002 on Copyrights and UAE Federal Law No. 17 of 2002 on the Protection of Patents.

These laws alone, however, are not sufficient to protect all types of IP, especially in certain sectors where it can sometimes be difficult to explain the process and functioning of cutting-edge technology. We often see entities resorting to protecting the source code of algorithms using copyrights or resorting to protection by way of trade secrets; two helpful protection mechanisms but not sufficient in their own right.

Ownership of an AI algorithm remains a grey area in the UAE for several reasons:

(1) The UAE's current IP laws are not currently built to handle the specific nature of algorithm protection.
(2) While algorithms in their own right may be complex to protect, AI algorithms add an additional layer of complexity as the source code may be changed several times in the lifetime of the system or process that uses the specific AI algorithm.

With regards to data, the mainland of the UAE does not have a principal data protection legislation that exists in its own right. Data privacy and protection is addressed across a number of separate regulations, not specifically focused on data protection, save for UAE Federal Law No. 2 of 2019 on the use of IT and Telecommunications in the Healthcare Sector. We are aware that there is a draft federal data protection law that is currently being reviewed with the aim to have it resemble the standard set by the GDPR.

Certain free-zones have their own respective data protection legislation which only applies within the confines of said free-zone, such as the Dubai International Financial Center ("**DIFC**"), the Abu Dhabi Global Market ("**ADGM**") and the Dubai Healthcare City ("**DHCC**").

Dubai Law No. 26 of 2015 regulating Data Dissemination and Exchange in the Emirate of Dubai (the "**Dubai Data Dissemination Law**") also addresses data protection. The Dubai Data Dissemination Law only applies to Federal Government Entities that have data relating to Dubai, to Local Government Entities, and to persons who produce or spread data relating to Dubai.

Antitrust/competition laws

UAE Federal Law No. 4 of 2012 on the Regulation of Competition (the "**UAE Competition Law**") was enacted in February 2013 to protect and promote competition and anti-monopoly practices. Its principle aim is to assist entities in enhancing efficiency, competitiveness and consumer interests while achieving sustainable development in the UAE. The UAE Competition Law also aims to maintain a competitive market in accordance with the principle of economic freedom, by prohibiting restrictive agreements as well as any practice that leads to endangerment, limitation or prevention of competition.

The UAE Competition Law does not itself address situations where machines may collude to form a monopolistic environment or to stifle competition. Such a scenario forms part of a much larger discussion with regards to liability.

The UAE Competition Law does however, in Articles 1 and 2, specifically prohibit agreements which "*fix, directly or indirectly, purchase or sales prices of goods or services by causing increase, reduction or fixing of prices thereby adversely affecting competition*". It can be argued that machines that collude would be an act of indirect price fixing and therefore would be deemed illegal under the UAE Competition Law. We expect the UAE Competition Law to continue to evolve as machine learning and algorithms are increasingly used to set the prices of certain goods.

Board of directors/governance

The UAE has not yet enacted any specific legislation addressing the usage of AI or big data in the context of governance or the role of directors.

Articles 22 and 23 of UAE Federal Law No. 2 of 2015 (the "**UAE Companies Law**") state that directors must exercise the care of a diligent person and must perform actions in accordance with their company's objectives and within the remit of their powers. The UAE Companies Law does not expressly disallow the usage of tools such as AI or big data in making decisions; however, one would need to analyse what percentage of an individual director's decision has been influenced by AI or big data to understand if such a decision remains within the standard set out above.

As part of the UAE Strategy for AI, the UAE has decided to focus specifically on governance using AI tools and is dedicating a significant amount of investment to develop AI principles

and AI ethics guidelines. This project will without a doubt eventually impact the governance of companies in the UAE in the near future.

Regulations/government intervention

We are aware that as part of the UAE Ministry of AI's mandate, the Federal National Council of the UAE has been looking at how to amend existing UAE federal legislation to take into account the usage of AI and other machine learning systems to protect the community from any potential risks arising out of their increased use.

In late 2018, the UAE formed the AI Council to oversee the integration of AI in government departments and the education sector. In 2019, the AI Council launched the UAE National Program for Artificial Intelligence or BRAIN to highlight the advances in AI and robotics with a special emphasis on the UAE's policy objective to become a leading participant in the responsible use of AI and its tools globally.

In order to support the UAE in becoming a hub for cutting-edge technology companies and start-ups, UAE Federal Decree No. 25 of 2018 (the "**Futuristic Projects Law**") was passed to allow for the temporary licensing of companies which are involved in the usage of novel technologies or AI. The purpose of the Futuristic Projects Law is to allow for an *ad hoc* sandbox environment in the UAE should there be a project that is deemed innovative and important enough to be tested in the UAE.

The Emirate of Dubai has issued Executive Council Resolution No. 3 of 2019 regulating Test Runs of Autonomous Vehicles with the objective of achieving Dubai's strategy with respect to smart transportation and regulating test runs of autonomous vehicles to ensure that they are safe.

Civil liability

UAE Federal Law No. 5 of 1985 (the "**Civil Code**") does not specifically address liability considerations when using AI technology. As stated above, there has already been a call for the Civil Code and other fundamental UAE federal laws to be amended to include provisions addressing AI.

Criminal issues

UAE Federal Law No. 3 of 1987 (as amended) also known as the UAE Penal Code, does not contain any specific provisions regarding criminal liability of an AI system or machine.

Discrimination and bias

UAE Federal Decree No. 2 of 2015 as amended by UAE Federal Decree No. 11 of 2019 on Combating Discrimination and Hatred forbids discrimination and bias on certain grounds including religion, creed, race and ethnic origin, among others; it does not however address the discrimination of AI or machine learning systems.

National security and military

UAE Cabinet Resolution No. 21 of 2013 addressing data security for Federal Authorities (the "**Data Security Resolution**") specifically outlines how data belonging to the UAE federal government, authorities, ministries and other official entities must be stored, treated and disseminated, specifically requiring the localisation of data due to its sensitivity. The Data Security Resolution applies to service providers who work with the UAE military and who collect, process and/or store data such as security cameras or Cloud solutions.

Nadim Bardawil
Tel: +971 4 368 5555 / Email: nadim.bardawil@bsabh.com

Nadim heads BSA's TMT practice based out of the DIFC office in Dubai. He advises regional and international corporates on commercial matters, including mergers and acquisitions, joint ventures and corporate governance. Nadim specialises in advising entities operating in the technology, media and communication sectors where he advises on complex technology-related agreements, e-commerce matters, cybersecurity, e-gaming and data protection. Nadim also advises on regulatory matters primarily in the FinTech space where he represents technology and payment service providers as well as regularly advises on draft legislation involving new technologies. He also has particular experience assisting technology focused private equity and investment funds in their investment activity across the Middle East start-up industry.

Fluent in a number of key languages including English, French and Arabic, Nadim is admitted to practice in the State of New York and also holds a Business Management degree.

BSA Ahmad Bin Hezeem & Associates LLP

Level 6, Building 3, The Gate Precinct, DIFC, P.O. Box 262, Dubai, United Arab Emirates
Tel: +971 4 368 5555 / URL: www.bsabh.com

United Kingdom

Rachel Free, Hannah Curtis & Barbara Zapisetskaya
CMS Cameron McKenna Nabarro Olswang LLP

1 Introduction

The UK is one of a group of leading countries in AI technology and policy. It is regarded as a centre of expertise in research and application. The turnover of the UK's digital technology sector was estimated at £170 billion in 2015. The UK now has 1.64 million digital technology jobs.[1] In a recent study, the UK ranked first in the world for its operating environment for AI and third in the world in research.[2] The UK was also ranked third in the Global AI Index for private investments in AI companies in 2019, with the US and China taking first and second place respectively.

1.1 AI in the UK

In common with most jurisdictions, there is no statutory definition of AI in the UK. The UK Government, in its "Industrial Strategy White Paper", defines AI as "technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation".[3]

1.2 UK Government support for AI

The UK Government has identified AI and Big Data as one of the four Grand Challenges which will lead the UK to become "the world's most innovative economy". The government paper, "[p]utting the UK at the forefront of the artificial intelligence and data revolution",[4] sets out its ambition.

The four Grand Challenges aim to co-ordinate the work of business, academia and civil society to "innovate and develop new technologies and industries in areas of strategic importance". Accordingly, the use and deployment of AI should:

- make the UK a global centre for artificial intelligence and data-driven innovation;
- support sectors to boost their productivity through use of artificial intelligence and data analytic technologies; and
- position the UK to lead the world in safe and ethical use of data and artificial intelligence, and help people to develop the skills needed for jobs of the future.

1.3 State funding

Artificial intelligence investment in the UK continues to surpass previous levels. The government has stated that it is committed to increasing the levels of AI research and development. In particular, the government's plan "to support the delivery of its modern Industrial strategy and make the UK one of the scientific and research centres of the world" includes an increase of annual public investment in AI R&D from £11.4 billion currently to £22 billion by 2024–2025.[5] The budget plan lays out the priority areas for R&D investment, aiming to:

- raise total R&D development investment to 2.4% of GDP by 2027;
- increase the rate of R&D tax credit to 12%; and
- invest £725 million in new Industrial Strategy Challenge Fund programs to capture the value of innovation.[6]

The effect of COVID-19 on funding commitments remains to be seen but AI has already shown its worth in the search for vaccines and treatments.

1.4 The effect of Brexit on the legal approach to AI

The UK is still subject to European Union (EU) legislation concerning AI and Big Data including the provisions of the GDPR. Similar to the UK, Europe's strategy is to become the most attractive, secure and dynamic data-agile economy worldwide. To this end, the European Commission (EC) has put forward a new legal framework relating to the development and use of "high-risk" AI that focuses on its human and ethical implications.[7] UK policymakers are currently considering whether or not to follow the EU approach. It is likely that this decision will be reached in conjunction with the decision on GDPR and data: to aim for alignment or divergence.

1.5 Competition by other countries in AI

The UK is unlikely to overtake China or the US in development spending on AI. It will, however, be likely to continue to see public and private sector investment levels that are similar to the next group of leading countries. Where the UK may have a truly leading role to play, however, is in developing policy, regulation and standards that can become internationally renowned and used internationally in much the same way that English law is used in many private international transactions. The British Standards Institution, which has a central role in developing consensus standards to accelerate product and service innovation for the global economy, aims to make the UK a "global standards maker, not a standards taker in AI".[8]

2 Regulatory landscape

The current UK regulatory landscape has the following features:

1. Active dialogue between the government, industry, non-profit sector and academia. The UK Government has established public bodies which are specifically dedicated to facilitating the adoption of AI technologies within both the public and private sector.
2. Focus across multiple sectors on the development of guidance in respect of deployment of ethical and trustworthy AI. Issues of liability in respect of AI are approached on a specific, targeted basis that appears more reactive than proactive. However, this may well change if the UK decides to follow the EC's proposed approach to regulating "high-risk AI".
3. Data protection principles are a challenge but not a barrier to the adoption of AI. The Information Commissioner's Office (ICO) has listed AI as one of its strategic priorities[9] and is focused on providing guidance on the compliance of AI technologies with data protection laws.

2.1 AI organisations

In line with the Industrial Strategy and AI Sector Deal, the government has set up three new bodies to facilitate the conversation around the adoption and deployment of AI technologies within the UK.

1. The AI Council is a non-statutory expert committee comprised of independent members from either industry, the public sector or academia, each of whom do not represent their

organisation or are in any way affiliating their business with the committee. It is each committee member's role to provide advice to the government on implementing the AI Sector Deal. The purpose of the AI Council is to "put the UK at the forefront of artificial intelligence and data revolution".[10]

2. The Government Office for AI is part of the Department for Digital, Culture, Media & Sport (DCMS) and the Department for Business, Energy & Industrial Strategy. The Office for AI works with industry, academia and the non-profit sector and is responsible for overseeing implementation of the AI and Data Grand Challenge.[11] In January 2020, the Office for AI and the Government Digital Service (GDS) published joint guidance on how to build and use AI in the public sector.[12]
3. The Centre for Data Ethics and Innovation (CDEI) forms part of the DCMS. CDEI serves as "a connector between government and wider society".[13] This is to say, it is an advisory body that advises the government on potential measures to develop the governance regime for data-driven technologies. In 2020, CDEI intends to develop an AI Barometer that identifies the highest priority opportunities and risks associated with data-driven technology within the CDEI's remit.[14]

2.2 Educate *versus* legislate?

In the last few years, there has been an increased focus on the ethical approach to AI both within the UK and more globally, in a way that supports and goes beyond pure compliance with legal requirements, such as data protection. The government recently stated that even though the UK already benefits from well-established and robustly enforced data protection laws, "the increased use of data and AI is giving rise to complex, fast-moving and far-reaching ethical and economic issues that cannot be addressed by data protection laws alone".[15] In April 2019, the EC and the High-Level Expert Group on Artificial Intelligence set up by the EC released documents that, amongst other matters, emphasised the importance of AI components following an ethical journey.[16] In May 2019, member countries of the Organisation for Economic Co-operation and Development (OECD), including the UK, adopted the OECD Principles on Artificial Intelligence – the first set of intergovernmental AI policy guidelines. These guidelines promote types of AI that are innovative, trustworthy and that respect human rights and democratic values.[17] In the UK, in June 2019, the GDS and Office for AI collaborated with the Alan Turing Institute to produce guidance on how to use AI ethically and safely.[18] This guidance is a summary of the Alan Turing Institute's detailed advice on responsible design and implementation of AI in the public sector.[19] Consistent with the OECD and EC's approach, the guidance stresses the importance of responsible innovation and the appropriate governance architecture. Responsible innovation means that AI projects must be ethically permissible, fair and non-discriminatory, justifiable and worthy of public trust. Governance architecture should consist of a framework of ethical values and actionable principles, supported by process-based governance that will integrate such values and principles into AI implementation.

The UK Parliamentary Committee on Standards in Public Life has specifically acknowledged the work of the Office for AI, the Alan Turing Institute, the CDEI and the ICO, but also noted an urgent need for guidance and regulation on the issues of transparency and the impact of data bias. Its recent report calls for implementation of clear ethical standards around AI in a way that will uphold the seven Principles of Public Life (Nolan Principles) and improve public standards to deliver a more accurate, capable and efficient public sector.[20] The Nolan Principles of Selflessness, Integrity, Objectivity, Accountability, Openness, Honesty and Leadership apply to everyone working in the UK as a public office-holder in the delivery of public services. The relevant principles must be considered in the context of AI systems to ensure that these build

public confidence and trust in the successful development of AI in the public sector. The report suggests that: (i) a new AI regulator is not needed, but all regulators must adapt to the challenges that AI poses to their sectors; and (ii) the UK's regulatory and governance framework for AI in the public sector remains a work in progress with notable deficiencies.[21]

Broadly, 2019 and the first few months of 2020 have seen: (a) an increase in cross-collaboration between various government and non-government stakeholders; and (b) a focus on creating compliance tools on development and deployment of AI technologies. For example, the Financial Conduct Authority (FCA) and the Bank of England announced the establishment of a forum to further dialogue with the public and private sectors, hoping to widen understanding of the use and impact of AI and machine learning within financial services.[22] The FCA has also announced a year-long collaboration with the Alan Turing Institute that will focus on AI transparency in the context of financial services.[23]

Although the government is actively engaging with many industry members via industry-focused departments, the UK currently lacks a tangible liability framework specifically applicable to harm or loss resulting from the use of emerging technologies such as AI. The specific characteristics of these technologies and their applications, including complexity, modification through updates or self-learning during operations and limited predictability, make it more difficult to determine what went wrong and who should bear liability if it does. Back in 2017, the House of Lords recommended that legal liability issues of AI are addressed as soon as possible and that the Law Commission is engaged to consider the adequacy of existing liability legislation.[24] The government in its response pointed out that the CDEI and the AI Council would take these concerns and engage the Law Commission as appropriate on the best course of action.[25]

However, at this stage, the overall question of legislating AI, including issues of liability, remains unanswered. By way of exception, the UK passed the Automated and Electric Vehicles Act 2018 pursuant to which liability for damage caused by an insured automated vehicle when driving itself lies with the insurer. The owner or insurer is not liable where the accident was caused by the person in charge of the vehicle (if different from the owner) allowing the vehicle to drive itself when it was not appropriate to do so. Insurers may exclude or limit liability if the accident occurred as a direct result of either prohibited software alterations or a failure to install safety-critical software updates.

However, with the EC's recent proposal to adopt a risk-based approach to regulation of AI, UK's approach of educating as opposed to legislating may well change. The EC's proposed framework is subject to public consultation and, accordingly, is mainly indicative of how the future legislation may look like. It is based on determining whether an AI application is "high risk", and consequently imposes specific compliance obligations on those applications. As the name suggests, "high-risk" applications are those that involve significant risks both in the AI sector more generally, and in its specific intended use – particularly from a safety, consumer rights and human rights perspective. In making a case in favour of legislating AI, the EC notes the following areas of uncertainty:

- *Limitation of scope of existing EU legislation*: Generally, it is not clear whether standalone software is within the scope of existing EU product safety legislation. In addition, general EU safety legislation applies to products and not services – thus also excluding services based on AI technology.
- *Changing functionality of AI systems*: Existing legislation predominantly focuses on the safety risk at the time of placing the product on the market and does not consider modification of the products and integration of software, including AI, during their lifecycle.

- *Allocation of responsibility in the supply chain*: EU legislation on product liability becomes uncertain if AI is added after the product is placed on the market by a party that is not the producer. That legislation only provides for liability of producers, thus leaving national liability rules to govern liability of others in the supply chain.
- *Changes to the concept of safety*: As well as existing safety concerns (i.e. physical safety), the use of AI in products and services can also give rise to risks not explicitly addressed by EU legislation, such as cyber security risks, or risks that result from a loss of connectivity.

The EC suggests that each obligation should be addressed to the actor(s) who are best placed to address any potential risks at each stage of the lifecycle – e.g. developers, manufacturers, coders – without adversely affecting the answer to the question as to which party should be liable for any damage caused. The EC seeks views on whether and to what extent strict liability may be needed in order to achieve effective compensation of possible victims of damage caused by AI applications that are "high risk".

Irrespective of whether the UK decides to follow the EC's approach, UK businesses may still be impacted. The EC has suggested that the territorial scope of this regulatory framework should be applicable to all relevant economic operators providing AI technologies in the EU, regardless of whether they are established in the EU or not.[26]

2.3 Data protection principles are a challenge but not a barrier to adoption of AI

GDPR has a significant focus on large-scale automated processing of personal data, specifically addressing the use of automated decision-making.[27] Big data analytics (which the ICO defines as the combination of AI, Big Data and machine learning) has the following distinctive features: (i) the use of algorithms in a new way (i.e. without a predetermined goal, but rather to find correlations in order to create new algorithms that can be then applied to a particular use case); (ii) opacity of the processing (i.e. where deep learning is involved); (iii) the tendency to collect all available data; (iv) repurposing data (i.e. using data for a purpose different from that for which it was originally collected); and (v) the use of new types of data (e.g. new data produced by the analytics, rather than being consciously provided by individuals).[28] These distinctive features do not necessarily sit well with the data protection principles – something that the ICO has clearly acknowledged. However, it has also stated that a different legal or regulatory approach is not required, and existing legislation is able to accommodate AI.[29] Consistent with this view, the ICO has taken a number of steps to help organisations to manage AI risk:

- As requested by the government in the AI Sector Deal and in collaboration with the Alan Turing Institute, the ICO has developed guidance (in draft form at the time of writing) on how organisations can best explain their use of AI to individuals.
- The ICO has developed guidance for auditing AI (also in draft form and open for public consultation at the time of writing). The purpose of this guidance is two-fold. It offers organisations best practices for data compliance of AI applications. The ICO will also utilise this guidance in the exercise of their audit functions.
- The ICO has also introduced the Sandbox service that allows 10 organisations to receive free support from the ICO when tackling complex data issues.

3 Intellectual property and AI

3.1 Patentability of inventions created by computers

In the past year there have been developments in the UK regarding inventions created by computers and whether or not these inventions can be protected with patents. The current

situation is patent protection is unavailable. However, there is ongoing debate including a consultation being led by the World Intellectual Property Organization (WIPO) as explained below. In December 2019 the UK Intellectual Property Office (UKIPO) found that DABUS is not a person and so cannot be considered an inventor of a patent.[30] DABUS is an AI machine. The UKIPO accepted the indication of DABUS as inventor at face value and did not argue that AI technology is only a tool which is incapable of independently creating an invention. The hearing officer found that even if DABUS is an inventor there was no valid chain of title from DABUS to the human applicant, even though the human applicant is the owner of DABUS. The hearing officer called for potential changes to the law and not to make attempts to "shoehorn arbitrarily into existing legislation". The UKIPO decision is encouraging because it calls for wider debate about the issue of AI machines which create inventions. It is a useful decision because it clearly sets out the arguments including the legal arguments and the ethical arguments, and it is expected that the decision will be appealed.[31] The UKIPO has updated Sections 7.11.1 and 13.10.1 of their Manual of Patent Practice such that where the stated inventor is an "AI Inventor", the Formalities Examiner should request a replacement statement of inventorship form.[32] An "AI Inventor" is not acceptable as this does not identify "a person" which is required by law. The consequence of failing to supply a correct statement of inventorship is that the application is taken to be withdrawn under Section 13(2).

In a recent submission to the WIPO consultation on AI and intellectual property policy the UK Chartered Institute of Patent Attorneys (CIPA) states, "CIPA does not have a single view on whether the law (as presently applied in the UK) should be changed such that an AI system can be named as inventor on a patent application. There are many who think this would be acceptable if the contribution made by the AI system is such that, if a human had made the contribution, the human would be recognized as inventor. Others however think patent applications should continue to require at least one human inventor. Importantly, UK law (at least) has existing statute and case-law for determining when a human is an inventor. There is a possibility that the validity of a patent relating to a solution generated using an AI system and naming a human inventor might be challenged if the contribution of the human inventor does not satisfy these existing provisions regarding inventorship. Note that such existing provisions are aimed at determining which humans, from a group of humans, have made an appropriate contribution to be recognized as an inventor; they may not be well-suited for addressing inventorship in cases having an AI contribution.

This potential risk to validity could be addressed in a number of ways, such as: (a) relaxing the requirement for a human inventor, as mentioned above; (b) clarifying the law on inventorship with specific regard to solutions generated using AI systems; (c) trying to obtain guidance from the courts on the application of existing provisions with respect to cases having an AI contribution. One complication is that inventorship is generally a question of national law, with little harmonization across states."[33]

3.2 Proposal for a new *sui generis* right for data

Issue 10 in the WIPO consultation about AI and IP policy is about a proposed new *sui generis* right for data. The reasons stated for the proposed new data right include:

- the new significance that data has assumed as a critical component of AI;
- the encouragement of the development of new and beneficial classes of data;
- the appropriate allocation of value to the various actors in relation to data, notably, data subjects, data producers and data users; and
- the assurance of fair market competition against acts or behaviour deemed inimical to fair competition.

The UK response to the consultation is available on the WIPO web site and includes the following positive comment from the UKIPO welcoming "further exploration of how additional protection for data as a right could incentive the AI industry". On the other hand, the UK's CIPA states in a submission that "CIPA does not advocate the creation of new data IP rights" perhaps because it takes the view that existing ways of protecting data through contract and licensing are enough.

Whilst it is the case that existing intellectual property rights for protecting data are patchy (trade secrets and database rights), it is not clear how a new data IP right would incentivise the AI industry and facilitate fair market competition. In addition, it is not clear how such a new right would apply to synthetic data which is often used in AI technology. Synthetic data includes data that is independently generated but which duplicates patterns or properties of existing data needed for machine learning. At a recent evidence meeting of the All Party Parliamentary Group on AI at the UK House of Lords the question of a new data right was discussed and views on all sides were heard although no conclusion was reached.

3.3 Trademark registrations held by AI brand holders covering "computer software"

AI technology comprises complex software and AI brand holders typically protect their brands with trademark registrations. This is especially important for AI brand holders where AI technology often has a "black box" nature and consumers need to trust the manufacturer or service provider such that reputation is key. Trademark registrations include a specification of goods and services which aid in defining the scope of protection and in the past, many AI brand holders have used terms such as "computer software" in their specifications of goods and services. Drafting the specification of goods and services for a mark of an AI product or service can be challenging due to the difficulties in defining the term "artificial intelligence" and the need to be clear and precise. In the UK there was a challenge to the term "computer software" as being vague. However, in January 2020 the CJEU found that terms such as "computer software" are acceptable in certain situations.[34] Under UK national trademark law, applicants must have a "*bona fide* intention to use" their trademarks in connection with the goods/services specified in their UK applications. Thus, AI brand holders are able to use terms such as "computer software for machine learning in the field of life sciences" where they have a *bona fide* intention to use their UK trademarks across the whole scope of the term in the UK. The UK High Court is hearing SkyKick on return from the CJEU on Thursday 2 April and so there may be more enlightenment on interpretation in the UK after that.

4 Healthcare and AI

AI has yet to transform the healthcare industry in the UK. Whilst its use and the significant opportunities and benefits it offers patients and clinicians are largely welcomed, the UK healthcare system has been somewhat late to recognise the potential of AI. That said, the NHS in general and NHS Digital specifically are catching up fast and taking a commendably realistic approach in an environment traditionally resistant to change.[35]

In August 2019 the UK Government announced a welcome boost for AI in healthcare, with £250m for a national laboratory in England[36] which is to prioritise technologies more likely to benefit the health system and patients in the short term, such as diagnostics and applications which improve operational efficiency. When investigating the use of AI in the healthcare industry Microsoft's most recent study[37] reported an "encouraging increase" in the use of AI in UK healthcare with 46% of healthcare leaders' organisations using the technology in some capacity, an 8% increase compared to 2018. The findings aligned with the government's current priorities, with automation and research-level AI being amongst the biggest growth areas identified.

A key question for UK AI healthcare solutions is the regulatory classification of the software on which they are based. It is essential to ascertain whether the software involved is a medical device, since medical devices can only be marketed after successful conformity assessment and CE-marking. In the UK, the EU Medical Devices Regulation 2017/745/EU (MDR) is due to come into mandatory application on 26 May 2020 (subject to certain exceptions and the European Commission's proposal to delay for one year its date of application in light of the COVID-19 global pandemic),[38, 39] and subsequently legislation will be implemented pursuant to the Medicines and Medical Devices Bill[40] which provides for the UK Government to take over the rulebook for medical devices post 31 December 2020.

Whether or not software is considered a medical device depends upon its intended purpose. If this is to detect or treat disease, there is a strong argument for classifying it as a medical device (e.g. if it assists in diagnosis, facilitates therapeutic decision-making or calculates the dosage of medication). On the other hand, if the software only provides knowledge or stores data, it will likely not qualify. Acknowledging the complexity of this assessment and subsequent classification, the EC's Medical Device Coordination Group has issued guidance.[41] Whilst historically the majority of medical device software (MDSW) has been class I, there is a growing concern that under the new legislation nearly all MDSW will fall within class IIa or higher and, accordingly, its manufacturers will be required to involve notified bodies, establish a certified quality system and bear the associated increased costs.

Examples of AI can be found throughout the healthcare ecosystem in the UK, getting increasingly better and doing what humans can do:

- **Efficiently detecting/diagnosing** – At Moorfields Eye Hospital, Google's DeepMind Health has been training software since 2016 to diagnose a range of ocular conditions from digitised retinal scans and matching the performance of top medical experts.[42]
- **Decision making** – Addenbrooke's Hospital uses Microsoft's InnerEye system to mark up scans to assist radiology treatment for cancer patients.[43]
- **Drug discovery and research** – January 2020 saw the first drug molecule invented entirely by AI (developed by Oxford-based AI start-up Exscientia in collaboration with the Japanese pharmaceutical firm Sumitomo Dainippon Pharma) enter clinical trials.
- **Patient experience**:
  - AI is being used to solve operational challenges and automate the most repetitive processes, e.g. Amazon Transcribe Medical automatically converts physician consultations and dictated notes from speech to text.[44]
  - Healthcare plans are being personalised at an individual and community level, e.g. Babylon Health and Royal Wolverhampton NHS Trust are working on an integrated health app covering the entire population of the city. It will not only offer remote diagnoses, but also live monitoring of patients with chronic conditions and the ability to connect people with doctors and others remotely.[45]
- **Mining and managing patient data** – IBM's Watson is working with the NHS to help healthcare professionals harness their data to optimise hospital efficiency, better engage with patients and improve treatment.[46]
- **Robot-assisted surgery** – Intuitive da Vinci platforms have pioneered the robotic surgery industry, featuring cameras, robotic arms and surgical tools to aide in minimally invasive procedures.[47]
- **End of life care** – By providing care in people's own homes, AI is giving patients who wish to the chance to die at home by remaining independent for longer and reducing the need for hospitalisation, care homes and hospices.

AI in healthcare promises a new era of productivity in the UK, where human ingenuity is enhanced by speed and precision. We have been told that AI will play a crucial role in the future of the NHS[48] and the data-rich nature of healthcare makes it an ideal candidate for its application across multiple disciplines. However, the sensitivities surrounding patient data raises crucial concerns around privacy, security and bias. These conflicts make the industry one of AI's most challenging and for AI to truly thrive in the UK healthcare system, the quality and scope of health data on which it is based needs to be significantly improved with the sophistication, security, interoperability and integration of the information systems being similarly optimised.

Acknowledgment

This chapter was written with Charles Kerrigan – charles.kerrigan@cms-cmno.com / https://cms.law/en/gbr/people/charles-kerrigan.

* * *

Endnotes

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf?fbclid=IwAR0nmoFvfUBp2m0-nxxxZuVEx0gDRr12a7pB0HKnoEBIHLJSb0L1-c26Hms.
2. https://www.tortoisemedia.com/intelligence/AI.
3. https://www.gov.uk/government/uploads./system/uploads./attachment_data/file/664563/industrial-strategy-white-paper-ready-version.
4. https://assets.publishing.service.gov.uk/government/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf.
5. https://www.gov.uk/government/publications/budget-2020-documents/budget-2020.
6. https://www.gov.uk/government/publications/artficial-intelligence-sector-deal/ai-sector-deal.
7. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-feb2020).
8. https://www.bsigroup.com/en-GB/industries-and-sectors/artificial-intelligence/.
9. Information Commissioner's Office – Technology Strategy 2018-2021 available at https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf.
10. The AI Council, Terms of Reference available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836907/AI_Council_Terms_of_Reference.pdf.
11. https://www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/missions.
12. https://www.gov.uk/government/publications/a-guide-to-using-artificial-intelligence-in-the-public-sector.
13. https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about.
14. *Ibid.*
15. Government Response to Lords Select Committee on Communication Report "Regulating in a Digital World" p. 4 available at https://www.parliament.uk/documents/lords-committees/communications-and-digital/InternetRegulation/government-response-regulating-in-a-digital-world.pdf.

16. "Ethics Guidelines for Trustworthy AI" by the High-Level Expert Group on Artificial Intelligence available at https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top, Communication by the European Commission "Building Trust in Human-Centric Artificial Intelligence" available at https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
17. https://www.oecd.org/going-digital/ai/principles/.
18. https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety.
19. https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf.
20. https://www.gov.uk/government/latest?departments%5B%5D=the-committee-on-standards-in-public-life.
21. *Ibid.*
22. https://www.fca.org.uk/news/news-stories/financial-services-ai-public-private-forum.
23. https://www.fca.org.uk/insight/ai-transparency-financial-services-why-what-who-and-when.
24. https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.
25. https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response.pdf at p. 31.
26. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf at p. 22.
27. See Articles 5(1)(a), 13–15, 22, 22(3) and Recital 71.
28. Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection at p. 9 available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.
29. Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.
30. https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf.
31. http://artificialinventor.com/.
32. https://www.gov.uk/guidance/manual-of-patent-practice-mopp.
33. https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/org_cipa.pdf.
34. http://curia.europa.eu/juris/document/document_print.jsf?docid=222824&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=3376591.
35. Indeed, the NHS has created a code of conduct which sets out principles expected from suppliers and users of data-driven technologies, with the aim of making it easier for suppliers to understand what the NHS requires to help providers choose safe, effective, secure technology to improved service provision. https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology.
36. https://www.bmj.com/content/366/bmj.l5106.
37. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3RFyw.
38. Article 123(2) of the MDR.
39. At the time of writing and in light of the coronavirus pandemic, it is uncertain whether this date of application will remain true. Indeed, the European Commission has recently confirmed it is working on a proposal to delay for one year the date of application of the MDR and that it intends to submit a proposal to the European Parliament and the Council in early April.
40. https://services.parliament.uk/Bills/2019-21/medicinesandmedicaldevices.html.

41. https://ec.europa.eu/docsroom/documents/37581?locale=en.
42. https://www.theengineer.co.uk/ai-medical-diagnostics/.
43. https://www.matt-hancock.com/news/my-vision-more-tech-driven-nhs.
44. https://aws.amazon.com/transcribe/medical/.
45. https://www.royalwolverhampton.nhs.uk/media/latest-news/january-2020/the-royal-wolverhampton-nhs-trust-and-babylon-to-create-the-worlds-first-integrated-digital-health-system/.
46. https://www.ibm.com/blogs/think/uk-en/ibm-and-the-nhs-working-in-partnership/.
47. https://www.intuitive.com/.
48. https://www.matt-hancock.com/news/my-vision-more-tech-driven-nhs.

Rachel Free
Tel: +44 20 7067 3286 / Email: rachel.free@cms-cmno.com
Rachel Free is a European and UK patent attorney with an MSc in Artificial Intelligence and a DPhil in vision science. She is a partner at CMS helping clients protect their AI technology. She is a member of the data governance task force of the All Party Parliamentary Group on AI and she is an independent advisory board member of the University of Bath centre for doctoral training on accountable, responsible and transparent AI.

Hannah Curtis
Tel: +44 20 7367 3726 / Email: hannah.curtis@cms-cmno.com
Hannah Curtis is a partner in the Technology & Media Team and a member of the firm's Life Sciences Sector Group. Hannah works across a number of sectors but has a particular focus on life sciences & healthcare, having studied biological sciences prior to law. Hannah is a member of techUK's Data Analytics and AI Leadership Committee and has more than 12 years' experience of advising clients on transactions with a technology and intellectual property focus within the life sciences and healthcare sector.

Barbara Zapisetskaya
Tel: +44 20 7367 2543 / Email: barbara.zapisetskaya@cms-cmno.com
Barbara Zapisetskaya is an associate in the Technology & Media Team. Barbara has a particular interest in the regulation of artificial intelligence and other emerging technologies as well their application. Barbara's experience lies in the areas of commercial and technology law. She has been advising clients on a variety of commercial matters, including sale, distribution and supply of products and services to the market and consumer protection. Barbara's other areas of practice are technology and business process outsourcing and technology projects, such as software licensing, support and system development and integration.

CMS Cameron McKenna Nabarro Olswang LLP

Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom
Tel: +44 20 7367 3000 / URL: cms.law

USA

Nathan Greene, David Higbee & Brett Schlossberg
Shearman & Sterling LLP

Artificial intelligence trends and considerations under U.S. law

Although autonomous machine technology is still in the nascent stages of development and implementation, the relatively recent emergence of "big data" aggregation and machine learning ("ML") analytics has nevertheless already presented numerous questions of how businesses and society writ large should address the myriad implications of truly autonomous systems. As legislators and regulators from around the globe seek to strike the right balance between encouraging innovation and protecting individual rights, it is becoming increasingly incumbent upon business leaders to ensure their operations and policies are nimble enough to adapt to a regulatory landscape that is as dynamic and unpredictable as autonomous machine technology itself. In order to mitigate the risks associated with entering the artificial intelligence ("AI"), big data analytics or ML industries, it is imperative to develop a nuanced understanding of the commercial and regulatory developments in that space to date. In order to avoid the pitfalls of AI and other autonomous technologies, each business must cater its approach based on its own unique considerations and circumstances. For businesses owned and operated within the United States ("U.S."), a good starting point is to examine the recent legal trends in the AI industry, the unique intellectual property ("IP") ownership considerations presented by AI technologies, and the application of antitrust and financial services regulations to AI systems and other autonomous technologies. The purpose of this chapter is to establish a foundational understanding of the issues, considerations and legal frameworks that businesses have thus far encountered when developing and commercialising autonomous technologies within the U.S., in order to enable business leaders and other stakeholders to discern, anticipate and adapt to future developments in this space.

Legal trends in the AI industry

From automotive and transportation,[1] to supply chain management,[2] human resource functions,[3] and financial services,[4] there are few industry sectors which have not been impacted by the evolution of AI technologies. The relatively rapid growth and adoption of this new technology has left legislators in an increasingly reactive position as new issues and potential risks materialise alongside the ever-growing compendium of AI applications. The U.S., in particular, has been slow to provide industry participants with guidance on the legal and regulatory landscape that is developing with respect to AI technologies. For instance, the first official statement from the White House[5] regarding how companies can leverage AI for economic and technological growth did not come until the final months of the Obama Administration. This initial report outlined recommendations related to AI regulations, security, ethics and fairness, and automation. The Obama Administration followed up that initial report with two companion reports, *National Artificial Intelligence Research and*

Development Strategic Plan[6] and *Artificial Intelligence, Automation, and the Economy*,[7] to expound upon the recommendations set forth in the initial report. The former set forth a strategic plan for providing publicly-funded research and development of AI technologies, while the latter analysed the economic and societal effects of automation in order to discern how public policy should be construed to maximise the benefits of AI technologies, while mitigating the costs of implementing AI systems. In May 2018, the Trump Administration held a summit on AI technologies[8] for industry, academia and government participants. At this conference, White House officials outlined the following four core goals of the U.S. government with respect to AI technologies: (i) maintaining American AI leadership; (ii) supporting American workers; (iii) an increased focus on research and development; and (iv) removing barriers to innovation. In February 2019, President Trump followed up on these previously stated goals by signing an executive order to create the "American AI Initiative", which, amongst other things, directs heads of federal agencies to budget an "appropriate" amount of funding for AI research and development.[9]

While these promulgations are instructive as to how the future of AI technologies will be fostered and supported by the U.S. government, they nevertheless fall short of actual policy implementation or providing new funding for AI development.[10] While the U.S. may be lagging behind other countries such as China when it comes to legislating and regulating AI systems, the task of constructing a viable legislative regime for AI systems is a veritable minefield of complexities and unknown variables. The challenge of holding AI systems accountable for the automated decisions they make comes from the fact that AI systems, and even the engineers who built them, are unable to explain the rationale or process by which an automated system reaches a decision. As noted by the Berkman Klein Center for Internet & Society at Harvard University, "[g]ood choices about when to demand explanation can help prevent negative consequences from AI systems, while poor choices may not only fail to hold AI systems accountable but also hamper the development of much-needed beneficial AI systems".[11] For legislation to be effective, AI and the systems they are incorporated into need to be able to give the reasons or justification for a particular outcome, not just a description of the steps taken throughout the decision-making process.

With the current state of ML technology, it can be difficult or even impossible to discern the reasons as to why a specific algorithm "chose" to take a certain action.[12] How an AI system weighed certain factors, exercised judgment, and adjusted its actions in anticipation of certain undesirable outcomes are all crucial components of enforcing laws against AI systems. And when even the engineers who built the AI cannot provide these explanations, crafting appropriate legislation around AI can become a Sisyphean task. And while other jurisdictions have made their first attempts to regulate decisions made by automated processes,[13] the U.S. has yet to see any such similar attempts.

As U.S. legislators struggle with these complexities, AI-based businesses are having to come up with creative solutions in the transactional context to account for the unsettled state of the law. In particular, the traditional models for licensing and commercialising IP in the software industry have required certain adjustments in order to account for the differences between software and AI-based systems.

AI considerations for IP transactions

Due to the technical aspects of how ML algorithms and models intersect with AI, the usual software licensing constructs either do not apply or require material adjustments to transactions involving ML systems. The most significant distinction between traditional software and ML is the manner in which ML algorithms ingest and learn from data inputs.

As a result, the IP rights to the input data is a crucial component of any transaction involving ML algorithms. Similarly, the output of the ML algorithm – whether that output is data or something else, such as training parameters – has also increased value in AI-based transactions. As a result, parties negotiating a contract for an AI-based service or product need to carefully analyse the various components of IP embodied by the AI system in order to determine how to apportion the IP rights accordingly.

The first step in the transactional process is making sure the parties have a complete understanding of the automated system itself. In order to address how the IP rights should be apportioned, it is necessary for the parties to make a clear distinction upfront as to whether they are contracting over an ML algorithm, an ML model, AI software, or the input and/or output data of an automated system, or any combination of the same. Without this distinction, the parties will not be able to clearly define the licence scope, which needs to account for various configurations, modifications, enhancements and parameters of the technology.

Each of the aforementioned components of an automated system are variable in value based on the needs and goals of the parties. For instance, the rights to the input data may contain sensitive customer info which the data licensor will want to retain ownership over, whereas the data licensee may want to retain ownership over a proprietary ML algorithm which is the core of their business model. Since the input data will train the ML algorithm and improve its efficiency and the accuracy of its output, it is imperative that parties in this sort of transaction clearly delineate the scope of rights and the type of rights needed for each component. Then, the parties will need to determine who gets what rights to the output data, as both parties have equally contributed to the creation of the output. These scenarios are highly fact-dependent, and the ultimate outcome of negotiations in a given AI-related transaction will vary widely; however, the following considerations should be taken into account regardless of the specific circumstances of a given transaction:

- for vendors of AI-based systems, being able to retrain, modify and improve their ML algorithm or model is a core component of creating a long-term revenue model – as a result, the vendor's rights to the learnings and algorithmic optimisations generated by the transaction are highly valuable to the vendor;
- parties need to be careful of entering into "gain sharing" arrangements, whereby the financial gains of AI-optimised processes are shared by the parties – the increased scale afforded by AI-optimised systems can still come with increased costs and fees, as accounting and administrative efforts to track the gains can be costly;
- since AI systems can become deeply engrained in a licensee's business, the parties need to understand how they can comply with any post-termination requirements, particularly with respect to the return or destruction of confidential information which may be irrevocably intertwined with a party's business; and
- residual rights to the learnings of an ML system, any algorithmic and parameter optimisations generated by a transaction, and to the input or output data need to be carefully constructed so each party retains its freedom to operate once the contractual relationship ends.

The commercial and regulatory complexities posed by the IP considerations in a transaction regarding AI systems are not the only concerns that companies conducting business in the AI field need to be cognisant of in a given instance. Sometimes, the implications of a given transaction could raise antitrust concerns as well.

The antitrust implications of big data and algorithmic pricing

In recent years, AI and ML have drastically changed how businesses are able to utilise big

data to more effectively compete for new customers. Businesses currently use machines to store massive amounts of economic data, including pricing information, consumer shopping patterns, and consumer address information. These machines can then use algorithms to process this raw data into information that the business can use to estimate consumer demand and forecast price changes in its relevant market, enabling it to react almost instantaneously to price movements by competitors. The impact has already been felt on Wall Street, where "algorithmic trading is a ubiquitous phenomenon across the financial markets today,"[14] as well as in the halls of Congress, where lawmakers are considering proposed legislation such as the Algorithmic Accountability Act of 2019, which would direct the Federal Trade Commission ("FTC") to require companies to affirmatively evaluate and minimise the risks of flawed computer algorithms that result in inaccurate, unfair, biased, or discriminatory decisions.[14B]

While utilising algorithmic pricing can lead to several pro-competitive benefits for consumers, there is also the dangerous potential for businesses to share pricing information collected through these algorithms with their competitors to fix prices or engage in other anticompetitive conduct. Antitrust enforcers have become increasingly wary of this potential for collusion, noting that algorithms "might facilitate cartel formation and maintenance… [or] tacit collusion between competitors."[15] Below, we analyse several potential antitrust concerns arising from big data and algorithmic pricing.

Pricing algorithms can facilitate collusion

Businesses can use pricing algorithms to collect and ultimately share competitively-sensitive information with their competitors, leading to illegal price fixing and market allocations. There are two possible types of collusion – overt collusion and tacit collusion.

Overt collusion: explicit agreements

Overt collusion occurs when humans use pricing algorithms as an instrument to facilitate a pre-arranged price-fixing conspiracy. For example, in *United States v. Topkins*,[16] the U.S. Department of Justice ("DOJ") prosecuted two e-commerce sellers for agreeing to align their pricing algorithms to increase online prices for posters. Here, the parties' agreement to violate the antitrust laws was explicit, and the application of antitrust law to the agreement was equally straightforward. As Margrethe Vestager, the European Commissioner for Competition, recently remarked, "no one should imagine they can get away with price-fixing by allowing software to make those agreements for them."[17]

Tacit collusion: what happens when machines "collude?"

The more complex issue could arise where pricing algorithms are the source of the collusion rather than simply an instrument used to further an already-existing agreement. Scholars have observed that algorithmic pricing has become so advanced that it has surpassed humans' ability to analyse market data and adjust pricing. Professors Ariel Ezrachi and Maurice E. Stucke have written that "as competitors' prices shift online, their algorithms can assess and adjust prices… for thousands of products… within milliseconds… [and] can swiftly match a rival's discount, thus eliminating its incentive to discount in the first place."[18] Similarly, Former Acting FTC Chairman Maureen K. Ohlhausen has remarked that tacit collusion through algorithmic pricing can be "extremely hard to detect," as computers can "react almost instantaneously" to changes in any of several variables.[19]

A recent study by four economists at the University of Bologna appears to validate some of these concerns, with the results suggesting that AI-powered algorithms "may be better than humans at colluding tacitly."[20] The study found that even relatively simple pricing algorithms,

operating in repeated price competition, would systematically learn to "collude" and charge supracompetitive prices, enforced by "punishing" defectors from the scheme. Notably, they learned to play these strategies "by trial and error", and "leave no trace whatever of concerted action", as the pricing algorithms were not designed to collude, nor were they able to communicate with one another. As the authors conclude, more research is needed, but "[f]rom the standpoint of competition policy, these findings should clearly ring a bell".

While no antitrust regulator has brought an enforcement action on the basis of tacit collusion using pricing algorithms, in 2015, private plaintiffs sued Uber, alleging that the pricing and payments mechanism at the heart of the Uber app violated the Sherman Act.[21] Plaintiffs argued that the pricing mechanism supported a hub-and-spoke conspiracy, whereby each driver used the mechanism to compare rates and ultimately ensure that other drivers would not undercut their prices. The court found the allegations in the complaint sufficient to withstand a motion to dismiss, finding that drivers would sign up for Uber understanding that all Uber drivers were agreeing to the same pricing algorithm. While the case was ultimately removed to arbitration, the court's rejection of Uber's argument that drivers had made independent decisions to enter into a vertical agreement with Uber in order to take advantage of the payment processing and rider matching services could influence the success of certain pro-competitive defences used in future antitrust cases involving pricing algorithms.

Algorithmic pricing as a factor in merger analysis

In addition to the threat of hub-and-spoke conspiracies, increased use of algorithmic pricing may have a significant bearing on Sherman Act Section 7 antitrust merger analysis. Former FTC Commissioner Terrell McSweeny has observed that advanced pricing algorithms can enable companies to engage in sophisticated price discrimination involving a combination of differential "list" prices and targeted discounts, without ever reaching an explicit agreement.[22] In McSweeny's view, increasingly nuanced and profitable price discrimination strategies by sellers could also lead to narrower product markets in the future.[23]

Former Director of the FTC's Bureau of Competition D. Bruce Hoffman has also suggested that autonomous machines may be able to achieve oligopoly outcomes more quickly or more sustainably than can humans, given their ability to quickly process, compare, and modify prices.[24] As "one of the fundamental principles of merger policy is the prevention of mergers that would allow firms to acquire the ability to achieve an oligopoly outcome,"[25] to the extent that algorithmic pricing could reach and/or sustain such an outcome more easily than humans, enforcers may become more aggressive in challenging a broader set of mergers.

Practical considerations for companies

Despite these recent advancements in technology, U.S. antitrust regulators continue to take the view that pricing algorithms are not all that novel from an antitrust enforcement perspective. Officials from both the DOJ and FTC have remarked that tacit collusion through pricing algorithms does not call for a new theory of competitive harm, and that the antitrust laws are "demonstrably capable of evolving with the times."[26] When considering collusion under Sherman Act Section 1 violations, for example, proof of agreement is key to determining whether parallel conduct amounts to an antitrust violation under U.S. law, whether that agreement is verbal, written, or reached through a pricing algorithm.[27]

As FTC Commissioner Rebecca Kelly Slaughter recently explained, "while many of the problems of AI—bad data, failure to test, proxy discrimination—have longstanding analogs, AI can simultaneously obscure the problems and amplify them, all while giving the impression that they don't or couldn't possibly exist."[27B] Thus, in her view, "the starting point

of nearly all discussions about AI ethics and the focal point of many regulatory responses is to require increased transparency and accountability in order to mitigate discriminatory effects". She observed that this emphasis on transparency and accountability is reflected in a number of pending legislative proposals, but is perhaps best illustrated by the Algorithmic Accountability Act, noted above. According to the Commissioner, "[t]he core insight of the proposed bill, through required impact assessments (IAs), is that vigilant testing and iterative improvements are the fair and necessary cost of outsourcing decisions to algorithms. Or, as [she] would put it, you can't have AI without IA."

Despite the regulators' hands-off approach to potential tacit collusion through the use of pricing algorithms to date, companies should still take the appropriate precautions in how they manage big data. Companies should create antitrust compliance programmes which include training specific to the use of pricing algorithms, and should instruct employees that algorithms contain competitively sensitive information that should not be shared with competitors. Further, companies should be very clear that employees must avoid discussing the use of pricing algorithms with their competitors, just as they would avoid any discussion of prices. Finally, while pre-deployment testing of any algorithm is critical, there is an emerging consensus that monitoring, evaluating, and retraining algorithms on an ongoing basis is an equally essential component of any algorithm-focused compliance programme.

While these antitrust concerns can apply regardless of the application for which an AI-based system is utilised, further complexities arise when the system is used in the financial services industry.

Financial services regulation for AI systems

The financial services industry covers a broad scope encompassing banking, money transmission, lending and finance, underwriting, brokerage, insurance, investment management and related sectors. The industry serves retail customers, high-net-worth customers and institutions and can be packaged as anything from extremely "low touch" to extremely "high touch". It is also among the most highly supervised industries, with a multiplicity of regulators at the federal and state level. Financial services regulators tend to both make rules and to carry out ongoing inspections and risk analyses, typically with a combination of goals that include customer protection, market integrity, and safe and sound operation of the supervised institutions.

Automated and AI-based applications are used throughout the industry. Marketing applications ingest social media and other source data to identify and profile customers. Chatbots interact with customers in service and marketing capacities. Quantitative programs trade in securities and derivatives markets, often at speeds and volumes far in excess of human trading; automated underwriting processes make lending and insurance decisions. Other automated programs identify and research anomalies to support risk management, fraud detection, anti-money laundering ("AML") profiling, and other control processes. Banking regulators and the U.S. Treasury Department's Financial Crimes Enforcement Network have generally encouraged the use of innovative technologies to meet AML requirements.[28]

Both financial services firms and their regulators appear to view these developments in the same way, namely that they are an inevitable reflection of an industry in flux. Most profoundly, the industry is awash in – and hungry for – data from many different sources, at a level of volume and complexity that cannot be efficiently managed without sophisticated technology. Firms that are not constantly re-examining how they can deploy technology and data-driven processes are at a real competitive disadvantage in the industry, and a real

disadvantage in identifying problems and maintaining their compliance with regulatory requirements before being identified by regulators using advanced technology.

How has the government responded?

The White House

As previously noted, the White House, both under President Obama and President Trump, has made AI a top national priority, publishing white papers and holding summits that, at bottom, call for the U.S. to be a leader in AI and cautioning that excessive governmental encumbrances should be avoided.[29]

Congress

Congress has organised an AI caucus, which proposed legislation on December 12, 2017 in the FUTURE of AI Act (Fundamentally Understanding the Usability and Realistic Evolution of AI Act). The primary purpose of both the caucus and the bill appears to be ensuring that Congress is familiar with AI and taking its potential into account when developing public policy.[30]

U.S. Treasury

The U.S. Treasury Department issued, as part of a series of reports designed to identify regulations that are inconsistent with core principles for the regulation of the financial industry, a broad and comprehensive discussion specific to AI in financial services (see "A Financial System that Creates Opportunities: Nonbank Financials, Fintech and Innovation" (July 2018)). The report observed that AI investment by financial services firms is accelerating and that AI innovations drive efficiencies for firms and improve outcomes and choices for customers. Treasury cautioned, however, that in other contexts, industries that rely heavily on technology and data-based platforms tend towards concentration, with attendant long-term risks to levels of innovation and choice.

Turning to specific challenges presented by AI, Treasury suggests that AI is a double-edged sword in many respects. As automated processes replace human judgment, opportunities for unlawful discrimination are reduced (for example, automated lending decisions should be more neutral than human decisions) – that is, unless the AI encodes or learns prejudice of its own, the risk of which increases as powerful, data-rich AIs may identify correlations to target characteristics that are also correlated to a discriminatory or impermissible characteristic. Powerful new risk and fraud detection tools can be used to block and root out rogue traders, money launderers, cyber criminals and other bad actors. But bad actors likewise might deploy AI of their own to circumvent existing controls. Massive investment in AI will lead to a boom in demand for engineers, data scientists and other specialists. But layoffs will follow in employment sectors where AI replaces existing staff.

Finally, Treasury notes the concern that "black box" systems are inconsistent with traditional regulatory norms that expect transparency and auditability for industry activities. Opaque decisions risk poor consumer outcomes; e.g., when AI makes an inappropriate financial recommendation to a customer. Opaque decisions are most concerning, of course, when the stakes are highest and involve matters such as institutional solvency or financial stability. In other words, Treasury is most concerned about possibilities like these: AI roiling financial markets with volatile trading; AI misrouting large money transfers; AI mispricing assets or accounts; or AI causing an institution or regulator to misunderstand risks.

U.S. Federal Reserve

The U.S. Federal Reserve, in addition to its role setting monetary policy as the nation's central bank, is also a regulator for many U.S. banks. In a thoughtful and widely cited speech, Lael

Brainard, a member of the Federal Reserve's Board of Governors, described the regulatory approach to AI as one that should start with "existing regulatory and supervisory guardrails". Governor Brainard then described two Federal Reserve guidance notes as directly applicable, the first being the Fed's guidance on risk management when using complex models (SR Letter 11-7), and the second being guidance on vendor risk management (SR 13-19/CA 13-21).

Regarding models, Governor Brainard noted "maker-checker" type controls that empower unbiased, qualified individuals separated from the model's development, implementation, and use as a "second set of eyes", as well as the potential for circuit breakers or other controls that would come into force to deal with unexplained or unexpected outcomes. Regarding vendor risk management, she noted due diligence, selection, and contracting processes, oversight and monitoring throughout the relationship with the vendor, and considerations about business continuity and contingencies for a firm to consider before the termination of any such relationship.

Speaking to questions of opacity and explainability, Governor Brainard agreed that existing guidance "recognizes that not all aspects of a model may be fully transparent, as with proprietary vendor models, for instance". In the absence of full transparency, however, upfront and ongoing risk monitoring efforts are heightened. Principles of proportionality also apply, with more caution required when AI will be used for major decisions or across a broad customer base. Finally, Governor Brainard referred to risks associated with invalid or improper data sets leading to potentially cascading failures in an AI's algorithms and outputs. Controls around how an AI system will source and consume data are critical.

SEC

The U.S. Securities and Exchange Commission ("SEC") is the primary U.S. regulator for public securities markets, investment advisers, and broker-dealers. The agency has not issued direct guidance as to how regulated firms should consider or review their use of AI, but has provided consistent principles around the evaluation of risk through exam results and in speeches that make clear the industry should be considering these issues carefully. Historically, the agency has brought a number of enforcement actions involving failures by firms to properly vet and implement complex investment models – generally also alleging related failures to disclose weaknesses or limitations in the models – which are obvious analogues to how faults in AI-driven models and systems may be considered. In particular, the SEC expects firms to carefully test and document technology before it is rolled out, and to continue testing technology over time as conditions change. A firm should understand and be able to explain the core operations and individual outcomes of their technology both to internal and external governance bodies (senior management, compliance and control functions, and regulators) and be able to provide documentation of its deliberative processes around both the evaluation of the technology and the individual outcomes. Risks that might be presented by reliance on the technology need to be accurately identified and disclosed to clients.[31]

CFTC

The U.S. Commodity Futures Trading Commission ("CFTC") is the primary U.S. regulator for derivatives markets and their participants, including trading facilities, clearing organisations and market intermediaries such as swap dealers, futures commission merchants and commodity trading advisors. The agency has not directly spoken on how its regulated firms should consider their use of AI, but the agency has considered a number of issues related to automated trading activity more generally. For example, the agency has long taken the position that provision of software that provides automated trading signals or directions

may constitute a form of commodity trading advice, which in some circumstances may be subject to regulation and registration. The CFTC has also looked at the impact of automated trading on regulated markets, and issued a controversial 2015 regulatory proposal aimed at high-frequency and other electronic trading on regulated futures exchanges, Regulation Automated Trading ("Reg AT"). (This proposal has not progressed, and is not expected to be adopted in its current form.[32]) Aside from the breadth of its proposed impact, one of the major stumbling blocks with respect to Reg AT was its requirement that the proprietary automated trading source code of registered traders be subject to inspection by the CFTC and DOJ, in some cases without requiring a subpoena.

Nonetheless, the CFTC has also continued to monitor developments with respect to automation of trading practices, releasing a report in March 2019 concerning the "Impact of Automated Orders in Futures Markets" that presented findings with respect to the amount and impact of orders generated or routed without human intervention, and the manner in which those orders are employed. More generally, the CFTC is engaging with innovators and the broader financial technology community to foster "responsible innovation" through its Technology Advisory Committee public meetings, its dedicated LabCFTC function and the related CFTC 2.0 initiative. Regarding enforcement and interpretative activity, the CFTC has made clear through various actions and no action positions that it remains focused on the manner in which automated trading systems, which could implement some form of AI, are accessed by and offered to market participants. Firms should understand that AI, like other automated systems, does not fall outside of the bounds of the CFTC's remit – the agency can be expected to use its authority to regulate derivatives markets and police fraudulent and manipulative activity in the derivatives markets, regardless of the underlying technology.

FINRA

The Financial Industry Regulatory Authority ("FINRA") is the largest self-regulatory organisation for securities firms operating in the U.S., providing regulatory oversight for broker-dealers and registered securities representatives, under the supervision of the SEC. For FINRA, technology applications to the securities markets has become a central regulatory priority.[33] FINRA has recently requested comment on emerging technologies and become a frequent convener of industry and government thought leaders to discuss not only the use of financial technology ("FinTech") by member companies, but also the use of technology in regulating the industry and enhancing member firm regulatory compliance mechanisms ("RegTech").[34] Indeed, FINRA has, itself, implemented AI and ML in its market surveillance operations, noting its ability to enhance the detection of market manipulation and collusion.[35] In April 2019, FINRA created the Office of Financial Innovation (an outgrowth of its Innovation Outreach Initiative), designed to coordinate issues related to significant financial innovations, particularly the use of FinTech. The establishment of the new office follows years of active monitoring of and engagement on technology developments, including the creation of a FinTech Industry Committee, publishing reports on FinTech and RegTech applications in the securities industry, and the hosting of four regional FinTech and RegTech conferences.[36]

Battles over source code

Different regulators have taken different tacks with respect to demanding access to sensitive source code when supervising businesses deploying AI or other sophisticated software applications. As noted above, the CFTC released a controversial proposal, Regulation AT, which would have required that source code be subject to regulatory inspection, without a subpoena. In light of the strong negative response, and as an indication of how concerned

some parties are that source code will be mishandled by the government (the highest order concern is that a company's intellectual property "crown jewels" might be stolen by hackers or even bad actors inside the government), Congress has considered (but not adopted) bills that would have prohibited the SEC and CFTC from accessing source code at their regulated firms without obtaining a subpoena. This effectively means that source code could not be accessed during an ordinary course examination of a regulated firm.

Regulation of data

Given the importance of large data sets to the effective operation of most AI, a discussion of AI is always linked to a discussion of data. There is no comprehensive legal and regulatory approach to data that applies across the U.S. Moreover, none of the federal financial regulators have put forth regulations on data that can be said to address the scope and diversity of today's data practices. Instead, a patchwork of often conflicting laws and regulations apply. Here are a few of them:

Privacy and protected classes. One constant is that many jurisdictions seek to protect "personal data" or "privacy" associated with individuals, especially names, addresses, government identification numbers, and the like. Closely related to privacy, populations deemed especially vulnerable, such as children or the elderly, are often given special data protections. Likewise, personal health and financial records, gender orientation information, political and religious affiliations and other special categories of personal information often have heightened protection.

Governmental data. Much governmental data, especially in democratic societies, is intended to be "open" and freely accessible to the public. However, it should not be assumed that any use of governmental data, even when it can be readily accessed, is permissible without consideration of the specific circumstances. Some public data sources may include restrictions that they are intended for or limited to research or other non-commercial purposes. Such restrictions may appear as disclaimers on the data itself, or may only be evident in the background laws or regulations, including criminal laws, of such governmental body. There is also a variety of instances when governmental data are explicitly non-public or restricted; e.g., in connection with governmental contracts, studies and approvals that have not yet been announced.

Website data. "Web scraping", also called crawling or spidering, is the automated gathering of data from a third-party website. Scraped data has become a vital component of the investment research programmes of many asset managers, and is critical to many business processes generally throughout the industry; and, accordingly, it is in wide use. But the permissibility of the practice – and associated legal risk – remains unclear. A variety of legal claims may apply under U.S. law to unauthorised scraping, including breach of contract, copyright infringement, trespass and other torts, and causes of action or even sanctions under state and federal laws specific to website access. Perhaps most significantly, federal law – enforceable both criminally and civilly – specifically protects websites from unauthorised access, with that phrase potentially extending the law's protections to any website whose terms of use forbid or limit automated scraping of data.[37]

Data ethics

It has been common over many years for firms that make heavy use of data to speak of their "data ethics". This is sometimes referred to as embodying the principle that the question for a firm is not whether it can (operationally or legally) put data to a particular use, but whether it *should* (whether doing so is "right"). Data ethics policies are intended to ensure that an organisation has a governance framework to answer that question and, in doing so, considers

a broad range of factors (e.g., legal and contractual requirements, technical capacity, social expectations, reputational considerations, etc.).

* * *

Endnotes

1. *AI Transportation Market Overview*, P&S Intelligence Prvt. Ltd., available at https://www.psmarketresearch.com/market-analysis/ai-in-transportation-market (last accessed April 24, 2019).
2. *The AI Journey: Artificial Intelligence and the Supply Chain*, International Business Machines Corporation, available at https://www.ibm.com/watson/supply-chain/resources/csc/desktop/index.html?page=4 (last accessed April 24, 2019).
3. *The New Age: Artificial Intelligence for Human Resource Opportunities and Functions*, Ernst & Young LLP, available at https://www.ey.com/Publication/vwLUAssets/EY-the-new-age-artificial-intelligence-for-human-resource-opportunities-and-functions/$FILE/EY-the-new-age-artificial-intelligence-for-human-resource-opportunities-and-functions.pdf (last accessed April 24, 2019).
4. Maskey, Sameer, *How Artificial Intelligence is Helping Financial Institutions*, Forbes Technology Council, available at https://www.forbes.com/sites/forbestechcouncil/2018/12/05/how-artificial-intelligence-is-helping-financial-institutions/#57695356460a (last accessed April 24, 2019).
5. *Preparing for the Future of Artificial Intelligence*, Executive Office of the President, National Science and Technology Council Committee on Technology, Oct. 2016, available at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (last accessed April 24, 2019).
6. *The National Artificial Intelligence Research and Development Strategic Plan*, National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, Oct. 2016, available at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf (last accessed April 24, 2019).
7. *Artificial Intelligence, Automation, and the Economy*, Executive Office of the President, Dec. 2016, available at https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF (last accessed April 24, 2019).
8. *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry*, The White House Office of Science and Technology Policy, May 10, 2018, available at https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf (last accessed April 24, 2019).
9. Exec. Order No. 13859, 3 C.F.R. 3967 (2019).
10. *See* Metz, Cade, *Trump Signs Executive Order Promoting Artificial Intelligence*, The New York Times, Feb. 11, 2019, available at https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html (last accessed April 24, 2019) (stating that "the [Trump] administration provided few details on how it planned [to] put its new policies into effect").
11. *Accountability of AI Under the Law: The Role of Explanation*, Berkman Klein Center Working Group on Explanation and the Law, Harvard University, Nov. 27, 2017, available at https://cyber.harvard.edu/publications/2017/11/AIExplanation (last accessed April 24, 2019).

12. Knight, Will, *The Dark Secret at the Heart of AI*, MIT Technology Review, Apr. 11, 2017, available at https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ (last accessed April 24, 2019).
13. *See* Article 22(1) of the General Data Protection Regulation (EU) 2016/679 (2018), stating: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."
14. Maureen Ohlhausen, Remarks to the Concurrences Conference on Antitrust in the Financial Sector: "Should We Fear The Things That Go Beep In the Night? Some Initial Thoughts on the Intersection of Antitrust Law and Algorithmic Pricing" (New York, May 23, 2017) at 2.

14B. Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (as referred to S. Comm. On Consumer Prot. & Commerce, Apr. 11, 2019); S. 1108, 116th Cong. (as referred to Comm. On Commerce, Sci., & Transp., Apr. 10, 2019), available at www.congress.gov/bill/116th-congress/senate-bill/1108/all-info.

15. Terrell McSweeny & Brian O'Dea, *The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement*, Antitrust, Fall 2017 at 75–76.
16. No. CR 15-00201 (N.D. Cal. 2015).
17. Margrethe Vestager, Comm'r, Eur. Comm'n, Algorithms and Competition, Remarks at the Bundeskartellamt 18th Conference on Competition, Berlin (Mar. 16, 2017).
18. Ariel Ezrachi & Maurice Stucke, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 62 (2016).
19. Ohlhausen, *supra* note 1 at 1.
20. Emilio Calvano, Giacomo Calzolari, Vincenzo Denicolò, & Sergio Pastorello, *Artificial Intelligence, Algorithmic Pricing and Collusion* (April 2019), available at www.ftc.gov/system/files/documents/ public_events/1494697/calzolaricalvanodenicolopastorello.pdf.
21. *Meyer v. Kalanick*, No. 1:15-cv-09796-JSR (S.D.N.Y.).
22. McSweeny & Brian O'Dea, *supra* note 2 at 75.
23. *Id.* at 77.
24. D. Bruce Hoffman, Remarks at Competition and Consumer Protection in the 21st Century (November 14, 2018).
25. *Id*.
26. D. Bruce Hoffman, Remarks at Computer & Communications Industry Association (April 12, 2018); *see also* GCRI, US DOJ Deputy: Algorithmic Cartel Requires Agreement (Miami, Feb. 3, 2018); Ohlhausen, *supra* note 1 at 11.
27. Ohlhausen, *supra* note 1 at 3; s*ee* Andrew Finch, Remarks at the 44th Annual Conference on International Antitrust Law and Policy (New York, September 14, 2017).

27B. Rebecca Kelly Slaughter, Comm'r, FTC, *Algorithms and Economic Justice*, Remarks at UCLA School of Law (Jan. 24, 2020), available at www.ftc.gov/system/files/documents/public_statements/1564883/ remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf.

28. *See Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.
29. *Preparing for the Future of AI*, National Science and Technology Council, Oct. 2016, available at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_

files/ microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. *AI, Automation, and the Economy*, Executive Office of the President, Dec. 2016, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf. *Summary of the 2018 White House Summit on AI for American Industry*, May 2018, The White House Office of Science and Technology Policy, available at https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf.

30. Available at https://artificial intelligencecaucus-olson.house.gov/. *Congress Takes Aim at the FUTURE of Artificial Intelligence*, Blank Rome, Jan. 2018, available at https://www.blankrome.com/publications/congress-takes-aim-future-artificial-intelligence.
31. For a discussion specific to regulator expectations of quantitative trading techniques, *see SEC Enforcements Against Quant Managers Show a Pattern*, Shearman & Sterling FinTech Blog (Jan. 15, 2019), available at https://fintech.shearman.com/sec-enforcements-against-quant-managers-show-a-pa.
32. *See* J. Christopher Giancarlo, Chairman, U.S. Commodity Futures Trading Comm'n, Remarks at the FIA Expo (Oct. 17, 2018), available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo58 ("I do not intend to advance [Regulation Automated Trading] in its current iteration").
33. FINRA, 2019 Risk Monitoring and Examination Priorities Letter (Jan. 22, 2019), available at http://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf.
34. FINRA Requests Comment on FinTech Innovation in the Broker-Dealer Industry (June 30, 2018), available at http://www.finra.org/industry/special-notice-073018.
35. FINRA, How the Cloud and Machine Learning Have Transformed FINRA Market Surveillance (July 16, 2018), available at http://www.finra.org/industry/podcasts/how-cloud-and-machine-learning-have-transformed-market-surveillance.
36. FINRA, Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry (September 2018), available at https://www.finra.org/sites/default/files/2018_RegTech_Report.pdf.
37. The most widely cited federal law in this area is the Computer Fraud and Abuse Act ("CFAA"), which makes it unlawful to "intentionally access" a computer or website without authorisation or in a manner that "exceeds authorized access". There are also numerous U.S. state law analogues.

Nathan Greene
Tel: +1 212 848 4668 / Email: ngreene@shearman.com

Nathan Greene is a partner in the Investment Funds practice at Shearman & Sterling LLP. He has extensive experience advising on the regulatory aspects of fund and investment advisory operations, and also counsels funds and financial institutions on regulatory considerations around emerging technologies like blockchain, big data and artificial intelligence. His practice includes the formation and representation of U.S. and foreign investment companies, sponsors, advisers and directors, including: SEC registration, exemptions, inspections and investigations; fund formation, distribution and marketing; fund board and governance matters; compliance manuals and testing; and high-profile corporate transactions involving asset management businesses. He is particularly well-known for his representation of prominent industry participants in the registered alternatives market, and has notable experience representing major players in M&A deals that have a registered fund component.

David Higbee
Tel: +1 202 508 8071 / Email: david.higbee@shearman.com

David Higbee is a partner in the Antitrust practice, Global Antitrust Practice Group Leader and Head of the Washington, D.C. office at Shearman & Sterling LLP. He focuses on antitrust government and internal investigations, merger review and complex litigation matters. He has represented clients in varied industries including defence, oil and gas, financial services and technology. David works regularly on matters before the Federal Trade Commission and the Antitrust Division of the U.S. Department of Justice.

David previously served at the Department of Justice as Deputy Assistant Attorney General and Chief of Staff of the Antitrust Division. In that capacity, he advised the Assistant Attorney General on all matters related to the enforcement of the U.S. antitrust laws and oversaw investigations, civil litigation, and criminal prosecutions.

Brett Schlossberg
Tel: +1 650 838 3753 / Email: brett.schlossberg@shearman.com

Brett Schlossberg is an associate in the Intellectual Property Transactions Group at Shearman & Sterling LLP. His practice consists of counselling clients in technology and data intensive sectors on transactions involving the complex allocation of IP rights, including the negotiation of key deal terms and evaluation of transactional risks, and in the context of the broader business objectives in order to provide comprehensive advice on how to optimise, manage and protect an IP portfolio. His practice also consists of general commercial transaction work advising clients on all phases of the product life cycle, from research and development through to distribution, marketing and post-launch regulatory compliance. He also assists in the navigation of evolving regulatory and legal frameworks in order to help drive growth through the intelligent commercialisation of a variety of hardware, software, pharmaceutical and medical device products.

Shearman & Sterling LLP

599 Lexington Avenue, New York, NY, 10022-6069, USA
Tel: +1 212 848 4000 / URL: www.shearman.com

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