GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2023

Fifth Edition

Contributing Editor: **Charles Kerrigan**

glg global legal group

Global Legal Insights
AI, Machine Learning & Big Data

2023, Fifth Edition
Contributing Editor: Charles Kerrigan
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – AI, MACHINE LEARNING & BIG DATA

2023, FIFTH EDITION

Contributing Editor
Charles Kerrigan, CMS Cameron McKenna Nabarro Olswang LLP

Publisher
James Strode

Production Deputy Editor
Maya Tyrrell

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Charles Kerrigan of CMS Cameron McKenna Nabarro Olswang LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-83918-272-3
ISSN 2632-7120

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
June 2023

CONTENTS

PREFACE

Artificial intelligence ("AI") is a difficult topic for lawyers. It is a broad topic, far broader than most topics that lawyers engage with. It does not align at all with the usual disciplines that lawyers work in; that is, it is not a creature of corporate law, property law, intellectual property law, etc. But it does touch on aspects of each of these and more. It does not align with sector or industry groups that commercial lawyers organise themselves into; that is, it is not confined to a single industry and is as relevant to the financial services industry and many others as it is to the technology industry. It relies on a certain level of technical knowledge of how software operates that is not part of the training or experience of many lawyers. The law and regulation that applies to AI is, by and large, not yet written. When it is written, it will differ between jurisdictions and AI developers and users will be subject to multiple overlapping rules. It will take forms that require interpretation beyond the conventional approach of many lawyers because it will involve judgments on risk and suitability, not just legalistic questions.

Borrowing from former American president John F. Kennedy, this is a topic for lawyers who like to work on things not because they are easy but because they are hard. In this case they are also necessary because AI is pervasive and lawyers have a substantial role to play in advising commercial, not-for-profit, governmental and clients of all other types on this topic.

The editorial team is therefore pleased to introduce a report in which so many colleagues around the world have again risen to the challenge. The headlines for this edition are:

- public interest and concern around generative AI use cases ("scary good", as Elon Musk correctly reports);
- policymaker interest and concern about the social implications of job loss, displacement and replacement; and
- the continuing progress towards implementation of the EU AI Act which is likely to set a set a standard for other jurisdictions.

Even in jurisdictions where there is no legislation directly relating to AI, clients request advice on best practice, risk management, horizon-scanning and a range of other topics related to the development and use of AI technologies. The approaches that we adopt are common to many other emerging technologies.

There is wide debate about whether AI is a technology that will do good or do harm in the world. Part of the lawyer's role here is to support AI for good.

Charles Kerrigan
CMS Cameron McKenna Nabarro Olswang LLP

AI Governance and Risk Management: Regulations and Case Law in 2023

Charles Kerrigan, Emre Kazim & Marcus Grazette
CMS Cameron McKenna Nabarro Olswang LLP & Holistic AI

Introduction

Companies are increasingly adopting artificial intelligence (AI). This has delivered value, including through efficiencies and cost savings. In parallel, individuals are increasingly aware of the AI systems they interact with daily. High-profile scandals, including where systems have caused harm, drive public concern and regulatory efforts to ensure that these systems are trustworthy.

The latest figures[1] from IBM's global AI adoption survey show 42% of companies are exploring AI adoption and 35% already using AI. The headline figures mask the fact that "adoption" is not simply a "yes/no" concept. Gartner[2] found that nearly half of organisations have hundreds or thousands of deployed models. Managing systems on this scale requires robust, systematic approaches to governance, risk, and compliance.

In parallel, public and consumer awareness of AI use, risks, and data practices is growing. Debates about AI's societal impact are not new. But public access to tools like ChatGPT and Stable Diffusion mean that such debates have become widespread. The spotlight on bias and discrimination – including through global, high-profile campaigns mean greater scrutiny on how organisations interact with stakeholders like employees, candidates for employment, and customers.

Finally, we are seeing interventions across the supervisory ecosystem to manage AI risks. These include new legislative proposals (e.g., the EU's proposed AI Act), robust enforcement of existing data protection or consumer protection rules, and a host of principles, standards, and best practice guidance under a broad "trustworthy AI" umbrella.

The OECD's AI policy tracker covers over 70 countries and nearly 300 regulatory oversight initiatives. But regulatory proliferation isn't as daunting as it first appears. We're already starting to see convergence around a need to protect individuals from harm and take a risk-based, proportionate approach.

Taken together, these three trends create a significant business challenge. Companies must respond to the commercial imperative to adopt AI, while ensuring that their systems are trustworthy, effective, and compliant. There is also a clear business imperative to improve confidence in AI systems. Whether building or buying, businesses need to be sure that their system will work as expected and deliver results in line with their investment. Our conversations often reveal that companies have little clarity on their system's performance or effectiveness.

This chapter explains how AI assurance and risk management can help companies to navigate the complexity. Assurance is partly about testing systems and revealing information about their performance. It supports broader governance initiatives by allowing organisations to make informed choices about the systems and context in which they are deployed.

Industry scan – who is adopting AI and why?

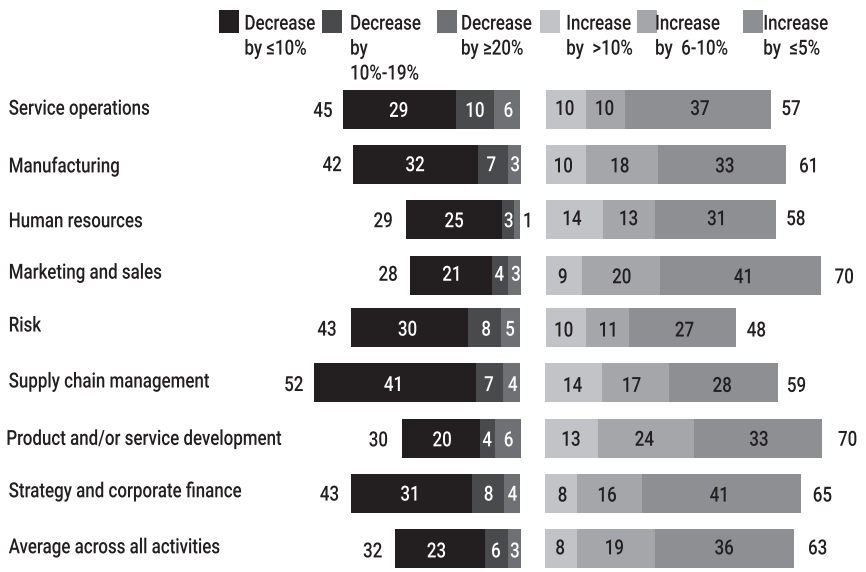
Adoption varies between sectors and use cases, but the IBM survey shows a clear theme around using automation to improve employee productivity and reduce costs. In many cases, automation focuses on so-called "back end" business processes such as IT network monitoring, IT security and threat detection, and analysing data from sensors. Nearly half of companies surveyed used AI to improve IT efficiency, giving time back to employees. Automation can also support front line services and customer interaction, for example when used for identity verification, fraud detection, personalisation or customer service chatbots.

Governance, risk and compliance issues vary by use case. For instance, a system designed to manage IT resource allocation may not use personal data and therefore not trigger data protection requirements. However, the organisation will still want to verify that it works as expected as the decisions it recommends, or takes, can have significant cost implications.

On the other hand, an identity verification system based on facial recognition will process biometric data and need to perform to an acceptable standard across a variety of skin tones. This triggers data protection requirements and the need to test for discrimination. We discuss examples of industry-specific requirements in the governance section below.

We're seeing a particular trend towards the use of AI in human resources (HR), where it is associated with significant cost savings and revenue increases, according to research conducted by McKinsey.[3] Technological advances, including natural language processing and AI-powered video interviews, allow companies to process candidates at scale. Some companies, particularly online platforms like Uber or Deliveroo, also use automated systems to assign work, and many others use AI tools to score or assess employee performance, including some 360° feedback systems.

Cost decrease and revenue increase from AI adoption in 2021, by function, % of respondents[4]

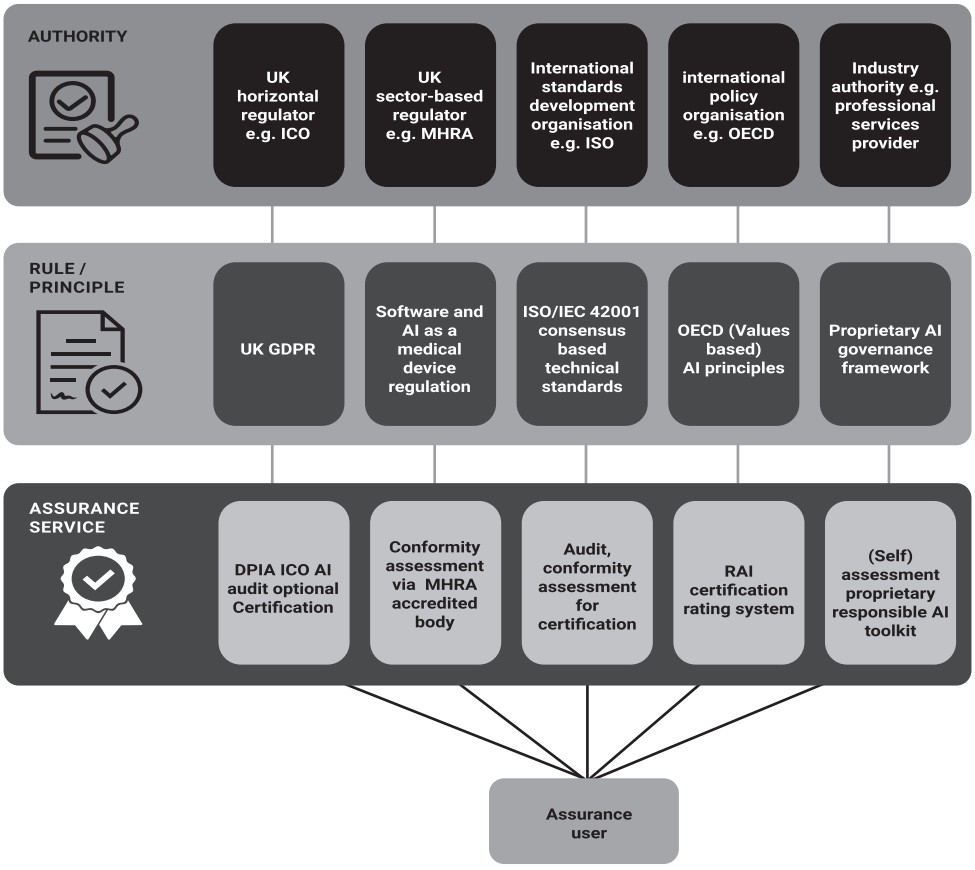


[Graph from McKinsey's State of AI in 2022 report]

The AI governance ecosystem

As recognition and understanding of AI risk grows, we are seeing supervisory interventions on several fronts. We group these into three broad categories: enforcement and interpretation of existing rules; new legislation or regulation; and standards development. The layers work together to form the AI governance ecosystem, with independent AI assurance services supporting and verifying compliance.

The role of AI assurance services in AI governance



[Image from CDEI Source: https://cdeiuk.github.io/ai-assurance-guide/governance]

Regulators and courts have focused on clarifying, updating and interpreting existing requirements with respect to AI and automated systems. We draw on examples from the main jurisdictions we cover in this chapter, the UK, EU, and US. Our key takeaway is that existing rules already impose clear governance requirements.

For example, **European** data protection authority decisions on Article 22 GDPR rights relating to automated decision making in the context of gig economy workers relies on concepts of fairness in Article 5(1) GDPR; interpreting fairness to include a requirement to assess whether a system displays bias. Similarly, the **US Federal Trade Commission** has confirmed that a biased system can be unfair within the meaning of banned "unfair and deceptive" trade practices.

However, AI also presents novel risks that existing regulation may not sufficiently address. We are therefore also seeing new AI-specific regulation, either covering AI generally or the use of AI in a sector or for specific purposes. We discuss these in more detail in the "Regulation" section below.

The third category is perhaps the most complex. Standards bodies at international, regional and national levels are developing the technical standards that organisations will use to implement the principles in legislation. These bodies include the National Institute for Standards and Technology (NIST), the Institute of Electronics and Electrical Engineers (IEEE), The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), and the International Organization for Standardisation (ISO).

Approaches to standardisation vary between jurisdictions, sector and context. For example, the NIST AI Risk Management Framework is explicitly a voluntary standard. In other contexts, certified compliance with relevant standards can create a presumption of compliance – for example for product liability purposes.

Laws, regulations and standards generate requirements for businesses, which fall into two broad categories: technical and "non-technical" (or "organisational"). Technical requirements tend to apply to the system itself, including the data used to train and test it, the choice of model, and so on. AI assurance providers would typically use quantitative measurement to evaluate technical requirements, relying on people with computer science and machine learning skills.

On the other hand, organisational requirements tend to focus on the decisions an organisation makes about a system, including when and how to use it, internal accountability processes, the level of human oversight, and so on. AI assurance providers would typically rely on people with legal and policy skills to make qualitative assessments.

Risk verticals

Risk verticals are the main thematic areas of risk associated with AI systems. From a legal perspective, we could describe the risk with respect to the requirements defined in laws, regulation and standards. The risk might be technical or relate to governance and compliance, either with legal or broader "responsible AI" obligations. There are several different approaches to grouping drivers of AI risk, although the different sets of principles broadly overlap or map onto one another. The OECD's AI principles[5] and EU's Assessment List for Trustworthy AI[6] are just two examples.

We will use four of the cross-sectoral principles from the **UK** government's 2022 paper on establishing a pro-innovation approach to regulating AI.[7] These are: safety; robustness; transparency; and fairness. The paper includes two further principles – legal responsibility and redress – that are less relevant technical aspects of AI assurance.

Safety

We typically think of safety in the context of medical devices and medical decision tools, industrial automation, driver assistance or self-driving cars. There is increasing recognition that systems with a less obvious link to safety can also cause harm. For example, in the context of the **UK's** Online Safety Bill a content recommendation system that exposed users to harmful content. In September 2022, the coroner concluded that the "negative effects of online content" were a factor in the death of a minor in 2017.[8]

We have already seen several UK examples of claims for distress in a data protection context. *Lloyd v Google*[9] and *Rolfe v Veale Wasborough Vizards LLP*[10] are perhaps the best-

known examples. In *Lloyd*, a privacy rights campaigner attempted to bring a representative action (or class action) against Google. Mr Lloyd claimed that Google used a technical workaround to access data on users' iPhones without their consent, and that Google's actions caused harm because users lost control over data about them.

In *Rolfe*, a demand for payment that should have gone to Mr & Mrs Rolfe was misdirected to another person because of a mistyped email address. The Rolfes argued that they suffered distress due to the breach of confidence that occurred when information about their account was accidentally shared with another person.

The courts rejected specific claims for damages in both *Lloyd* and *Rolfe* but left the possibility of future claims open. Article 82 of the GDPR defines harm broadly, so we may start to see a new category of claims for harm caused by AI systems emerge. For example, would an organisation deploying a customer service chatbot be liable for the bot causing distress by generating offensive or insensitive responses?

Robustness

A system is robust if it is technically secure and performs as designed under normal conditions of use. This clearly links to safety – as a system may be unsafe if it is not robust. Some approaches to AI risk consider safety and robustness as a single requirement, for example the **EU's** Assessment List for Trustworthy AI (ALTAI). AI assurance includes testing systems for robustness, either by adversarial attack or manipulating input data.

Testing systems by attacking them is well-established cybersecurity practice. The **UK's** National Cyber Security Centre (NCSC) describes penetration testing as "a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might".[11]

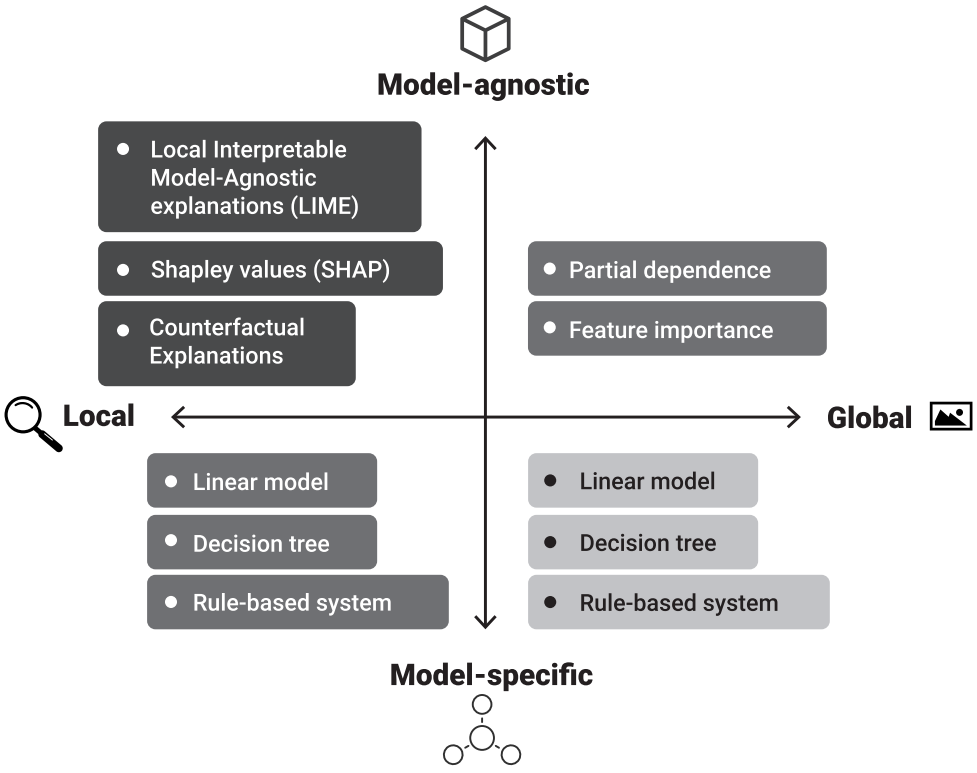
Researchers have demonstrated several AI security vulnerabilities, including model inversion attacks which enable the attacker to recover data used to train the model. For models trained on personal data, a model inversion attack could lead to a data breach. Organisations need to be confident that they are meeting the Article 32 **GDPR** requirements to implement appropriate technical and security measures, with respect to the current state of the art.

Researchers have also demonstrated techniques for manipulating input data. For example, applying stickers to "stop" signs caused image classifier systems used in autonomous vehicles to misclassify the sign – incorrectly identifying it as a speed limit sign in nearly all lab tests and in most drive-by tests. The same principles apply to other systems receiving unexpected inputs.

The proposed **EU AI Act** shows that legislators are drawing on concepts of robustness and proper functioning under normal conditions of use from the product liability space. Article 19 envisages a conformity assessment and CE mark for high-risk systems to enable them to be placed on the market and Article 62 a monitoring regime for incidents and malfunctions once a product is on the market.

Transparency

Transparency operates at three main levels. First, transparency around why and how the system generates outputs. This is linked to explainability or interpretability. Technical approaches to transparency sit on a spectrum between local and global and between model-specific and model-agnostic, summarised in the diagram below.



[Image source: https://www.holisticai.com/blog/ai-transparency]

Second, transparency can also relate to system governance and decisions about a system throughout its life cycle. Organisations typically operationalise transparency in this sense through documentation, which can support assurance and verification and help to discharge regulation requirements. For example, the **EU's** proposed AI Act includes specific transparency requirements for high-risk systems. These are required to have extensive technical documentation described in Article 11 and Annex IV of the proposed text.

Finally, transparency involves an element of communication with relevant stakeholders. Each stakeholder's needs, and therefore the appropriate communication, will vary. For example, an internal data science team working to improve a model will need different explanations than a customer presented with an output (e.g., model-generated a credit score). Explainability is a legal requirement in some cases, links to fairness and robustness and can play an important role if an organisation is challenged on its use of AI. Our summary of the Apple Card case in section 4 below, where gender bias was alleged but found not to exist, provides an example.

We are seeing significant regulatory focus on transparency. Ranging from rights to be informed that an automated system is being used, to meaningful information on the logic and performance, including on the risk of bias or discrimination. However, regulators recognise the need for balance. Transparency can lead to unintended consequences if publishing information about the model allows the system to be gamed or exploited.

Fairness

There are three main definitions of fairness in a computer science context. These are: (1) disparate impact; (2) equality of opportunity; and (3) disparate treatment. To explain how

they work in practice, imagine a system that aims to predict whether individuals in a group are "high" or "low" risk of defaulting on a loan. The group of individuals may contain several sub-groups, perhaps linked to protected characteristics like gender or ethnicity.

Taking each of the three technical definitions of fairness in turn:

- Disparate impact: The system is fair if the proportion of individuals sorted into the "high" or "low" risk categories is the same for each sub-group. For example, if classifier predicts than 20% of men are "high" risk, it will also predict that 20% of women are "high" risk.
- Equality of Opportunity: The system is fair if the accuracy of its prediction is the same across all subgroups. For example, if the system is 80% accurate at predicting whether a man is "high" risk and is also 80% accurate at predicting whether a woman is "high" risk. In more technical terms, prediction accuracy is unaffected by group membership.
- Disparate Treatment: The system is fair if the error rate affecting the accuracy is the same across different subgroups. This is not simply the flipside of the "equality of opportunity" definition, because different types of errors can affect accuracy.

The examples of fairness above only compare impacts based on membership of one subgroup. Real world assessments should also consider intersectionality, as individuals may belong to several groups. In addition, organisations need to choose a definition of fairness – it is mathematically impossible for a system to satisfy all three.

Definitions of fairness also derive from legislation. For example, the **US** Equal Credit Opportunities Act and Fair Housing Act recognise disparate treatment and disparate impact. In that context, disparate treatment refers to the intentional use of a protected characteristic in lending decisions. On the other hand, disparate impact is much closer to the computer science definition above; it refers to policies that result in unequal outcomes for members of protected classes. From a legal perspective, disparate treatment is prohibited while disparate impact can be justified in some circumstances.

Legal responsibility

The **UK's** Digital Regulators Cooperation Forum (DRCF) notes that AI systems often involve several parities. For example, one organisation might collect and label data then license such data to another who builds and trains a model. This can leave developers, businesses, and consumers unsure about their responsibilities. The **EU's** proposed AI Act places responsibility mainly on providers (the natural or legal person developing the system and placing it on the market) and users (the natural or legal person using the system).

Routes to redress

The **DRCF** is also keen to provide routes to redress for individuals, including through simplifying complaints processes to enable individuals to see redress "without having to navigate separate regulatory systems". We are also seeing requirements for organisations to provide options for individuals to request alternative treatment. For example, the **New York City** bias audit law (Local Law 144) requires companies using automated employment decision tools to allow candidates for employment to request alternative processes. This is similar to "reasonable adjustment" requirements in existing equality law.

Regulation

The following subsections describe developments in 2022 and outline our expectations for 2023 in the UK, EU, US, and China. We are seeing a trend towards risk-based approaches, with businesses required to assess and manage risk. AI assurance and governance processes

are becoming increasingly important as a source of evidence that appropriate action has been taken.

We are also seeing alignment on the rights and responsibilities approach. Consumers have various rights, for example not to be subject to fully automated decision making. Businesses have responsibilities around transparency, governance and risk management. The main contrast between jurisdictions is their approach to AI specific laws. The **UK** wants to avoid horizontal AI regulation, while the **EU** is embracing it.

Note that this section focuses on AI-specific regulation. There may be a range of other compliance requirements depending on the sector and context in which a business plans to use AI. For example, data protection, product liability and broad reputation management considerations will all be relevant. See the country specific chapters for more detail on these.

The United Kingdom

The UK aims to develop a coherent, context-specific approach to AI regulation. Rather than setting out rules for AI generally, the Department for Culture, Media, and Sport wants individual regulators to define requirements for specific sectors or use cases. Some sector regulators are already consulting on specific rules, including the Medicines and Healthcare Regulatory Authority,[12] and others have published guidance, including the Bank of England.[13] Changes in central government on 7 February 2023 mean that the new Department for Science, Innovation and Technology[14] will likely take over responsibility for the UK AI policy.

The UK is also keen to lead AI assurance by building a sector modelled on the financial audit industry. The UK's Centre for Data Ethics and Innovation published a roadmap[15] to a mature AI assurance ecosystem in 2022. This ecosystem will provide the services to "independently verify the trustworthiness of AI systems".

UK regulators already have powers to examine data and algorithms in certain circumstances. We are seeing a clear statement of their intention to focus on AI in HR and employment. For example, the ICO's annual action plan[16] for 2023 states that they "will be investigating concerns over the use of algorithms to sift recruitment applications, which could be negatively impacting employment opportunities of those from diverse backgrounds" and "will also set out our expectations through refreshed guidance for AI developers on ensuring that algorithms treat people and their information fairly".

Similarly, the Equality and Human Rights Commission also flag "addressing the equality and human rights impacts of AI" in their strategic plan for 2022–25.[17] The EHCR will focus on discriminatory decision making and the risk that some groups are excluded from accessing information or services, particularly older and disabled people, and those from ethnic minorities.

The European Union

The EU continues to focus on a risk management approach to AI. We expect the EU AI Act to pass in mid-2023 and come into force in 2024, and the European standardisation organisations to publish the detailed standards that organisations will need to implement the AI Act on the same timeframe. Two other pillars of the EU's package of digital regulation, the Digital Services Act (DSA) and Digital Markets Act (DMA), also include specific requirements for algorithmic systems but have a narrower scope, as we explain below.

The EU AI Act[18] groups AI systems into risk categories based on whether they pose a low, limited, high or unacceptable risk to individuals. Systems deemed to carry an unacceptable risk are banned from sale on the EU market. These include systems that

manipulate behaviour, exploit vulnerabilities based on age, physical or mental disability, or socioeconomic status, are used for social scoring by governments or for real time biometric monitoring in a public area by law enforcement.

EU legislators expect that most systems currently used will be low risk. This includes systems such as spam filters and AI-powered games. On the other hand, a system is classed as limited risk if it interacts with humans (e.g., a simple chatbot), detects humans or determines a person's categorisation based on biometric data (e.g., matching a selfie to a person's photo ID document during customer onboarding) or can produce manipulated content (e.g., text, images, or video). Systems in the limited risk category will need to comply with transparency requirements, ensuring that users are aware that they are interacting with, or consuming content produced by, an AI system.

The AI Act focuses on high-risk systems, listing three criteria companies can use to determine whether their system should be classed as high-risk: (1) if the system is a product that requires third party conformity assessment before being placed on the EU market; (2) if the system is intended to be used as a safety component in a product that requires conformity assessment; or (3) if the system is listed in Annex III of the AI Act.

The Annex III list is hotly debated, and we expect it to continue to evolve. A new proposal, introduced on 6 February 2023,[19] aims to add biometric identification to this list and move categorisation based on biometrics from the limited risk to the high-risk category, among other changes. It also creates a residual category for generative AI systems, like ChatGPT, that create content that could be mistaken for human generated content. The debate highlights the challenges with defining proscribed lists of use cases and reacting quickly to technological developments.

In parallel, European standardisation organisations are working to bridge the implementation gap by translating high level principles in the AI Act into actionable standards documents. Defining objectives and measurement criteria will support the AI assurance ecosystem. The European Commission has taken the unusual step of asking CEN/CENELEC, the standardisation body, to work in parallel with the legislative process.[20] It's likely that the Commission aims to accelerate adoption considering concerns about the impact high risk systems can have on individuals.

Unlike the AI Act, both the DMA and the DSA apply to a narrowly defined set of online businesses. The DMA applies to online gatekeepers, who provide services like search engines, social networking, video sharing, and so on. A company providing these services is in scope for the DMA if they meet the three objective criteria: (1) are of a size that impacts the internal market; (2) control and important gateway linking businesses to consumers; and (3) are in an entrenched and durable position. Similarly, the DSA applies to very large online platforms, defined as having more than 45 million average monthly users in the EU and very large online search engines.

The DMA and DSA both impose transparency requirements for AI systems and the DMA additionally requires independent audits for systems used to profile customers (defined in Article 4 of the GDPR) across any of the core platform services. We anticipate that companies active in the online advertising ecosystem will be among the most affected as they often use detailed profiles to deliver ads and measure advertising performance.

The DSA also imposes clear audit and transparency requirements. For example, Article 28 requires annual, independent audits and Article 29 requires platforms to describe the main parameters used in their recommendation systems. The focus on recommendation systems may read across to the UK's online safety bill with its focus on how platforms identify and remove harmful content.

Beyond the specific AI regulation package, EU proposals[21] for a revised Product Liability Directive, revisions[22] to the eIDAS Regulation on European Digital Identity and instruments including the Data Act,[23] Data Governance Act,[24] NIS2 Directive[25] and Cyber Resilience Act[26] may also be relevant to organisations developing and deploying AI systems.

The United States

Elsewhere, the Biden White House issued a series of Executive Orders on AI in late 2020. Taken together, these help to define the US regulatory approach at the federal level. For example, EO 13859[27] directs the National Institute for Standards and Technology to develop standards and tools to support trustworthy AI and EO 13960[28] creates an inventory of AI use cases.

The White House also published a blueprint for an AI Bill of Rights in October 2022. The blueprint is framed as a "guide for society" and is likely to remain a voluntary set of principles, all of which are all relevant to AI assurance, particularly the focus on safe and effective systems and on protection from discrimination.

In addition to voluntary standards, legislation is progressing too. The Algorithmic Accountability Act was reintroduced[29] in 2022 and state legislatures are active, passing or proposing AI specific rules and developing their data protection rules. The table below summarises the main US legislation:

Name	Summary	Status
Illinois Artificial Intelligence Video interview Act	Requires employers to give candidates notice that AI will be used to evaluate their video interview and the characteristics it will consider.	In force – 1 January 2020
NYC Local Law 144	Requires bias audits of automated employment decision tools, publication of a summary of the results of the audit, and disclosure of the use of an automated tool and the characteristics it will consider.	Enacted – in force from 15 April 2023
California Proposed Amendments to Employment Regulations Regarding Automated Decision Systems	Prohibits employers from discriminating against candidates based on protected characteristics, including using automated decision systems.	Proposed
California Workplace Technology Accountability Act	Limits electronic monitoring to locations and activities, requires impact assessments of automated decision systems and worker information systems, gives workers' rights about their data, and introduces notification requirements.	Proposed
DC Stop Discrimination by Algorithms Act	Prohibits covered entities from using systems that discriminate based on protected characteristics and prevent subgroups from accessing important life opportunities.	Proposed
US Algorithmic Accountability Act of 2021	Requires impact assessments of systems used in critical decisions such as employment to identify issues such as bias, performance, transparency, privacy and security, and safety.	Proposed

We are also seeing regulators interpret existing rules to bring AI systems explicitly into scope. For example, the Federal Trade Commission (FTC) reminded companies deploying AI to keep their practices "grounded in established FTC consumer protection principles" and confirmed that the FTC can challenge discriminatory models as "unfair".

China

In the East, the Chinese legal and regulatory regime continues to focus on protecting consumers, particularly vulnerable groups, from deepfakes and disinformation. We're seeing legal requirements at national, regional, and local levels.

China's deep synthesis provisions (formally the Provisions on the Administrate of Deep Synthesis of internet-based information services)[30] came into force in January 2023. The provisions apply to algorithmic systems that produce synthetic text, images, or video. They also apply to AI systems that alter content, such as face replacement. Companies using this technology are required to implement controls to ensure transparency (informing users when they are interacting with synthetic content), and to establish broad governance systems to review algorithms, ensure real-name user registration, and protect children.

We are also seeing moves to regulate automated recommendations systems. China's Internet Information Service Algorithmic Recommendation Management Provisions came into effect on 1 March 2022 and requires audits and transparency for automated recommendation systems. This applies to price discrimination and dynamic pricing, and the transparency requirements are likely to be significant for gig economy workers.

As well as these national efforts, we are also seeing developments at the regional level. For example, in Shanghai, regulations aim to promote the AI industry by creating regulatory sandboxes, supervised spaces where companies can develop and test new technologies. Additionally, Shenzhen has taken a similar risk management approach but focuses on the need for risk assessments to identify adverse effects from products and services. The Shenzhen government will develop and manage a risk classification system.

We expect that companies in the West could feel the impact of Chinese AI regulation through the global supply chain, as Shenzhen is a global manufacturing hub and increasingly producing AI enabled products.

Case law

Overview

As the preceding section on legal and regulatory interventions suggests, hooks for enforcement action are increasing. The case law and regulatory decisions summarised below illustrate some of the key trends. These include: (1) a focus on transparency and explainability in the Apple Card investigation; (2) leveraging existing requirements for fairness in data protection and anti-discrimination law in the gig worker decisions; and (3) class action suits, particularly in the US.

The case law also raises a question on the definition of AI. Definitions vary, but common elements[31] include AI as a machine-based system for generating outputs, including predictions or scores, based on an abstraction or model of the relationships between variables in some input data. AI does not need to operate autonomously and can be used as a decision-aid.

New York State Department of Financial Services, 2021

Apple and Goldman Sachs launched Apple Card in 2019. High-profile social media users questioned whether the credit scoring systems were biased against women after anecdotal evidence of couples with shared finances in which the male partner was offered a much higher credit limit than the female partner.

The New York State Department of Financial Services launched an investigation[32] into the allegations. Relying on fair lending rules that prohibit lenders, including credit card issuers,

from considering an applicant's sex and marital status in issuing credit, the Department noted that lenders are permitted to offer different terms to borrowers based on "objective differences in their creditworthiness".

The Department examined underwriting data for around 40,000 Apple Card applicants. They did not find violations of fair lending laws. They found that the bank's lending policy and statistical models did not consider prohibited characteristics and would not produce disparate impacts.

At the Department's request, the bank explained Apple Card credit decisions to any individuals who submitted a discrimination complaint. The Department found that the bank was able to identify the factors that led to credit decisions and that decisions were consistent with the bank's credit policy and did not entail any unlawful bases for credit determination.

Italian Data Protection Authority decisions in 2019 and 2021

The Italian Data Protection Authority (the *Garante*) investigated two gig economy platforms, namely Foodinho and Deliveroo, and published decisions in 2019 and 2021, respectively. The investigations focused on personal data processing and whether the platforms were complying with their GDPR obligations, including the Article 5(1) requirement to process data fairly and the Article 22 rights with relation to profiling and automated decision-making.

The *Garante* found that Foodinho was profiling riders within the meaning of Article 22.[33] Foodinho calculated an "excellence score" based on parameters including (1) efficiency, (2) customer feedback and (3) rider feedback. Foodinho used the excellence score to guide job allocation; if several riders were available to complete a job the system allocated the job to the rider with the highest excellence score.

Since job allocation could have a significant effect on riders, the *Garante* criticised Foodinho for failing to implement technical and organisational measures to protect riders' interests. These could include regularly assessing whether scores were correct and accurate. The *Garante* also found that Foodinho did not take appropriate measures to avoid the improper or discriminatory use of customer feedback, which counted for 20% of the overall score.

The findings in the Deliveroo case were similar. Again, the *Garante* concluded that Deliveroo should identify and implement appropriate measures to verify the accuracy and correctness of scores and minimise the risk of errors.

Huskey v State Farm, 2019

State Farm is a US insurance company that uses AI to evaluate insurance claims. The defendant, Jacqueline Huskey, alleges that State Farm's fraud detection system is biased against Black customers in that it is more likely to flag their claims as high risk, delaying or reducing pay outs. Ms Huskey relied on the US Fair Housing Act[34] and aims to bring a class action claim on behalf of State Farm's Black policyholders.

The case is based on a survey by the Center on Race, Inequality and Law at the NYU School of Law. The Centre worked with You Gov, a polling company, to survey around 800 State Farm customers. Compared to White customers, Black customers were 20% more likely to have three or more interactions with a State Farm employee at 39% more likely to have to submit extra paperwork to support their claim.

State Farm issued a statement in response.[35] "We take this filing seriously", said Gina Morss-Fischer, a State Farm spokeswoman. "This suit does not reflect the values we hold at State Farm. State Farm is committed to a diverse and inclusive environment, where all customers and associates are treated with fairness, respect, and dignity. We are dedicated

to paying what we owe, promptly and courteously". We are not aware of any further detail, for example results from a bias assessment on the automated system, at the time of writing.

Governance, risk and compliance

Governance and risk management underpin an organisation's approach to compliance. Governance typically includes all an organisation's processes for making decisions about an AI system, including whether it is appropriate to use AI in each context and how to identify, document and manage risks associated with the system.

Governance

Effective governance supports AI assurance, accountability, risk management and compliance activity. Governance should run through a system's whole life cycle. For example, at the concept stage, this could include questions about the system's objectives and how to measure them, whether appropriate data sources are available for training and testing – including whether GDPR considerations apply, either to sourcing data or collecting information about protected characteristics to test for bias.

Governance processes would apply throughout the development and testing phases, as decisions about how the system should function and the metrics used to test it are documented. Organisations should also consider how they will monitor and intervene to correct errors or model drift post-deployment. Some organisations, mainly in the public sector, may also need to add the system to public transparency registers.

Gartner research suggests that most organisations are not actively managing or monitoring model performance and data integrity post-deployment.[36] This suggests that businesses relying on outputs from automated systems to inform or guide business decisions are running a significant operational risk.

Risk management

An effective governance process enables an organisation to identify and manage risks. As we discussed above, risks can be technical (e.g., relating to the model, training data) or organisational (e.g., legal or reputational risk or the financial risks associated with a poor business decision based on an automated recommendation).

AI assurance should include recommendations to manage both categories of risk. For example, suppose testing identifies bias in a model used to recommend candidates for interview. The organisation could make a technical intervention to adjust training data or model weights or change the way human HR professionals use system-generated recommendations. In practice, both types of intervention are likely to be required and organisations will also need to account for residual risk.

Compliance

As we have seen, there is a clear trend towards risk management approaches in new AI regulation and the GDPR already embeds risk-based approaches to personal data use. Organisations with robust governance and risk management are therefore best placed to ensure compliance with the increasing number of AI or use case specific rules. Embedding a risk management culture allows organisations to move away from a costly, reactive, *ad hoc* approach to regulation.

Conclusion

Throughout this chapter, we have discussed the critical importance of a risk management approach to AI systems and seen the value of AI assurance. Governance and risk

management are already, or are quickly becoming, legal requirements, and there are plenty of examples of what can happen when AI systems are misused or not governed adequately. AI governance, risk management, and compliance can increase trust, improve public image, and avoid liability; they make good business sense.

Research by Infosys found that companies with strong governance are more satisfied with their AI outputs.[37] It makes sense that governance leads to better outcomes. Defining of what a system should do, the data that will be used to train and test it, metrics for success and assurance to independently verify its performance are all key elements of a robust governance programme. This helps organisations to make better decisions about AI and means that AI is an asset, rather than a liability.

* * *

Endnotes

1. https://newsroom.ibm.com/2022-05-19-Global-Data-from-IBM-Shows-Steady-AI-Adoption-as-Organizations-Look-to-Address-Skills-Shortages,-Automate-Processes-and-Encourage-Sustainable-Operations.
2. https://www.gartner.com/en/newsroom/press-releases/2022-08-22-gartner-survey-reveals-80-percent-of-executives-think-automation-can-be-applied-to-any-business-decision.
3. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review.
4. Question was asked only of respondents who said their organisations have adopted AI in a given function. Respondents who said "no change", "cost increase", "not applicable", or "don't know" are not shown.
5. https://oecd.ai/en/ai-principles.
6. https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal.
7. https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement.
8. https://techcrunch.com/2022/09/30/molly-russell-inquest-verdict/.
9. https://www.supremecourt.uk/cases/uksc-2019-0213.html.
10. https://uk.practicallaw.thomsonreuters.com/Document/I2c910cf0326211ecbea4f0dc9fb69570/View/FullText.html?ppcid=d7f1c356c1a04660a91e259c1f493b93&originationContext=assetPage&transitionType=KnowHowItem&comp=pluk&contextData=%28sc.Default%29.
11. https://www.ncsc.gov.uk/guidance/penetration-testing.
12. https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap.
13. https://www.bankofengland.co.uk/prudential-regulation/publication/2022/june/model-risk-management-principles-for-banks.
14. https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology.
15. https://www.gov.uk/government/publications/the-roadmap-to-an-effective-ai-assurance-ecosystem/the-roadmap-to-an-effective-ai-assurance-ecosystem.
16. https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/annual-action-plan-october-2022-october-2023/safeguard-and-empower-the-public/.
17. https://www.equalityhumanrights.com/en/publication-download/strategic-plan-2022-2025.

18. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.
19. https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-crunch-time-on-high-risk-categorisation-prohibited-practices/.
20. https://ec.europa.eu/docsroom/documents/52376?locale=en.
21. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807.
22. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid.
23. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.
24. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-governance-act.
25. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive.
26. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act.
27. https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.
28. https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.
29. https://www.congress.gov/bill/117th-congress/senate-bill/3572.
30. http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm.
31. https://www.holisticai.com/blog/comparing-definitions-of-ai.
32. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202103231.
33. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.
34. https://www.justice.gov/crt/fair-housing-act-1.
35. https://www.nytimes.com/2022/12/14/business/state-farm-racial-bias-lawsuit.html.
36. https://www.gartner.com/en/newsroom/press-releases/2022-08-22-gartner-survey-reveals-80-percent-of-executives-think-automation-can-be-applied-to-any-business-decision.
37. https://www.infosys.com/iki/podcasts/ahead-cloud/understanding-ethics-algorithms.html#audio-player-part.

Charles Kerrigan
Tel: +44 20 7067 3437 / Email: charles.kerrigan@cms-cmno.com
Charlie Kerrigan is a lawyer working in finance and emerging technology with specialisms in AI, crypto and DeFi. He is an Advisor to Cointelligence Fund; a Board Advisor to Holistic AI; an Advisory Board Member of the Investment Association's Engine; and an Advisory Board Member of the UK APPGs on AI and Blockchain. He is editor of *Artificial Intelligence Law and Regulation* (Edward Elgar) and author of *The Financing of Intangible Assets*:*TMT Finance and Emerging Technologies* (Butterworths, 2019).

Emre Kazim
Tel: +44 78 2766 6944 / Email: emre.kazim@holisticai.com
Emre Kazim is the co-CEO and co-Founder of Holistic AI.

Marcus Grazette
Tel: +447817957799 / Email: marcus.grazette@holisticai.com
Marcus Grazette works on public policy at Holistic AI. He is a tech policy expert with 15 years' experience and has previously worked at the Information Commissioner's Office (ICO), as a consultant at EY, for a software company developing Privacy Enhancing Technologies, and as a diplomat at the UK's foreign ministry.

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom
Tel: +44 20 7367 3000 / URL: www.cms.law

Holistic AI
18 Soho Square, London, W1D 3QH, United Kingdom
Tel: +44 207 0310822
URL: www.holisticai.com

Emerging Technologies Around the World: Seeking Common Ground

Emma Wright & Harry Wells
Interparliamentary Forum on Emerging Technologies

Introduction

Artificial intelligence (AI) and emerging technologies are transforming our societies. In the last year, public consciousness of AI has been piqued by an increasingly widespread focus on powerful new developments, from ChatGPT and TikTok to worker-tracking technologies, algorithmic bias and, some would argue, the monopolistic behaviour of Big Tech. In order for governments to create frameworks that take advantage of emerging technologies while safeguarding societies against their vulnerabilities and ensuring trust in new systems, legislative bodies must keep pace with this transformation. This must be achieved while also maintaining cooperation, especially in an environment where geopolitical tensions surrounding the threat to national security posed by emerging technologies are increasing. It is against this backdrop that the role of legislators takes on new importance. They must be able to hold governments to account as they draw up specific legislation and encourage the thinking necessary to produce laws that successfully implement legal frameworks that withstand the test of time. One of the central challenges for legislators is to create a framework for a general-purpose technology that affects different industries in different ways. It raises a similar challenge to that posed by electricity in its founding years. However, as with electricity, while we might not understand all the applications, it is clear there are serious health and safety concerns that will undermine public trust if not addressed. Furthermore, legislators must balance this against over-regulating an immature market, which may stifle or stop innovation.

In facing up to these key challenges, international cooperation can help legislators to achieve much more than they would alone. It is in this environment where the Interparliamentary Forum on Emerging Technologies (IFET) sits as a global non-profit organisation working with legislators across the world to facilitate international communication and cooperation on the regulation of AI and emerging technologies. Established in 2019, the IFET is uniquely placed due to a growing network of legislators committed to this aim across over 25 countries globally. Case studies from IFET's programme of roundtable discussions with our legislator network illustrate the extent to which international dialogue can expedite progress and contribute to finding global standards on health and safety aspects that can be agreed on a multilateral level. We facilitate collaboration, and through this aim to provide legislators with the tools to hold governments accountable and push them to tackle the challenges that the rapid development of emerging technologies poses to their ethical implementation and governance.

Overcoming challenges through international dialogue and cooperation

Promoting a global ethical framework

While advances in computing power have seen emerging technologies move at breakneck

pace, many countries are still grappling with the concept of AI legislation. Recent developments in generative AI have demonstrated the importance of a more united, international strategy to combat the risk of algorithms reinforcing and entrenching existing prejudices. In basing generative AI text on enormous swathes of publicly available, global data, unregulated AI learns to replicate and, at times, amplify the human biases it encounters, thereby implicitly producing text that reflects society's ills.[1] Research reveals more broadly the wide variety of practical applications of algorithmic bias in AI and emerging technologies. In the criminal justice system, sentences for prisoners have been extended based on technologies using racially biased algorithms, which overestimate the rate at which black prisoners will reoffend.[2] Similarly, in recruitment, CVs have been downgraded by sexist technologies if they contain the word "women's". Indeed, a recent experiment with a machine-learning algorithm saw robots become overtly racist and sexist.[3] As the amount of data that organisations collect on individuals globally increases with the Global North creating more online footprints than the Global South, the risk of AI and emerging technologies widely amplifying existing prejudices is therefore intensified. Developments in facial recognition have also served to highlight where AI and ethics intersect, with some public authorities using it to conduct mass-surveillance on citizens. Equally, leaving control of these technologies in the hands of relatively few large private organisations gives them enormous power and creates an imbalance with public authorities attempting to avert risks. Eighty per cent of global private investment in AI between 2012 and 2013, for example, came from the United States and China.[4] With Big Tech dominating much global data collection, search engines and social media can filter content and become the centre of misinformation controversies, exerting huge power over what information citizens can access.[5]

For legislators to be able to address these issues, they must both be aware of these risks and possess a framework through which to analyse and assess ongoing legislative development. A major challenge lies not just in the broad-based nature of AI applications, but in the fact that it can often be difficult to identify the harms caused by these technologies. Many of those subjected to facial recognition technology are unaware that their data is being collected and so do not speak out against privacy issues.[6] The women rejected for a job would be unaware that it was a potentially sexist algorithm that made the decision, and so would not know to raise it publicly with legislators. Research also suggests that at a societal level, Western interpretations of AI particularly tend to focus on its extremes, such as its dystopian or even existentially threatening potential, without looking at the reality in the present.[7] The process of legislative scrutiny and activity, then, begins with a greater awareness of the ubiquity of AI and emerging technologies, alongside an ethical framework through which to analyse legislative proposals.

International cooperation can help promote awareness and provide important tools for legislators to better understand the purpose of AI and emerging technologies regulation. This was apparent at IFET's roundtable discussion on the United Nations Educational, Scientific and Cultural Organization's (UNESCO) work to promote a global agreement on the ethics of AI. The existence of different legislating cultures with regards to AI is clear. Where China utilises technologies for mass-surveillance and control, the EU's approach attempts to use regulation to protect fundamental rights and minimise social disruption, while the US focuses on maintaining its global competitiveness and not hampering innovation.[8] Amid disagreement on detail, however, there is an opportunity to find global standards that can be applied across different legislative outlooks. The session allowed legislators to discuss, in the context of UNESCO's Recommendation on the Ethics of Artificial Intelligence, what

that should look like. Legislators raised the issue of algorithmic bias and how best to combat this with an ethical framework. The use of ethical impact assessments was discussed, where the benefits, concerns and risks of AI systems are examined alongside risk prevention, mitigation and monitoring measures. This would allow governments in different legislating environments to set out procedures by which appropriate oversight and assessment of technologies can be made, including the use of algorithmic audit, to predict and mitigate the potential risks of using AI. In this desire for legislation to protect human rights and fundamental freedoms, some also raised the issue of how to legislate for machine learning technologies where their full application is unknown, and consequences can be unintended.

Preparing for specific legislative action

Although 193 Member States have signed up to the ethical guidelines set out by UNESCO, this number is not matched by countries whose governments have enacted significant, targeted legislation. Positively, research by Oxford Insights shows that most national AI strategies announced or published in 2022 were by middle-income countries, catching up with their high-income counterparts that had already taken this step.[9] However, it also illustrates the absence of low-income nations from the AI regulatory environment.[10] For these countries to utilise AI in combating issues like water shortages and health outcomes they must be included in AI governance conversations, and laws enacted elsewhere can provide a roadmap for legislative development. In the UK, an AI regulation white paper is due in May 2023. In the US, congressional representatives have called for a more hands on approach, while lamenting the unpreparedness of lawmakers to deal with rapid accelerations in AI capability.[11] Under the Biden administration, the US has demonstrated a more proactive approach, exemplified by the signing of an executive order that aims to promote racial equity within the federal government. This order directs agencies to address algorithmic discrimination, indicating the administration's commitment to combatting biases that may be embedded in technology.[12] Preparing legislators to develop regulation in their own countries accordingly necessitates analysing and critiquing existing legislative action. The EU AI Act, scheduled to be voted on this year, will be a significant law that will have ramifications for AI regulation far beyond its borders, and has the potential to have a global impact on the direction of regulation.

In this context, international dialogue provided a valuable method for legislators to discuss the content and effect of legislation during IFET's joint roundtable with the Ditchley Foundation, titled 'The Global Implications of the EU's AI Act'. Alongside IFET directors, James Arroyo OBE, director of the Ditchley Foundation, hosted the hybrid event at Ditchley Park where Professor Lilian Edwards of the Ada Lovelace Institute and Maciej Kuziemski of the Ditchley Foundation also gave speeches. These expert presentations focused on both the content of the proposed law and what it means for regulation in other parts of the world. Professor Lilian Edwards posited that shifts in international attitudes to regulation make it likely for the EU's AI Act to become an acceptable global model of governance that others will look to for their own law-making. The panel discussed the Act's risk-based approach with a focus on regulating 'high risk' AI, and the obligations it places on providers of AI systems and their 'users', such as businesses that utilise recruitment technologies or local authorities that use fraud detection systems. Several legislators requested details on the Act's approach to technologies like facial recognition, and the panel were able to explain that real-time biometric identification in publicly accessible places was prohibited, but that negotiations were ongoing as to whether this would apply to retrospective and private use. Asking more about what was deemed 'high risk' and the level of regulation that technology in this category would be under, the panel were able to explain this to legislators from four different continents. Including critical infrastructure, education,

employment, law enforcement, and border management, the use of AI in these areas will be subject to a detailed certification regime.[13] Legislators were able to hear that the regime will include measures like human oversight, quality of data sets, and transparency, and should be embedded in the design of the 'high risk' AI system. Ultimately, the roundtable was able to move beyond frameworks and directly evaluate specific legislation that has the potential to shape global governance of AI and emerging technologies. In doing so, legislators were able to discuss how best to practically embed principles into their own legislative frameworks, as well as being able to exchange information on how the EU's AI Act interacts with proposed regulation in their own corners of the world.

Comparing international standards

Geopolitical dynamics can also act as a barrier to strong governance of AI and emerging technologies. As countries focus on using technologies to further their own aims, regulation can become subordinated to national goals. For example, the AI 'arms race' is often noted as an important factor in AI regulation, as nations seek to become the pre-eminent technology power and take advantage of the influence this provides. Alongside this is the rapidly growing importance of security of energy and natural resources, such as silicon and lithium, and technology supply chains. The various semiconductor legislation passed in the EU, China and the US respectively aims to promote digital sovereignty and focus on domestic production.[14] As chip quality becomes increasingly advanced, countries focus on protecting the vast developments in AI that occur alongside, and end goals diverge. Technologies like TikTok have also become the site of geopolitical contest between the US and China, stimulating a wider public debate about privacy, how our data should be controlled and by whom.[15] On a less overt level, each nation will pursue subtly different goals with regards to its approach to AI and may find that such goals conflict with those of other states. Yet, AI and emerging technologies do not operate within borders and can often be accessed remotely. If we are to create an international environment of strong governance for these new technologies that protects fundamental rights, cooperation between nations is still vital to share developments and promote global standards.

It was in this spirit that IFET brought together legislators from across four continents to discuss how democracies around the world are dealing with harmful content circulating online, and how to balance protections for freedom of speech while reducing the extent of online harms. Expert presentations gave legislators an overview of how the UK, EU, Ireland, Australia, Canada and Germany are approaching online safety legislation. It was put to legislators that regulatory initiatives are often a mix of two or more different approaches: systems; and content takedown. The UK's Online Safety Bill and the EU's Digital Services Act are the most notable to take a systems approach and are much less prescriptive than other laws. On the other hand, first amendment concerns mean the US is not pursuing a content agenda and is focused on data transparency and algorithmic processes. Legislators discussed how best to protect young people online, their experience of dealing with technology companies, and the unique problems posed by the proliferation of deep fakes. On the latter, it was explained that tech companies can deploy robust measures to screen for these images, and examples of businesses that employ this technology to prevent harm to its, often female, users were given. It was noted that many companies lack transparency about their data and algorithms, so it is difficult for lawmakers to ask the right questions or know exactly what needs to be regulated. Legislators were given guidance as to who publishes information for legislators on this precise problem. Connecting legislators with expert bodies, which IFET will also do in an upcoming roundtable with the International Telecommunication Union, also fosters stronger relationships with international organisations that can help facilitate the development

of international standards. In this case, exchanging best practices and directing legislators to sources of expertise brought attention to the importance of viewing AI as a concept that should be addressed internationally, if its benefits are to be utilised and fundamental rights protected.

Hope for the future

The opportunities for AI – and emerging technologies more widely – to solve some of society's most critical issues, from transforming healthcare and education to addressing climate change and improving national security, are endless. While previous years have seen much public discussion about how new technologies exist in the abstract, recent developments have demonstrated that breakthroughs in use and public consciousness are occurring now. Although this rapid development poses challenges to their ethical implementation, legislators can, through international collaboration and dialogue, address key challenges and play a crucial role in how the world will approach AI for decades to come. Multinational organisations can provide a crucial forum for this, and IFET will continue to introduce legislators to bodies like the ITU and UN. Moreover, IFET will collaborate directly with UNESCO to highlight their global agreement on AI ethics and, in addition, work on tools for implementing solutions to the various ethical issues raised by the deployment and subsequent use of artificial systems. International cooperation provides the crucial opportunity to find global standards, and through discussion, comparison and analysis, legislators can find innovative solutions and ensure countries take advantage of the unique strengths of these new technologies within a framework that limits harms and promotes long-term trust.

* * *

Endnotes

1. Vock, I., 2022. "ChatGPT proves that AI still has a racism problem", *New Statesman Online*, available at https://www.newstatesman.com/quickfire/2022/12/chatgpt-shows-ai-racism-problem [last accessed 13/03/2023].
2. O'Neil, C., 2016. *Weapons of Math Destruction*, New York: Crown.
3. Hundt, A., Agnew., Zeng V., Kacianka, S. and Gombolay, M. 2022. "Robots Enact Malignant Stereotypes". In *2022 ACM Conference on Fairness, Accountability, and Transparency* (FAccT '22). Association for Computing Machinery, New York, NY, USA, 743–756, available at https://doi.org/10.1145/3531146.3533138 [last accessed 13/03/2023].
4. Ramos, G. and Mazzucato, M., "AI in the Common Interest", *Project Syndicate*, available at https://www.project-syndicate.org/commentary/ethical-ai-requires-state-regulatory-frameworks-capacity-building-by-gabriela-ramos-and-mariana-mazzucato-2022-12 [last accessed 13/03/2023].
5. Noble, S.U., 2018. *Algorithms of oppression: how search engines reinforce racism*, New York: New York University Press.
6. Big Brother Watch. 2020. "Big Brother Watch Briefing on facial recognition surveillance" Big Brother Watch, available at https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf [last accessed 13 March 2023].
7. Cave, S. and Dihal, K., 2019. "Hopes and fears for intelligent machines in fiction and reality". *Nature machine intelligence*, 1(2).

8. Roberts, H. and Luciano, F., 15/11/21, "The EU and the US: two different approaches to AI governance", *Oxford Internet Institute*, available at https://www.oii.ox.ac.uk/news-events/news/the-eu-and-the-us-two-different-approaches-to-ai-governance/ [last accessed 13/03/2023].
9. Oxford Insights. 2022, "Government AI Readiness Index 2022", [pdf] *London: Oxford Insights*, available at https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf [last accessed 13/03/2023].
10. *Ibid*.
11. Representative Ted Lieu, 2022, "I'm a Congressman Who Codes. A.I. Freaks Me Out", *The New York Times*, available at https://www.nytimes.com/2023/01/23/opinion/ted-lieu-ai-chatgpt-congress.html [last accessed 13/03/2023].
12. "Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through The Federal Government", 2023, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/ [last accessed 13/03/2023].
13. Edwards, L., 2022. "The EU AI Act: a summary of its significance and scope", *Ada Lovelace Institute* [pdf], available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf [last accessed 13/03/2023].
14. Larsen, B., 2022. "The geopolitics of AI and the rise of digital sovereignty", *Brookings* [online], available at https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/ [last accessed 13/03/2023].
15. Gray, J. E., 2021. "The geopolitics of 'platforms': the TikTok challenge", *Internet Policy Review*, 10(2). https://policyreview.info/articles/analysis/geopolitics-platforms-tiktok-challenge [last accessed 13/3/2023].

Emma Wright
Tel: +44 20 7667 5000 / Email: emma.wright@harbottle.com

Emma Wright is a telecoms and technology lawyer and the lead partner for the tech, data and digital practice within a renowned international law firm. She has frequently been noted as one of the UK's leading women in technology and has spoken internationally on global trends in AI regulation. She is Director of the Interparliamentary Forum on Emerging Technologies' operating company and acts as IFET's legal counsel. She has been appointed to the UNESCO Women4EthicalAI Platform – a network of senior women globally expert in AI.

Harry Wells
Tel: +44 7733 026 478 / Email: harry.wells@parliament.uk

Harry Wells is a researcher for IFET and is responsible for organising roundtable events and generating the content for such events. He has experience working in a variety of roles for MPs in Parliament and has worked as a legal intern for technology start-ups. He is currently a postgraduate law student in London.

Interparliamentary Forum on Emerging Technologies

C/O Darren Jones MP, House of Commons, London, SW1A 0AA, United Kingdom
URL: www.ifemergingtech.com

Australia

Jordan Cox & Bryce Siu
Webb Henderson

Trends

Artificial intelligence (**AI**), big data and machine learning offer significant opportunities in business and our personal lives, reshaping much of our world. Public interest in AI is being fuelled by the advent of large language models like ChatGPT, Microsoft's new Bing and Google's Bard. ChatGPT alone has grown its user base to over 100 million since its launch in November 2022.[1] These AI tools are lauded for their ability to generate human-like responses to a wide range of technical and creative queries. While these tools offer tangible benefits to business, businesses are also grappling with the ethical, accountability, transparency and liability implications emerging from its use.[2] These issues are compounded by the speed of innovation with these tools, demonstrated by the recent launch of GPT-4, which OpenAI touts as its most advanced system while being more creative, safe and secure than its predecessor.[3]

Businesses are recognising the importance of investing in emerging technologies for their long-term sustainability. It is therefore no surprise that AI is estimated to contribute more than $20 trillion to the global economy by 2030.[4] In 2021, the former Federal Government released its first AI Action Plan to help boost the development and adoption of AI, pledging to invest $124.1 million "*to establish Australia as a global leader in developing and adopting trusted, secure and responsible AI*".[5] A National AI Centre was established as part of the AI Action Plan in partnership with the Committee for Economic Development of Australia (**CEDA**) and Google.[6]

Recently, the National AI Centre established the Responsible Artificial Intelligence Network, a cross-system program to support Australian companies in using and creating AI in accordance with ethical and safety standards.[7] The program is expected to assist Australian industries in the use of responsible AI, and has attracted initial knowledge partners including the Australian Industry Group, Australian Information Industry Association, CEDA, Data61 (the data science research team of the Australian Government research agency, the CSIRO), Standards Australia, the Ethics Centre, the Gradient Institute, the Human Technology Institute and the Tech Council of Australia.[8]

Alongside this initiative, the National AI Centre published a report "*Australia's AI ecosystem momentum*",[9] which evaluates the current state of AI adoption and innovation in Australia. The report comprises 200 respondents and four qualitative interviews targeting IT and business decision-makers.[10] This report indicates that Australian businesses have matured their understanding of AI, with 60% of respondents stating that they are accelerating and expanding their AI-related solution offerings to meet market demand. While many businesses engage AI technology and service providers to assist with projects, with an average of four AI partners per AI project, many businesses are also developing in-house capabilities in the areas of AI strategy, data analysis and AI operations.[11]

Reviews of the regulatory and legal framework for AI in Australia have been launched to ensure Australia's regulations, laws and regulatory systems remain fit for purpose. A key example is the Federal Government's Digital Technology Taskforce's inquiry into automated decision making (**ADM**) and AI regulation, which closed its consultation process in May 2022,[12] with a discussion paper to be released as the next step.

A key challenge for Australia is upskilling the Australian workforce to unlock the full benefits of AI.[13] The Government invested $1 billion in skills through the JobTrainer Fund and Digital Skills Organisation in 2022 as part of its Digital Economy Strategy.[14] Data61 estimates that by 2030 the Australian industry will require up to 161,000 new specialist workers in AI, big data and machine learning.[15] AI and big data are being used broadly among Australian businesses, but certain industries are paving the way – these include the logistics, utilities, construction, food and beverage, emergency, human resources, clean energy, recycling, environment, healthcare, farming and mining industries.[16] Automated systems and AI are increasingly being used in the growing e-commerce industry to address fraud, product safety and other consumer protections issues,[17] for example, Amazon Australia claims to have prevented over six million attempts by bad actors to create new selling accounts in 2020.[18] AI is also being used in the healthcare sector to improve supply chain efficiencies, convert electronic health records to usable data and forecast demands at hospitals.[19] AI has also played a role in diagnoses. For example, Fujitsu Australia, GE Healthcare, Macquarie University and Radian Network are developing an AI solution to quickly and efficiently detect and monitor brain aneurysms on scans.[20]

Australia does not have specific laws regulating AI, big data or ADM at this time. However, a range of other laws may indirectly shape the adoption and implementation of these emerging technologies, including those relating to privacy and data security, corporate law (e.g., corporate governance and risk management responsibilities), financial services regulations, intellectual property laws, competition law and anti-discrimination laws.

Case law can also be relevant. For example, the Federal Government in 2016 ran a widely criticised "Robodebt" programme, which used an automated debt recovery programme that averaged incomes to infer individuals who may have under-reported their income when receiving a welfare benefit.[21] These individuals were sent a notice identifying a debt payable by them based on algorithmic inference. Recipients of these demands then had to displace the algorithmic assumptions through administrative processes, which effectively shifted the burden to the individual to prove that they had not been overpaid welfare benefits. The Federal Court of Australia ruled that this programme was unlawful on the basis that the decision maker could not have been satisfied that the debt was owed.[22] Following this decision, the Albanese Government established a royal commission (an independent investigation) to examine the establishment of the scheme and recommend measures to prevent such a scheme from happening again.[23] The Commissioner overseeing the inquiry is expected to provide a report of the results by June 2023.[24]

Ownership/protection

There is no *sui generis* ownership right for an AI or other algorithm. To the extent the AI algorithm is implemented in software, the software will be protected as an "original literary work" under the *Copyright Act 1968* (Cth) (**Copyright Act**).[25] If a company's employee creates the software in the course of their employment, the Copyright Act deems the company as the author and owner of the rights in that creation.[26] However, this position is different if the company engages a third party to develop the software. Outside of an employment relationship, copyright can only be assigned in writing.[27] Therefore, in the

absence of a written agreement between the third party and the company, the third party will be the owner of the AI algorithm.

Intellectual property rights (**IPRs**) may also arise in the form of business method patents (which can be granted where a manner of manufacture brings about a useful product in a new and inventive way) and trade secrets (which arise naturally and are not registered). In 2021, the Federal Court of Australia ruled that an AI machine can be an "inventor" under Australian patent laws.[28] However, this decision was appealed by the Commissioner of Patents in 2022, and on appeal, the full Federal Court unanimously held that an "inventor" must be a natural person, shutting down the concept of AI-led patent applications in Australia for now.[29]

It is less clear if the output of the AI application, being the improvement of the application through learning and the output itself, would attract the same IPRs and protections as the AI software itself. The uncertainty arises because there is no human author required in the process of creating the output. The requirement for human authorship was considered by the Federal Court of Appeal (**FCA**) in *Telstra Corp Ltd v Phone Directories Co Pty Ltd* [2010] FCA 44.[30] In agreement with the trial judge, the FCA held that copyright did not subsist in Telstra's phone directories, as the extraction process used to produce the directories was largely computerised.[31] This suggests that output from AI applications is generally unlikely to be protected by IPRs in the absence of any human authorship (for example, in how the data is organised and presented).

In Australia, there is no general copyright in data itself, but copyright will subsist in the arrangement or structure of the data where it is created by independent intellectual effort or through the exercise of sufficient efforts of a literary nature.[32]

Given that Australian law does not recognise IPRs subsisting in data, companies will need to use commercial agreements to clarify their rights and the agreed positions on how each party with access to the data may use it, and to what extent. These agreements should clearly state which party is to control the use and exploitation of modifications, enhancements and improvements of the AI application and the actual AI output, such as data or information. It may also be beneficial, if appropriate in the context, to clarify limitations on uses of the data inputs that are used to train the AI application. More broadly, commercial agreements containing appropriate confidentiality and intellectual property clauses are necessary to protect technology and data assets in a range of contexts (for example, where a company licenses these assets to a third party on a limited basis as part of the provision of a service).

With respect to data protection, it is critical that businesses have robust data security measures, particularly as nefarious actors seek to take advantage of the vulnerabilities arising from the COVID-19 pandemic and remote working. This impact has been observed in Australia by the Australian Cyber Security Centre, which reported that it received nearly 450 ransomware cybercrime reports in 2021–22, with the report acknowledging that the actual figure may be far higher due to underreporting.[33]

The scale of some recent large data breaches has prompted amendments to the maximum penalties for serious privacy breaches under the *Privacy Act 1988* (Cth) (**Privacy Act**), which was passed by each of the Houses in November 2022.[34] These amendments increased the maximum penalty for companies from $2.22 million to the greater of:

- $50 million;
- three times the value of any benefit obtained through the misuse of information (if quantifiable); or
- 30% of a company's adjusted turnover in the relevant period (if the court cannot determine the value of the benefit obtained).

The maximum penalty applicable to individuals was increased from $444,000 to $2.5 million. The amendments also provide the Office of the Australian Information Commissioner (**OAIC**) and Australian Communications and Media Authority (**ACMA**) with greater regulatory powers and the ability to quickly share information about data breaches with other enforcement bodies.[35]

Australian businesses typically have, and will require service providers to have, a range of information security management and data security standards at their disposal. For example, ISO/IEC 27001 (Information Security Management), while not mandatory, is a widely recognised industry standard.[36] In addition, the Australian Signals Directorate, the government agency responsible for information security and cyber warfare, has developed an "Essential Eight" set of mitigation strategies which sets out specific minimum technology controls to assist businesses to protect their data security.[37] Also, the Australian Cyber Security Centre publishes the Australian Government Information Security Manual, which outlines a cyber security framework that organisations can apply.[38]

Further, it is common for supply contracts in Australia to contain requirements for suppliers to implement minimum standards for privacy and data security, particularly if either party is likely to disclose personal or commercially sensitive information to the other party in the course of their commercial arrangement, or if sensitive personal information is likely to be disclosed.

There are no specific data ownership laws in Australia but there are a range of laws that apply to data security and information privacy. The Privacy Act applies to "personal information", which is defined to be "*information or an opinion about an identified individual, or an individual who is reasonably identifiable*"[39] – this is generally a narrower set of information than comparable concepts like "personal data" as defined in Europe's General Data Protection Regulation (**GDPR**). The Privacy Act, including the Australian Privacy Principles,[40] establishes a framework for the collection, use and disclosure of personal information.

Recently, the Attorney-General's Department released its Privacy Act Review Report 2022, which represents the culmination of a two-year consultation and review process of the Privacy Act. It contains 116 proposals that, if passed, would significantly overhaul the Privacy Act.[41] Relevantly, the report raises concerns about the transparency and integrity of decisions being made using ADM. Due to the increasing use of ADM across government and the private sector, the report introduces three proposals to enhance individuals' confidence in taking up ADM:[42]

- The first proposal, in its current form, would require organisations that utilise ADM to set out in their privacy policies the types of personal information that will be used in substantially automated decisions which have a legal, or similarly significant, effect on an individual's rights.[43]
- The second proposal is to develop OAIC guidance on the types of decisions that would be considered to have a legal or similarly significant effect on an individual's rights.[44]
- The third proposal would introduce a right for individuals to request meaningful information about how substantially automated decisions are made.[45]

Following a consultation process ending in March 2023, the Government is expected to publish draft legislation as early as the second half of 2023.

In the telecommunications sector, Part 13 of the *Telecommunications Act 1997* (Cth) (**Telco Act**) sets out strict rules for entities involved in the telecommunications supply chain when using and disclosing telecommunications information (i.e. the contents or substance of a communication passing over telecommunications networks; telecommunications service information and personal particulars about a person).[46]

The *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) contains a number of provisions dealing with information privacy. The primary objective of the TIA Act is to protect the privacy of individuals using Australia's telecommunications system and to create a framework for lawful access to telecommunications data by law enforcement agencies.[47] It prohibits the interception of communications passing over a telecommunications system and prohibits access to stored communications (e.g., emails and SMS).[48] The TIA Act then creates a regime for lawful interception for national security or law enforcement purposes.[49] In 2015, the TIA Act was amended to include a data retention scheme. Under this scheme, telecommunications providers are required to collect and retain specific types of metadata, known as retained data, for a minimum of two years.[50]

The Federal Government is also increasingly concerned with protecting assets that are critical to the functioning of Australia's economy, society and national security. On 2 December 2021, Parliament passed the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) (**SOCI Act**). The SOCI Act introduced a range of security obligations on owners and operators of critical infrastructure and systems of national significance across 11 sectors, including communications, data storage or processing, banking and finance and space technology. This includes a requirement to notify the Australian Government of cyber security incidents, as well as a step-in right under which the Minister may direct an owner or operator to take action in some circumstances (as part of its "Government assistance measures"). On 30 March 2022, the Parliament passed the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth), the second tranche of the reforms. Responsible entities are required to adopt and maintain a critical infrastructure risk management programme and comply with enhanced cyber security obligations for systems of national significance, which includes vulnerability reporting and cyber incident response planning and exercises.

The Telecommunications Sector Security Reforms, which commenced in 2018,[51] introduced a regulatory framework to manage the national security risks of sabotage and foreign investment to Australia's telecommunications networks and facilities. They create a security obligation for entities involved in the telecommunications supply chain to do their best to protect their networks and facilities from unauthorised access or interference.[52]

The *Data Availability and Transparency Act 2022* (**Data Act**) created a scheme to authorise and regulate access to Australian government data to other government and private sector entities.[53] The Data Act permits data sharing for three purposes: (1) delivery of government services; (2) informing government policy and programmes; and (3) research and development.[54] Under the Data Act, access to Australian government data is controlled and overseen by a new independent regulator, the National Data Commissioner.

On 24 January 2022, the Federal Government proposed to expand the consumer data right (**CDR**) to the telecommunications sector in Australia.[55] At the time of writing, a timeframe for this expansion has not been finalised. The CDR is intended to give consumers greater access to and control over their data, improve consumers' ability to compare and switch providers, and encourage competition between service providers.

Antitrust/competition laws

In 2017, the *Competition and Consumer Act 2010* (Cth) (**CCA**) was amended to (among other things) introduce a prohibition on "concerted practices".[56] Under the new sub-paragraph (1)(c) in section 45 of the CCA, a corporation must not "*engage with one or more persons in a concerted practice that has the purpose, or has or is likely to have the effect, of*

substantially lessening competition".[57] The term "concerted practices" is not defined in the CCA but the competition regulator, the Australian Competition and Consumer Commission (**ACCC**), has commented that it would involve communication or cooperative behaviour between businesses that may not necessarily amount to an understanding between them but extends beyond a business responding to the market.[58]

In the context of AI, an AI algorithm could – in response to other firms or another AI – set prices or otherwise act in a way that mimics price fixing. The complicating factor is that this process could potentially occur without human intervention, however the existing framework requires coordination between the parties. As it presently stands, it is unclear the extent to which the CCA would apply to AI algorithms but the ACCC has considered this issue in detail at a policy level, noting its view that a person cannot avoid liability by saying "*my robot did it*".[59] The specific role of big data in influencing market practices and its potential impact on lessening competition is becoming more apparent. With the emergence of digital markets and their growing use and reliance on big data, the Federal Government in 2019 requested an inquiry into markets for the supply of digital platforms by the ACCC. In its inquiry, the ACCC concluded that Meta and Google held substantial market power in these markets, having acquired large amounts of data over a long period of time that would be difficult to replicate, placing them at a strong advantage.[60]

This issue is also being explored and expanded upon by the ACCC in its separate five-year inquiry (2020–25) into the market of digital platform services, such as search engines, social media platforms, content aggregation services and electronic marketplaces.[61] The ACCC has produced interim reports every six months, with a final report due in March 2025. In November 2022, the ACCC released its fifth interim report in the series, focusing on competition and consumer issues arising from the increasing market concentration and expansion of digital platforms and proposals in response. The ACCC concluded that existing competition laws are not likely to provide adequate or timely protection and promotion of competition in digital platform markets, and that digital platforms have engaged in, or have incentives to engage in, various forms of anti-competitive conduct. This includes self-preferencing (particularly in the app market), tying and bundling (such as app stores requiring the use of their in-app payment systems), exclusive pre-installation and default agreements that prevent switching and multi-homing, and creating barriers to entry and expansion by restricting third-party access to user data and denying interoperability. The solution, the ACCC considered, is targeted, upfront (*ex ante*) regulation, involving mandatory, service-specific codes of conduct. These codes would apply to 'designated' digital platforms only.

The report also discusses the possibility of anti-competitive acquisitions by digital platforms, with the ACCC stating that acquisitions by such large digital platforms should be subject to a higher level of scrutiny, considering their market dominance. The ACCC considered that acquisitions of entities in emerging areas, such as AI and virtual reality, may enable digital platforms to position themselves in a manner "*to control new and emerging technology… where this enables dominant platforms to expand their ecosystems and erect barriers to entry or otherwise control access to key inputs (such as data) required for effective competition in services across those ecosystems*".

Under the *Treasury Laws Amendment (New Media and Digital Platforms Mandatory Bargaining Code) Act 2021* (Cth) (**Media Bargaining Code**), the Federal Government can now make designated digital platforms negotiate with news outlets to pay for news content. While no digital platforms have been designated to date, the threat of government intervention is considered to have played a role in Meta and Google electing to negotiate

with news businesses and strike over 30 commercial agreements that reportedly would not have been made without the Media Bargaining Code.[62]

Board of directors/governance

Companies must ensure that their corporate governance programme sufficiently addresses the risks associated with implementing or adopting AI and big data strategies and technology, including by addressing these risks in their policies and processes. The *Corporations Act 2001* (Cth) (**Corps Act**) establishes a general obligation on directors to effectively manage risks. Some entities (e.g., financial services providers) may also be subject to additional risk management obligations in respect of the services they provide.[63] As a general principle, a board cannot derogate their responsibility for oversight of a company's decisions, and there is no reason to conclude that this would be different where decision making has involved an AI.

Boards should regularly review their governance framework and consider what changes might be needed to address and manage the risks associated with using AI and big data. In doing so, one (non-Australia specific) resource is the World Economic Forum's toolkit for company directors called Empowering AI Leadership (An Oversight Toolkit for Boards of Directors).[64] While it is non-Australia specific, the Australian Institute of Company Directors (**AICD**) contributed to the creation of the toolkit and provided input from an Australian perspective. This toolkit includes 12 learning modules aimed at helping companies make informed decisions about AI solutions.[65] The AICD also provides informal guidance to directors.[66]

Publicly listed companies are required under section 674 of the Corps Act and the Australian Stock Exchange (**ASX**) rules to satisfy continuous disclosure obligations.[67] The rules require a publicly listed entity to disclose information that a reasonable person would expect to have a material impact on the price or value of the company.[68] This disclosure obligation could arise in the context of AI and big data. For example, if a company owns and operates an AI solution that is a significant asset, or introduces significant risk, it could be required to disclose a potential sale of that asset to its shareholders via the ASX.

With respect to vendor communication, it is important that vendors are properly informed of any compliance risks and programmes for any AI used within a customer's organisation. In addition, companies will need to manage supply-chain security risks associated with using particular vendors and their technologies.[69]

Civil liability

The question of liability is particularly difficult when it comes to AI technology. This is mainly because Australia's civil liability regime does not specifically contemplate or address damage or harm resulting from the use of an AI technology. To the extent the adoption or use of AI technology causes damage, redress for victims could potentially be addressed contractually, through existing consumer protection laws or through the laws of negligence (although, the application of this is unclear).

Given the uncertainty about the application of the law of negligence to AI technology, parties can allocate liability contractually. Contracts should clearly state who is responsible for any harm or damage that results from using AI. Ideally, the contract should address the following matters:

- who is responsible if the data inputs are incorrect, misleading or result in an adverse outcome (i.e., data quality issue);
- who is responsible if the AI application fails to properly process the data, resulting in an adverse outcome;
- who is responsible for interpreting the AI outputs;

- what is the specified purpose for using the AI output; and
- who is responsible for training the AI and ensuring its continuous improvement.

Addressing these matters contractually may be difficult where the data or AI application are provided or developed by several parties. Due to the limitations of addressing these issues contractually, other measures should also be considered to ensure that the AI performs as intended. Often, these are outside the four corners of a contract and concern issues such as the design of the AI and how the parties will ensure data integrity and data security.

With respect to decision-making, the Australian Human Rights Commission (**AHRC**) recommends that there should be a rebuttable presumption that legal liability for any harm that may arise from an AI-informed decision should primarily lie with the legal person responsible for making the decision itself.[70] However, the AHRC appreciates that complexities can arise, including where an AI system operates autonomously or multiple parties are involved in developing and using the system.[71]

In the medical context, the question of causation, what constitutes reasonable steps, and the accepted standard of care, may be difficult to establish when an AI tool is involved in the relevant harm or damage. For example, if a doctor uses an AI medical tool that is commonly accepted in the industry as accurate, would the doctor be liable if the use of that tool on a particular patient results in an adverse outcome? Conversely, where the AI tool recommends a particular treatment model, but the doctor exercises judgment to take a different approach, is that doctor more exposed to liability than if they had followed the AI recommendation? These are very much live issues, which we expect to see clarified in time; however, we expect courts would likely seek to apply existing jurisprudence to the extent possible – for example, consistent with current approaches to allocating liability between the primary caregiver and the manufacturer of a faulty product.

Criminal issues

At the time of writing, these issues remain largely untested in Australian courts and we are not aware of any proposed laws seeking to directly address these issues.

Discrimination and bias

Australian law prohibits discrimination based on protected attributes, and anti-discrimination laws could in theory apply where decision making using AI results in unlawful discrimination.[72] This concern has been raised and discussed by independent statutory authority, the AHRC in its detailed Human Rights and Technology Final Report (**Report**) released and tabled in the Australian Parliament in 2021, a culmination of a three-year project.[73] The Report covers four main topics: (1) a national strategy on emerging technologies; (2) the growing use of AI in decision making by government and the private sector "*with significant implications for how human rights are fulfilled*"; (3) establishing an AI Safety Commissioner to support effective regulation; and (4) accessible technology for people with disabilities.[74] The AHRC goes on to make 38 pertinent recommendations.[75] Further, in December 2022, the AHRC published a Guidance Resource, which provides guidance on complying with federal anti-discrimination legislation in relation to the use of AI in insurance and underwriting decisions.[76] The Guidance Resource provides six tips to avoid unlawful discrimination when using AI.

Regulations/government intervention

There are no specific AI, big data or machine learning laws or regulations in Australia to date. The Federal Government's Digital Technology Taskforce's release in March 2022

of an issues paper, *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation*[77] invited businesses, AI experts, academics and researchers, and the public to comment on the current regulatory barriers to AI, whether there is a need for new regulation or guidance and what international frameworks Australia should consider adopting.[78] The Taskforce has not yet issued a subsequent discussion paper, as the Taskforce's function has transferred from the Department of the Prime Minister and Cabinet to the Department of Industry, Science and Resources on 1 July 2022 (with the change of Government).

In March 2022, the New South Wales government published its *NSW Artificial Intelligence Assurance Framework* in an effort to assist government departments using AI to comprehensively analyse and document their AI-specific risks.[79] The framework introduces an AI assurance self-assessment and a review process through the establishment of an AI review body.

Currently, the use and adoption of AI, big data and machine learning by businesses is subject to existing laws that apply, in varying degrees, to such technologies as discussed above. Privacy, anti-discrimination and competition law, for example, are topics that are regularly discussed in the context of emerging technologies.

The potential for AI technologies to be misused has been widely acknowledged both in Australia as well as globally. In Australia, the AHRC has expressed concerns regarding the potential for AI to threaten human rights, stating "*our challenge as a nation is to ensure these technologies deliver what Australians need and want, rather than what they fear*".[80] The AHRC explains that adopting the right governance framework is difficult given the complex nature and varied use-cases of these technologies,[81] and suggests that the focus shift to the outcomes of AI, rather than regulating AI itself, when it comes to decision making (although significantly risky uses of AI could be directly regulated).[82] To realise the benefits of AI, the AHRC recommends "*carefully crafted laws supported by an effective regulatory framework, strong incentives that apply to the public and private sectors, and policies that enable Australians to navigate an emerging AI-powered world*".[83]

Despite being voluntary, tools such as the AI Ethics Framework developed by the Department of Industry, Science, Energy and Resources and the OECD/G20 AI Principles adopted in May 2019, are important resources to promote responsible use of AI technologies – seeking to encourage organisations using AI to aim for the best outcomes for Australians when designing, developing, integrating, or using AI technologies.[84] With regard to the development of the AI standards, the OAIC recommends that the standards must draw on domestic and international privacy and related frameworks to ensure alignment[85] – suggesting that Australia's response, particularly in relation to privacy, will be informed by international approaches. In July 2021, the Regulator Performance Guide came into effect, which outlines the Government's expectations for regulator performance and reporting.[86] A key best practice principle includes encouraging regulators to "*manage risks proportionately and maintain essential safeguards while minimising regulatory burden, and leveraging data and digital technology to support those they regulate to comply and grow*".[87]

National security and military

In 2021, the Government identified a list of 63 critical technologies that have implications for defence and security, which include AI algorithms and hardware accelerators, machine learning and natural language processing.[88] The Government went on in 2022 to hold a public consultation to provide an opportunity to give feedback on the list, including feedback

on which technologies should be retained or removed.[89] The Critical Technologies Hub is working with the Minister to refine and publish the updated List.[90] The national security laws relating to AI, big data and machine learning focus on managing the risks associated with foreign investment in these assets.

From 1 January 2021, changes to the F*oreign Acquisitions and Takeovers Regulation 2015* (Cth) and the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (collectively, the **FATA**) took effect in Australia. The FATA implemented significant reforms to Australia's foreign investment framework by (among other things) introducing a zero-dollar screening threshold, meaning that any direct investment by a foreign entity in a "national security business" requires government approval.[91] A national security business is defined in the regulations to include businesses operating in the communications, technology and data sectors.[92]

The use of AI in the military domain is actively being discussed by Australia's Department of Defence (**Defence**). A key concern for Defence is ensuring ethical use of AI to avoid any adverse outcomes, with Defence commenting that "*premature adoption without sufficient research and analysis may result in inadvertent harms*".[93] In 2019, Defence held a workshop with various representatives from Defence and other government agencies to explore the ethical use of AI in Defence.[94] One of the outcomes of the workshop was the development of a practical methodology, which included three tools: an Ethical AI for Defence Checklist; Ethical AI Risk Matrix; and a Legal and Ethical Assurance Program.[95] The findings from the workshop were published in Defence's technical report "*A Method for Ethical AI in Defence*" in February 2021.[96]

Of late, the Federal Government has made considerable investment in AI applications for Defence. In September 2022, the Defence Innovation Hub entered into a $4 million contract with Athena AI to develop an automated decision support tool to provide rapid guidance to users when making tactical decisions under pressure.[97] A further $4 million investment in Penten was announced to develop an AI tool for active cyber protection for Defence applications.[98] Defence also announced a $5 million contract with Deakin University to utilise virtual reality, augmented reality and AI technologies to develop an immersive training for naval firefighting.[99] These contracts represent the Defence Innovation Hub's increasing investment portfolio in AI-enabled defence applications.

Lastly, as discussed above, the concerns around foreign investment have been addressed through the FATA and the SOCI Act are intended to address key national security concerns regarding national critical infrastructure.

* * *

Endnotes

1. "The AI chatbots are here, what does this mean for you?", Governance Institute of Australia (Web Page, 15 March 2023).
2. *Ibid*.
3. "GPT-4", OpenAI (Web Page).
4. Digital Technology Taskforce (2022) "Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation", (Issues Paper, 2022).
5. Australian Government (2021) "Australia's AI Action Plan", (Paper, June 2021); Treasury. 2018. Budget Strategy and Outlook 2018/19. Budget Paper #1. Australian Government. Canberra.

6. *Ibid*.
7. "Australia announces world first responsible AI Network to uplift industry", CSIRO (Web Page, 16 March 2023).
8. *Ibid*.
9. "Australia's AI ecosystem momentum report", CSIRO (Web Page, 14 March 2023).
10. *Ibid*.
11. *Ibid*.
12. Digital Technology Taskforce (2022) "Positioning Australia as a Leader in Digital Economy Regulation" (Issues Paper, March 2022).
13. CSIRO, Data61 (2019) "Artificial intelligence: Solving problems, growing the economy and improving our quality of life" (Report, 2019).
14. Digital Technology Taskforce (2022) "Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation" (Issues Paper, 2022).
15. CSIRO, Data61 (2019) "Artificial intelligence: Solving problems, growing the economy and improving our quality of life" (Report, 2019).
16. Digital Technology Taskforce (2022) "Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation" (Issues Paper, 2022).
17. Australian Competition & Consumer Commission (2022) "Digital platform services inquiry Interim report No. 4 – General online retail marketplaces" (Report, 2022).
18. Amazon Commercial Services Pty Ltd (2021) "Amazon Australia submission to Australian Competition and Consumer Commission Digital Platform Services Inquiry" (Issues Paper Response, 2021).
19. "Adopting AI in Healthcare: Why Change", PWC (Report).
20. Digital Technology Taskforce (2022) "Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation" (Issues Paper, 2022).
21. "Class Action Settlement", Services Australia (Web Page).
22. See Shalailah Medhora, "Federal Court Rules Robodebt 'Unlawful' in Significant Court Case", ABC (Web Page, 27 November 2019).
23. "RoboDebt", Royal Commission into the Robodebt Scheme (Web Page).
24. "Amended Letter Patent – Robodebt Royal Commission", Royal Commission into the Robodebt Scheme (Web Page).
25. Copyright Act 1968 (Cth), s 32.
26. *Ibid* s 35.
27. *Ibid* s 196(3).
28. *Thaler v Commissioner of Patents* [2021] FCA 879.
29. *Commissioner of Patents v Thaler* [2022] FCAFC 62.
30. *Telstra Corp Ltd v Phone Directories Co Pty Ltd* [2010] FCA 44.
31. *Ibid.*
32. *IceTV Pty Limited v Nine Network Australia Pty Limited* [2009] HCA 14.
33. Australian Cyber Security Centre (2022) "ACSC Annual Cyber Threat Report – 1 July 2021 to 30 June 2022" (Report, 4 November 2022).
34. Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth).
35. *Ibid*.
36. "ISO/EIC 27001 Information Security Management", ISO (Web Page).
37. "Essential Eight Explained", Australian Signals Directorate (Web Page).

38. "Australian Government Information Security Manual", Australian Cyber Security Centre (2 March 2023).
39. Privacy Act 1988 (Cth), Part 2.
40. *Ibid* Schedule 1.
41. Australian Government Attorney General's Department (2022) "Privacy Act Review" (Report, 2022).
42. *Ibid*.
43. *Ibid*.
44. *Ibid*.
45. *Ibid*.
46. Telecommunications Act 1997 (Cth), Division 3.
47. Australian Department of Home Affairs (2019) "Telecommunications (Interception and Access) Act 1979 Annual Report 2018-19" (Report, 2019).
48. Telecommunications (Interception and Access) Act 1979 (Cth), s 7.
49. *Ibid* pt 2-2.
50. *Ibid* pt 5-1A.
51. "Telecommunications Sector Security Reforms", Department of Home Affairs (Web Page).
52. *Ibid*.
53. Data Availability and Transparency Bill Act 2022 (Cth).
54. Ibid s 15.
55. Australian Government Treasury (2022) "Competition and Consumer (Consumer Data Right) Rules 2020 with proposed amendments" (Exposure Draft, 2022).
56. Competition and Consumer Act 2010 (Cth), s 45(1)(c).
57. *Ibid*.
58. "Anti-competitive Conduct", ACCC (Web Page).
59. "The ACCC's approach to colluding robots", ACCC (Web Page).
60. Australian Competition & Consumer Commission (2019) "Digital Platforms Inquiry" (Report, June 2019), pages 8–9.
61. "Digital platform services inquiry 2020–25", ACCC (Web Page).
62. Australian Government Treasury (2022) "News Media and Digital Platforms Mandatory Bargaining Code" (Report, November 2022).
63. See Corporations Act 2001 (Cth), Chapter 2D and s 912A.
64. "Empowering AI Leadership", World Economic Forum (Web Page).
65. *Ibid*.
66. Malcolm Crompton and Michael Travato, "The New Governance of Data and Privacy", Australian Institute of Company Directors (2018).
67. Corporations Act 2001 (Cth), s 674; ASX rule 3.1.
68. *Ibid*.
69. See, for example, the SOCI Reforms which require regulated entities to manage supply-chain security risks.
70. Australian Human Rights Commission (2021) "Human Rights and Technology Final Report" (Final Report, 2021).
71. *Ibid*.
72. See, for example, Age Discrimination Act 2004 (Cth), Disability Discrimination Act 1992 (Cth), Racial Discrimination Act 1975 (Cth).
73. Australian Human Rights Commission (2021) "Human Rights and Technology Final Report" (Final Report, 2021).

74. *Ibid*.
75. *Ibid*.
76. "Guidance Resource: Artificial intelligence and discrimination in insurance pricing and underwriting (2022)", Australian Human Rights Commission (Web Page, 1 December 2022).
77. Digital Technology Taskforce (2022) "Positioning Australia as a Leader in Digital Economy Regulation" (Issues Paper, March 2022).
78. *Ibid*.
79. "NSW Artificial Intelligence Assurance Framework", Digital.NSW (Web Page).
80. "Artificial Intelligence: Governance and Leadership Whitepaper (2019)", Australian Human Rights Commission (Web Page, 1 February 2019).
81. Australian Human Rights Commission (2021) "Human Rights and Technology Final Report" (Final Report, 2021).
82. *Ibid*.
83. "Artificial Intelligence: Governance and Leadership Whitepaper (2019)", Australian Human Rights Commission (Web Page, 1 February 2019).
84. "AI Ethics Principles", Department of Industry, Science, Energy and Resources (Web Page).
85. "Developing Standards for Artificial Intelligence: Hearing Australia's Voice – submission to Standards Australia", OAIC (Web Page, 26 August 2019).
86. Australian Government, "Regulator Performance Guide" (July 2021).
87. *Ibid.*
88. Critical Technologies Policy Coordination Office, "List of critical technologies in the national interest" (17 November 2021).
89. Department of Industry, Science and Resources (2022) "2022 List of Critical Technologies in the National Interest" (Consultation Paper, August 2022).
90. Department of Industry, Science and Resources (2022) "2022–2023 October Budget Estimation" (Budget Report, August 2022).
91. "Foreign Investment Reforms", The Treasury (Report, June 2020).
92. *Ibid*.
93. "Technical Report | A Method for Ethical AI in Defence", Department of Defence.
94. *Ibid*.
95. *Ibid*.
96. *Ibid*.
97. "Investing in innovation to boost Defence capability", Australian Government Defence (Web Page, 27 September 2022).
98. *Ibid*.
99. "Deakin University signs $5M contract to develop high-tech ADF training system", Australian Government Defence (Web Page, 19 January 2022).

* * *

Acknowledgment

The authors are grateful to Rubaba Rahman for her assistance.

Jordan Cox
Tel: +61 4 3810 8628 / Email: jordan.cox@webbhenderson.com

Jordan is a specialist telecommunications, media and technology partner at Webb Henderson, and has been advising clients in this sector since his admission in 2009.

Jordan has particular experience in the telecommunications sector, where he advises clients in Australia, New Zealand, Asia, Europe, the Middle East and the Pacific Islands. His expertise in the telecommunications sector spans a wide range of commercial and regulatory matters, including:

- the development and supply of wholesale broadband services, particularly next generation access networks;
- global internet infrastructure, including broadband, subsea and satellite networks;
- the design, implementation and reform of regulatory frameworks for next generation access networks; and
- privacy design and compliance, including notifiable data breaches, responses to complaints and investigations.

Bryce Siu
Tel: +61 2 8214 3502 / Email: bryce.siu@webbhenderson.com

Bryce is a commercial and regulatory lawyer in the Sydney office of Webb Henderson, with a focus on telecommunications, media and technology. Bryce assists major international and Australian clients to navigate some of their most nuanced legal and regulatory matters across the telecommunications, media and technology sectors. He has expertise in the regulation and development of next generation broadband networks in Australia, digital identity/distributed ledger technology service agreements and AI commercial agreements across Asia-Pacific and the Middle East.

Webb Henderson

Level 18, 420 George St, Sydney NSW 2000, Australia
Tel: +61 2 8214 3500 / URL: www.webbhenderson.com

Austria

Veronika Wolfbauer & Tullia Veronesi
Schoenherr Attorneys at Law

Trends

Artificial intelligence (AI) is often seen as having great potential for practical use across a wide range of industries. Accompanied by big expectations, opportunities and risks, AI is making its way into corporate practice in Austria. The domain of AI's applicability is steadily expanding and, particularly in industry, its potential is being clearly demonstrated. However, AI is of little interest to small and medium-size companies in Austria. This is principally due to the fact that such organisations either have too little know-how or the acquisition costs are too high.[1] Ignorance about the possibilities and use cases of AI systems is another reason why SMEs are less enthusiastic about adopting AI than larger companies. AI is currently relevant mostly in those sectors that use advanced manufacturing and key enabling technologies. Sectors with high productivity and a significant degree of technological embedding and digitalisation have the most use cases. Other use cases can be found, for example, in the medical field, where virtual online health assistants and chatbots provide patients with information about their medical requests. In (online) retail, the focus is on marketing and individual customer recommendations. Banks and insurance companies rely on AI to simplify complex risk assessments or fraud detection procedures. In Austria, there is an increasing trend towards the utilisation of AI, machine learning (ML) and big data. These technologies are, in summary, gaining popularity in the country.

The persistent spotlight on AI motivated the Austrian government to revamp its AI strategy. Accordingly, in 2021, the government issued its federal strategy on AI – the Artificial Intelligence Mission Austria 2030 (AIM AT 2030)[2] – which will ensure that AI systems are only deployed in a safe environment and for purposes that serve public interests. The strategy also aims to establish Austria as an industrial hub for AI and, moreover, strengthen the country's competitiveness with respect to the development and expansion of this technological area.

Key legal issues

Like many other economies, Austria has recognised the potential of AI and – as a Member State of the EU – is investing and working on suitable framework conditions. It is imperative for Europe to create suitable and agile framework conditions in which innovative companies with AI applications can develop. So far, Europe has only been moderately successful in this endeavour, which explains Austria's 16th place ranking among Organisation for Economic Co-operation and Development (OECD) countries in the Government AI Readiness Index by Oxford Insights.[3]

AI must be designed, developed and deployed in a responsible manner. In order to establish a "social license to operate" for such systems, ethical frameworks are necessary to build public trust at every level. The responsible design, development and deployment of AI also ensures its sustainable use and facilitates the realisation of its many benefits. Thus, the European Commission is currently working intensively on a coherent and holistic AI legal framework.

The AI Act

The AI Act, taking a "horizontal" approach, sets out harmonised rules for developing AI, placing it on the market and using it in the EU. The Act draws heavily on the model of "safe" product certification used for many non-AI products in the new regulatory framework. It is part of a series of draft EU proposals to regulate AI, including the Machinery Regulation and product liability reforms. The law needs to be read in the context of other major packages announced by the EU, such as the Digital Services Act, the Digital Markets Act and the Digital Governance Act. The first two are primarily concerned with the regulation of very large commercial online platforms. The AI Act does not replace the protections offered by the General Data Protection Regulation (GDPR), but will overlap with them. However, the scope of the former is broader and is not limited to personal data. The AI Act also draws on the Unfair Commercial Practices Directive for parts relating to manipulation and deception. Existing consumer law and national laws, such as tort law, are also relevant.

In a nutshell, the AI Act aims to govern the development and utilisation of AI systems deemed as "high risk" by setting standards and responsibilities for AI technology providers, developers and professional users. Certain harmful AI systems are also prohibited under the Act. The Act encompasses a broad definition of AI and distinguishes it from traditional IT. There is ongoing debate in the EU Parliament on the need for a definition for General Purpose AI. The Act is designed to be technologically neutral and future-proof, potentially affecting providers as greatly as the GDPR did. Non-compliance with the Act could result in penalties of up to EUR 30m or 6% of the provider's or user's worldwide revenue for violations of prohibited practices.

Businesses need to determine if their AI systems fall within the scope of the legislation and conduct risk assessments of their AI systems. If they are using high-risk AI systems, they must establish a regulatory framework, including regular risk assessments, data processing impact assessments and detailed record-keeping.

The AI systems must also be designed for transparency and explainability. The terms of use for these systems are deemed crucial for regulating high-risk AI systems, requiring a review of contracts, user manuals, end-user licence agreements and master service agreements in light of the new legislation.

The Regulatory Framework defines four levels of risk in AI:

- Unacceptable risk.
- High risk.
- Limited risk.
- Minimal or no risk.

The AI Act splits AI into four different bands of risk based on the intended use of the systems in question. Of these four categories, the AI Act is most concerned with high-risk AI, but it also contains a number of "red lines". These are AIs that should be banned because they pose an unacceptable risk. Prohibited systems are considered unacceptable insofar as the product of their functionality conflicts with the values of the Union, for example, through the violation of fundamental rights. These include AI that uses subliminal techniques to

significantly distort a person's behaviour in a way that causes or is likely to cause physical or psychological harm, and AI that enables manipulation, social scoring and "real-time" remote biometric identification systems in "public spaces" used by law enforcement.

The Act follows a risk-based approach and implements a modern enforcement mechanism, where stricter rules are imposed as the risk level increases. The EU AI Act establishes a comprehensive "product safety framework" based on four levels of risk. It requires the certification and market entry of high-risk AI systems through a mandatory CE-marking process and extends to ML training, testing and validation datasets. For certain systems, an external notified body may participate in the conformity assessment evaluation. Simply put, high-risk AI systems must go through an approved conformity assessment and comply with the AI requirements outlined in the EU AI Act throughout their lifespan.

Limited-risk AI systems, such as chatbots, must adhere to specific transparency obligations. The AI systems in this category must be clear about the fact that the person is interacting with an AI system and not a human being. The providers of such systems must make sure to notify its users of this.

Product liability and AI liability

The EU Commission has published two proposals for directives aimed at adapting product liability rules to the digital age. The first proposal (Product Liability Directive (PLD))[4] modernises, expands and clarifies the outdated PLD to include AI systems. Proposal number II (AI Liability Act)[5] introduces liability rules for damage caused by AI systems. Specifically, the AI Liability Act establishes new procedural rules for the application of existing Member State non-contractual civil liability rules for harm caused by AI systems.

The EU Commission justifies its need for action, among other factors, with the existing uncertainties among companies and the fear of a premature legal development by national legislators or even by independent legislative measures of the Member States. If a legislator were confronted today with special characteristics of AI, it would have to find an *ad hoc* solution by interpreting the existing regulations.[6] This legal uncertainty also inhibits innovation, because it is difficult for companies to predict how existing liability rules will be applied. This makes it almost impossible to assess one's own liability risk and take hedging measures. The result of a survey conducted by the EU Commission shows that companies consider liability for potential damages, standardisation of data and regulatory barriers (each with around 30%) as major challenges for the adoption of AI.[7] Legislative measures taken hastily by Member States would also lead to fragmentation and, ultimately, legal uncertainties.

The proposed directives are intended to complement each other and the AI Act.[8] The PLD deals with the "strict" liability of a manufacturer for defective products (including AI) and their related damages. The AI Liability Act, on the other hand, deals with liability for "wrongful conduct" by AI systems.

AI-related changes of the revised PLD

- Extension of the product definition: The definition of the term "product" will also include software and digital construction documents. Digital construction documents aim at 3D printing.[9] Software should be understood as a product regardless of how it is delivered or used (i.e. including cloud applications).[10] The product definition does not refer to AI specifically, but to software in general, with the exception of open source software.[11] Free and open source software that is developed and provided non-commercially should be excluded from the scope of the PLD, in order to not prevent the pursuit of

research and innovation. In addition, the Directive specifies when a connected service is considered part of a product, extending strict liability to certain digital services, provided they are equally fundamental to the safety of the product. However, this only applies if the connected services are under the control of the manufacturer of the product, i.e. if they are provided by the manufacturer itself or the manufacturer recommends them or otherwise influences their provision by a third party.

- Extension of the liability reasons (redefinition and extension of the concept of fault): A product is defective if it does not meet the justified safety expectations of the average consumer. The assessment in each individual case depends on the objectively justified safety expectations and presentation of the product. So far, so well known. In the future, however, other factors will also have to be taken into account. The networking and self-learning functions of products are explicitly mentioned in the draft PLD, but also the requirements for the cybersecurity of the product.[12] This change pays tribute to digitalisation and is particularly relevant to the use of neural networks and self-learning algorithms as embedded software.
- Extension of the material scope of protection: Up to now, personal injury (life, body, health) and damage to property, insofar as it occurred to a movable physical object *different* from the product, led to a claim for compensation. Pure financial losses, however, are not eligible for compensation. This restriction to fault-related violations of legal rights is maintained in principle, but the PLD provides for certain extensions. For example, the "*loss or corruption of data not used exclusively for professional purposes*" is defined as "damage" in the product liability regime. In relation to AI systems, this proposal means that in the case of damage caused by faulty AI systems, such as physical damage, damage to property or loss of data, the provider of the AI system or any manufacturer who integrates an AI system into another product can be held responsible and, regardless of fault, compensation can be claimed.
- Disclosure obligations/easier evidence for injured parties: The plaintiff bears the burden of proving the damage, the defectiveness of a product and the causal connection between the two. To do so, the plaintiff must present facts and evidence that sufficiently support the plausibility of the damages claim. Due to the information deficit that consumers naturally have when using products *vis-à-vis* their manufacturers, the EU Commission's draft provides for "access to evidence". According to this, the defendant must "produce relevant evidence within their control". If the defendant does not comply with this court order or does not do so completely, there is a high risk of losing the case, because the defectiveness of the product is then presumed by law.[13] However, this disclosure is still to be preceded by a proportionality test, which is also intended to protect trade secrets, among other things.

The key topics of the AI Liability Act

- Addressees and material scope of application: Both providers of AI systems and, in certain cases, their users can be liable parties according to the meaning of the draft AI Liability Act. The definitions[14] refer to the definitions in the AI Act. Accordingly, the "provider" is the natural or legal person, authority, institution or other body that develops an AI system or has it developed with a view to placing it on the market or putting it into operation in its own name or under its own brand (in short: the manufacturer). A "user" is a person who uses an AI system under his or her own responsibility, in the context of a professional activity (in short: a professional user). The material scope of application is limited to non-contractual fault-based civil damages claims and extends primarily to high-risk AI systems and to "other" AI systems.

- Access to evidence: Member State courts are granted the power to order the disclosure of evidence by the provider/user if the latter has already refused to comply with the direct request of a "potential claimant" (injured party or another person entitled to make a claim). This only applies to the use of high-risk AI, and only if the high-risk AI is suspected of having caused harm.[15] To obtain this order, the potential claimant must have "made all reasonable efforts" to obtain the evidence from the defendant.[16] This draft also obliges the courts to take into account the legitimate interests of all parties in their orders to disclose or preserve evidence and to limit them to a necessary and proportionate extent.[17] Particular consideration is to be given to the protection of trade secrets, leaving it to national courts to balance disclosure against such protection in individual cases. Courts should be empowered to take specific measures to protect the confidentiality of trade secrets, for example, by restricting access to documents containing trade secrets to a limited number of persons. If the defendant fails to comply with the disclosure or seizure order, it can be assumed that the defendant has breached a relevant duty of care. However, this presumption can be challenged or disproven.[18] The problem with this broad formulation ("relevant due diligence") is that it is unclear whether this provision is limited to the obligations under the AI Act or also includes breaches of other (national) laws, such as the GDPR, or general due diligence obligations. The wording of the standard rather argues for a limitation to "relevant due diligence obligations" in the sense of those obligations under the AI Act that affect high-risk AI system providers. The related recital 26 of the AI Liability Act, on the other hand, allows for a broader understanding ("*In addition, the fault of users of high-risk AI systems may be established against the backdrop of Article 29(2) [of the AI Act] if other duties of care set out in Union or national law have been breached*").
- Presumption of causality: As mentioned, one aim of the draft is to relieve injured parties of causality issues when claiming damages in connection with non-compliance with the AI Act, in order to create an incentive to comply with the AI Act. Specifically, the (rebuttable) presumption of causality[19] is intended to make it easier for the plaintiff to prove the causal link between the defendant's fault and the output produced by the AI system that caused the damage. These presumption rules are important because, without them, establishing causality would likely require a plaintiff to conduct a "review of the AI decision", which can be nearly impossible to do. However, the presumption of causality only applies if, in the opinion of the court, it is "excessively difficult" for the plaintiff to demonstrate the veracity of this presumption of causality.[20] The plaintiff must also ensure that the following conditions are met:
  - the plaintiff has proven the defendant's fault or the defendant's fault is presumed due to non-compliance with a duty of care;
  - the circumstances of the case make it sufficiently probable that the defendant's fault influenced the AI output (the "behaviour of the AI system"); and
  - the plaintiff has proven that the AI output caused the damage.

In addition, differentiated rules are provided for high-risk AI systems, whereby the application of the presumption of causality in relation to high-risk AI systems is to be limited to non-compliance with certain obligations under the AI Act. In addition, the presumption of causality will not apply if the defendant proves that the plaintiff had sufficient evidence and expertise to establish such a connection.[21]

It should be emphasised, however, that the draft does not contain an all-encompassing presumption of causality (no reversal of the burden of proof), but that the causality between

the breach of duty of the provider and the AI output is presumed (under the outlined conditions). Hence, the injured party must still prove the existence of damage, the causal connection between the output and such damage, etc.

Austrian perspective

In Austria, the proposal of those draft legal frameworks has been reflected in and monitored by the media. However, since those drafts are still subject to discussion and frequent amendment, the media contented itself with reporting rather than explaining the proposal's potential impact.

The proposed regulations will have a significant impact and will affect many stakeholders. Depending on the outcome of the discussions about the definition of AI, the framework will certainly encompass impacts on companies and stakeholders beyond those dedicated groups that are already actively working with AI systems.

Depending on the outcome of the discussions about the definition of AI, companies using software that makes predictions or decisions that guide or provide options to individuals will also be subject to the proposed regulation. This includes commonly used tools such as telematic software in cars, e-learning tools in work environments and self-creating content in private cloud solutions. There is also an expected strong merger of AI regulation and data protection regulation, as AI involves software, which entails the processing of data. The proposed AI regulation aims to regulate both the providers and users of AI, in order to protect individuals impacted by the deployed AI. A speedy resolution on the definition of AI and the establishment of a final legal framework would be beneficial for Europe, while failure could result in the continent losing its competitive edge.

* * *

Endnotes

1. Frauenhofer Austria KI-Study, *Künstliche Intelligenz in Österreichs Unternehmen*, 2022; (https://publica.fraunhofer.de/entities/publication/33a3eab0-210e-4991-9489-9fb4d39226f4/details).
2. The AIM AT 2030 paper is available for download at https://www.bmk.gv.at/dam/jcr:8acef058-7167-4335-880e-9fa341b723c8/aimat_ua.pdf (German-English).
3. Oxford Insights, *Government AI Readiness Index*, 2022; (https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf).
4. Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, COM (2022) 495 final.
5. Proposal for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive), COM (2022) 496 final.
6. AI Liability Directive-E, 2.
7. European enterprise survey on the use of technologies based on artificial intelligence, IPSOS 2020, Final Report, 12, available at https://op.europa.eu/en/publication-detail/-/publication/f089bbae-f0b0-11ea-991b-01aa75ed71a1 (accessed 3.1.2023).
8. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union acts, COM(2021) 206 final; for more details see Herst, AI Regulation Act – the Regulation of Artificial Intelligence in this issue.

9. Recital 14.
10. Recital 12.
11. Recital 13.
12. Art 6, Rec 23.
13. Art 9 para 2.
14. Art 2.
15. Art 3 para 1.
16. Art 3 para 2.
17. Art 3 para 4.
18. Art 3 para 5.
19. Art 4.
20. Art 4 para 5.
21. Art 4 para 4.

Veronika Wolfbauer
Tel: +43 1 53437 50791 / Email: v.wolfbauer@schoenherr.eu

Veronika Wolfbauer has been with Schoenherr since 2013, having become an attorney at law in 2016 and counsel in February 2019. Prior to joining Schoenherr, she gained experience at well-known national law firms in Vienna and was legal counsel at a gas trading hub. Veronika is part of the firm's IP & technology and regulatory practices, a leading member of its privacy and data protection team, and the head of the technology regulation and audio-visual media law team. She provides strategic and legal advice to national as well as international corporate clients and also lectures in those areas. In addition, she leads administrative proceedings before the DP regulator and appeal proceedings, including addressing the Austrian Highest Administrative Court, the Austrian Constitutional Court and the European Court of Justice.

Tullia Veronesi
Tel: +43 1 53437 50310 / Email: tu.veronesi@schoenherr.eu

Tullia Veronesi has been with Schoenherr since 2021 and is an attorney at law. Her main areas of practice are IT, blockchain, cryptocurrencies, AI, E-commerce, digitalisation, start-ups, cyber security as well as intellectual property and data protection law. Before joining Schoenherr, Vienna, she practised with another international law firm as an associate and as a CLO in the new tech area. Tullia graduated from the University of Linz (Mag. iur. 2017) and from the University of Vienna (LL.M. 2018). She regularly lectures and has published articles in the field of crypto and data protection, as well as a book and a podcast on blockchain technology and is a jury and board member in various committees.

Schoenherr Attorneys at Law

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 370 / URL: www.schoenherr.eu

Canada

Simon Hodgett, Ted Liu & Sam Ip
Osler, Hoskin & Harcourt LLP

Trends

Artificial intelligence (AI) has continued to become more mainstream, as real, practical use cases, such as chatbots, image and facial recognition, and robotic process automation, are deployed across industries. As global competition to lead the AI race increases, Canada, propelled by a stellar research community that has been 30 years in the making, as well as an innovative and dynamic technology ecosystem, is becoming a global leader in AI.

Canada has been at the forefront of AI advancements for decades and has gained recognition as 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 AI advancements. The Canadian research community continues to produce and attract leading machine learning and AI researchers, data scientists and engineers, earning the fourth overall ranking among 62 countries in The Global AI Index.[1] Canada was the first country in the world to adopt a national AI strategy and is home to a dynamic technology ecosystem with more than 4,000 active startups, making it one of the world's largest innovation hubs.[2] The Canadian AI industry is quickly accelerating, supported by research labs, Government funding and global investors. Businesses and Governments are already implementing innovative AI solutions developed by Canadian startups.

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 has increased over the past five years. In 2022, Toronto startups raised upwards of $3.7 billion.[3] AI startups across Canada by themselves raised over $1 billion in funding in 2022.[4] The Canadian government has also unveiled a new agency, the Canada Innovation Corporation, to encourage innovation in areas such as AI.

The flourishing AI community and policy interest has presented opportunities for creative solutions to unique AI-related legal challenges, as well as the application of general legal principles to the application of this increasingly important technology.

Ownership/protection

Intellectual property

The ownership of intellectual property in the AI models that are derived from/produced by 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, the data

comprising such work product does not meet the legal threshold necessary for intellectual property protection, as Canada does not have a statutory or common law regime that protects ownership of raw data elements. There has been increased focus and discussions regarding whether copyright should be granted to works created by or with the help of AI, and whether AI can be the inventor of a patentable invention. Canada is an active participant in these global discussions;[5] however, these questions remain outstanding.

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) has significant value also for a supplier's future customers. Consequently, suppliers also have an interest in obtaining the right to use this data. It is imperative that suppliers and customers clearly allocate data use rights contractually as between supplier and customer in their commercial contracts.

Ownership of AI

In Canada, negotiations around the ownership of an AI solution often involve a case-by-case consideration of the various elements of the solution, which typically comprise: (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. In some cases, 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. In other cases, however, 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, provided it retains ownership of the ancillary algorithms. Ultimately, the typical allocation of ownership in standard technology agreements must be carefully re-considered 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 simply 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 rights in data are often referred to as "ownership" of the data; however, within the Canadian legal framework, most data is not owned, and it is therefore essential that the parties clearly negotiate their respective use rights in the contract. The typical default position with respect to data use rights likely will not meet the needs of a developer or supplier of AI, whose business model likely relies 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 and confirmation of data use rights 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 before AI or even advanced data analytics attained widespread use. As a result, the licensee of data 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.

Antitrust/competition laws

The Organization of Economic Co-operation and Development (OECD) has recognised the potential risk that algorithms could: "(1) make markets more prone to collusion, by changing structural characteristics such as transparency and frequency of interaction; and (2) replace explicit collusion with tacit coordination, by providing companies with automatic tools to implement a collusive agreement without direct communication."[6]

The Competition Bureau of Canada (Competition Bureau) has acknowledged the theoretical possibility of AI technologies reaching collusive agreements without human involvement. However, it has not publicly commenced any investigations related to collusion based on AI technologies and, in 2018, commented that it had yet to see any evidence of this type of collusion occurring in practice.[7]

The Competition Bureau has indicated that use of algorithms could form the basis of a cartel offence. However, the existence of an agreement – actual or tacit – to fix or control prices is necessary, and conduct that amounts to conscious parallelism (for example, use of a price matching algorithm) alone is not sufficient to form the basis for the offence.[8]

Board of directors/governance

With the growing relevance of AI technology to organisational strategy and operations, AI-related issues have become an increasingly important governance consideration for boards of directors in Canada. Canadian directors are expected to oversee the business and affairs of the corporation, and as part of such stewardship need to understand the strategic implications of adopting emerging technologies like AI, as well as the associated risks.[9]

It has become increasingly important for corporate boards to understand the role currently played by data and emerging technologies within the organisation to understand the risks and the opportunities available to the organisation to leverage AI to enhance performance and efficiency. Boards are sensitive to the value of organisational data and the importance of implementing measures to safeguard the security of the organisation's data and the need for cybersecurity monitoring and reporting systems, as well as the associated regulatory risks (e.g., data use and privacy law). Increasingly, boards are focussing on AI opportunities, understanding how such technologies can bolster or hinder an organisation's competitive edge, shape new corporate opportunities and drive value across the supply chain.[10] Boards

are also becoming more sensitive to ethical considerations from the use of data (e.g., related to fairness, transparency, explainability, etc.) and their role in setting the ethical culture of the organisation, including with respect to the use of data and AI.

The speed of change of business models in general, and particularly rapid advances in technology, are making it difficult for boards to remain current, and to anticipate potential threats to business operations. In order to exercise appropriate oversight, Canadian boards typically leverage internal or third-party expertise to enhance technology education at a board-level and engage in regular discussion with management to understand strategic planning as it relates to AI and other emerging technologies. The outcome of such activities can be expected to result in: (i) development of an AI strategy; (ii) establishing an AI governance and risk management framework, including to protect against unauthorised data access and use; (iii) AI talent management; and (iv) compliance with emerging laws, standards and industry norms.[11]

Regulations/Government intervention

Consumer protection legislation

Canadian provinces and territories have legislation related 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 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 comprises a patchwork of provincial legislation with similar themes but different requirements, may pose real challenges where AI-based goods or services are caught within its framework.

Autonomous vehicle regulation

In general, the regulatory landscape for autonomous vehicles in Canada is evolving as federal and provincial governments play a role in regulation.

At the federal level, Transport Canada is responsible for approving the safety of autonomous vehicles and their testing. Transport Canada published version 2.0 of its "Guidelines for Testing Automated Driving Systems in Canada" in 2021, which set out the best practices for the safe conduct of autonomous vehicle testing. The federal government also has jurisdiction regarding which autonomous test vehicles can be imported into Canada under the *Motor Vehicle Safety Act*.

At the provincial level, provinces are responsible for regulating the use autonomous under their respective provincial motor vehicle or traffic safety acts, such as the *Highway Traffic Act* in Ontario. A number of provinces, such as Ontario, Quebec British Columbia, and Alberta have pilot programs for level 5 vehicles, a generally accepted classification regime promulgated by the Society of Automotive Engineers that defines such vehicles as fully autonomous vehicles that do not require any human inputs to drive in all conditions.

Governments at the federal and provincial levels have also been proactively funding the development of R&D in Autonomous vehicles and their deployment. At the federal level, National Research Council grants, Strategic Innovation Fund investments, and Industrial Research Assistance Programs are available for startups and larger corporations that are engaged in autonomous vehicle research and commercialisation. On a provincial level, Ontario in 2021 for example launched the Ontario Vehicle Innovation Network, which

dedicates $56.4 million to programs for next generation automobiles, which includes autonomous vehicle projects.

Copyright and copyright reform

Under current copyright law in Canada, it is unclear whether AI-generated works are protected by copyright, as those laws protect works that are the product of an author's skill and judgment. Copyright jurisprudence in Canada suggests that an author must be a natural person, although the Canadian Intellectual Property Office (CIPO) has in one instance granted registration of copyright where AI is named as a co-author.[12]

As part of its review of the Copyright Act, the House of Commons' Standing Committee on Industry, Science and Technology in 2019 issued a report that made a series of recommendations related to AI.[13] Most noteworthy were recommendations that the Government of Canada amend the Copyright Act to: provide clarity around the ownership of a computer-generated work; 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 jurisdictions, including the US, Japan and the EU. These jurisdictions have copyright regimes that allow for information analysis of works without a separate licence, including for commercialisation purposes.

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.[14] As AI increases in complexity, obtaining meaningful consent and satisfying the reasonable purpose test is becoming more difficult.[15] As a result, organisations are increasingly seeking to limit the application of privacy laws by "anonymising" the data that their AI solutions require. Achieving "anonymisation" of personal data, both by itself or in combination with other data, is not a trivial task and there remain many questions about when true anonymity is achieved.

Proposed Artificial Intelligence and Data Act

On June 16, 2022, the Minister of Innovation, Science and Industry tabled Bill C-27, introducing updates to the federal private sector privacy regime and appending a new law on AI, the *Artificial Intelligence and Data Act* (AIDA). If passed, the AIDA would be the first law in Canada specifically regulating the use of AI systems. The stated objective of AIDA is to establish common requirements across Canada for the design, development and deployment of AI systems that are consistent with national and international standards and to prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or their interests, in each case, in a manner that upholds Canadian norms and values in line with principles of international human rights law. While the general approach in AIDA is apparent, the full impact of the legislation will only be appreciated with the release of associated regulations which will set out most of the detailed application.

In brief, AIDA adopts a risk-based approach, focusing on areas where there is greatest risk of harm and bias and establishes rules for the use of AI systems that are "high-impact" (a term that will be defined in the regulations). This is similar to the approach found in the proposed

AI Act in the EU. AIDA applies to private sector organisations that design, develop or make available for use AI systems[16] in the course of international or interprovincial trade and commerce, an area of regulation within the federal government's legislative authority under Canada's constitution. Notwithstanding considerable uncertainty with respect to its application, the financial penalties for contraventions of AIDA will be significant: up to 3% of global revenue or C$10 million, with higher penalties of up to 5% of global revenue or C$25 million or imprisonment, in the case of an individual.

A high-level overview of requirements AIDA imposes on organisations are as follows:

- **Assessment and risk mitigation measures:** Organisations responsible for AI systems must assess whether it is a high-impact system (a term to be defined in the regs), and establish measures to identify, assess and mitigate risk of harm or biased output that could result from use of the system.
- **Monitoring:** Organisations responsible for high-impact systems must establish measures to monitor compliance with the risk mitigation measures.
- **Transparency:** Organisations that make available for use, or manage the operation of a high-impact system, must publish on a publicly available website in plain English a description of:
  - how the system is, or intended to be used;
  - the types of content that it generates and the decisions, recommendations or predictions it makes;
  - the mitigation measures established to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system; and
  - any other information prescribed by regulation.
- **Recording keeping:** Organisations that carry out a regulated activity must comply with prescribed record keeping requirements.
- **Notification:** Organisations responsible for high-impact systems must notify the Minister if use of the system results or is likely to result in material harm.
- **Use of anonymised data:** Organisations that carry out activities regulated by the act and who process or make available for use anonymised data in the course of the activity must, in accordance with the regulations, establish measures with respect to: (a) the manner in which data is anonymised; and (b) the use/management of anonymised data.

Bill C-27 is now being debated at its second reading, and will then be reviewed, potentially changed, and further debated, although current indicators are its broad approach will carry forward into the final legislation.

Privacy Legislative Developments: Québec and Federal

Québec's private-sector privacy law was substantially amended by the Québec National Assembly in September 2021 through the passage of *An Act to modernize legislative provisions as regards the protection of personal information* (Law 25). Law 25 introduced sweeping changes, including: (1) requirements for companies to implement internal privacy policies; (2) privacy impact assessment obligations; (3) data localisation restrictions; (4) breach reporting and notification provisions; (5) enhanced consent requirements; (6) notice obligations for identification, location and profiling technologies; and (7) new data subject rights, such as a functional "right to be forgotten", a right to data portability, and rights with respect to automated decision-making.

Law 25 also bolsters the Québec Privacy Act's enforcement regime. Organisations that contravene the Québec Privacy Act will be subject to fines of up to the greater of $25 million or 4% of worldwide turnover, and administrative monetary penalties of up to the greater of $10

million or 2% of worldwide turnover. Certain provisions under Law 25 come into force over the three years following its enactment, but the majority come into force in September 2023.

In particular, Law 25 has introduced multiple provisions applicable to AI:

1. *De-identified information.* Law 25 allows an organisation to use an individual's personal information without their knowledge or consent for the organisation's internal research and development purposes, if the information is de-identified before it is used.[17]
2. *Re-identification*. Law 25 creates an offence, punishable by fines of up to up to $25 million, or the amount corresponding to 4% of worldwide turnover for the preceding fiscal year (whichever is greater) for anyone who identifies or attempts to identify a natural person using de-identified information, without the authorisation of the person holding the information or using anonymised information.[18]
3. *Automated decision making.* Law 25 provides that Québec organisations using automated processes to make decisions about individuals based on their personal information, must (a) inform each individual of the decision-making process, and (b) provide details of the factors informing the decision upon request.[19]
4. *Right of cessation of dissemination and de-indexing.* Law 25 provides that Québec organisations must cease disseminating an individual's personal information or de-index hyperlinks providing access to their information via technical means on request, if certain conditions are met. Conditions may be met if dissemination of the information contravenes a law or court order, or if harm to the individual's reputation or right to privacy outweighs the public's interest in knowing about the information and the interest of free expression.[20]
5. *Biometrics*. Law 25 provides that as of September 2022, Québec organisations must inform the provincial privacy regulator of (a) the creation of any biometric data bank, and (b) the use of a biometric system for verifying or confirming individuals' identities, even if the organisation does not store such information. [21]
6. *Confidentiality by default.* Law 25 provides that as of September 2023, Québec organisations' technological products or service that collect personal information must have privacy settings providing the highest level of confidentiality by default, without any intervention of the user. This obligation does not apply to browser cookies.[22]
7. *Enhanced transparency*. Law 25 provides that as of September 2023, Québec organisations must inform an individual before using technology that allows the individual to be identified, located or profiled.[23]

As described above, in 2022 the Government of Canada introduced new privacy legislation for the privacy sector the *Digital Charter Implementation Act, 2022*.

If it passes, Bill C-27 will establish a new federal private-sector privacy law in Canada, comprised of the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* (DPTA), and the *Artificial Intelligence and Data Act* (the third part of Bill C-27, which would enact AIDA, described above, will be voted on separately from the parts that would enact the CPPA and the DPTA).

Among the most significant changes to the existing privacy legislative framework proposed by Bill C-27 are: (1) the imposition of potentially severe administrative monetary penalties for non-compliant organisations;[24] (2) an expanded range of offences for certain serious contraventions;[25] (3) the establishment of a Personal Information and Data Protection Tribunal;[26] (4) enhancements to the consent requirement;[27] and (5) the granting of data mobility rights to individuals.[28]

In particular, the CPPA seeks to introduce provisions related to de-identification,[29] re-identification,[30] and automated decision making[31] substantially similar to those introduced by Law 25 in Québec.

Provisions in both Law 25 and the CPPA have raised significant concerns for organisations developing or using AI systems. By way of example:

- Law 25 and the CPPA both adopt a strict test for assessing whether information is de-identified and excludes de-identified information, under certain conditions, from the statutes' consent requirements. Although the CPPA defines anonymised information and clarifies that properly anonymised information falls outside of the regulatory regime (similar to the GDPR),[32] commentators have suggested that the CPPA's proposed definition of "anonymise" is so stringent as to be practically unworkable.[33]
- Neither Law 25 nor the CPPA references pseudonymised personal information (which contrasts with the GDPR's approach to permitting use of pseudonymised information for archiving purposes in the public interest, scientific or historical research purposes, statistical purposes, or general analysis).
- Law 25 provides, and the CPPA will provide, only narrow exceptions to the prohibition on re-identification.
- Law 25 regulates, and the CPPA will regulate, a much broader scope of automated decision-systems than under the GDPR, applying to predictions and recommendations, in addition to decisions and regardless of whether there is human oversight. Furthermore, the right of explanation applies to all automated decision-making, even if the prediction, recommendation or decision does not produce legal or similarly material effects on the individual.

Other privacy developments: British Columbia, Ontario, federal, and industry

On April 13, 2021, the Legislative Assembly of the Province of British Columbia appointed a Special Committee to review British Columbia's *Personal Information Protection Act* (PIPA). The Special Committee completed its review and provided recommendations to update PIPA to reflect the changing privacy landscape.

As it relates to AI, the Special Committee recommended that PIPA (a) include a requirement for organisations to notify individuals when an automated process is used to make a significant decision about them, and (b) allow the individual to request human intervention in the decision-making process.

The Special Committee also recommended that the Office of the Information and Privacy Commissioner for British Columbia "undertake a public consultation to study the long-term socioeconomic impacts of artificial intelligence, including automated decision making and automated profiling, and provide the Ministry of Citizens' Services with any recommendations for proposed amendments".[34]

From May to June 2021, the Ontario Government held an open consultation to solicit input and ideas on how to develop an AI framework that is accountable, safe and rights-based. The consultation was part of the Government's Digital and Data Strategy and the framework was developed following the Open Government Partnership principles. The proposed AI framework is centered on three main commitments:

1. No AI in secret.
2. AI use Ontarians can trust.
3. AI that serves all Ontarians.[35]

These commitments are supported by the Information and Privacy Commissioner of Ontario, provided that adequate definitions and frameworks are implemented to serve these broad objectives.[36]

On June 17, 2021, the Ontario Government released a white paper outlining a proposal to develop standalone private sector privacy legislation. The white paper states that safeguards

need to be put in place when AI is used and suggests prohibiting "the use of AI and automated decision-making systems when they could cause harm to citizens". The white paper also recommends "providing stronger rights to inform Ontarians when and how their data is used" by AI technologies and suggests providing a right to object or contest the use of AI in decision making. The white paper also suggests prohibiting the use of AI to make a decision about an individual, including profiling, that could have a significant impact on the individual.[37]

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. A CANON working group has recently published its recommendations for Parliament to enhance the deidentification and anonymisation provisions in Bill C-27.[38]

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.[39] 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.[40]

Algorithmic transparency and trustworthiness

Governments in Canada are also considering algorithmic transparency and trustworthiness. The Government of Canada issued the Directive on Automated Decision-Making, April 1, 2019.[41] 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 and applies to most federal government institutions, with notable exception of the Canadian Revenue Agency (CRA). The Directive includes a risk-based framework that includes providing advance notice of automated decision-making and meaningful explanations after decisions are made.

The Province of Ontario has published the beta version of its Principles for Ethical Use of AI that sets out six principles that apply to the data enhanced technologies in Ontario Government processes, programmes and services that are designed to be aligned with Ontario's ethical consideration and values. These include ensuring use of AI is: (1) fair and explainable; (2) good and fair; (3) safe; (4) accountable and responsible; (5) human centric; and (6) sensible and appropriate.[42]

The Province of Ontario has also published the alpha version of its Transparency Guidelines, which sets out points to help minimise risks and maximise benefits of using data-driven technologies within Government processes, programmes and services through transparency, which includes: (1) ensuring people who will benefit most and who will be impacted by such technology are kept in focus and in the loop; (2) providing public notice and clear communication channels to help foster trust that the use of AI is safe and appropriate; and (3) allowing meaningful access to enable accountability of the computational model.[43]

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.[44] A majority of the provinces and territories have adopted open data policies, directives or guidelines, along with open data websites or portals, evidencing a commitment to leveraging open data solutions in the public sector.

Several organisations have developed data standards and frameworks for open data. For example, the Digital Governance Standards Institute (part of the Digital Governance Council and formerly known as the CIO Strategy Council) has published four standards on data governance: (1) Data Centric Security (CAN/CIOSC 100-1:2020); (2) third-party access to data (CAN/CIOSC 100-2:2020); (3) Specification for Scalable Remote Access (CIOSC/PAS 100-4:2020); and (4) the responsible use of digital contact tracing and monitoring data in the workplace (CIOSC/PAS 100-6:2021).[45] There are also new standards on data governance in development.[46] These standards set out the requirements for data protection and privacy safeguards in the context of open data sharing.

Implementation of AI/big data/machine learning into businesses

Managing risk

When implementing AI, big data and machine learning into businesses, it is important to consider the allocation of risks. 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.

As businesses expand their use of AI-based solutions, we are seeing use cases where AI-based solutions are becoming an integral part of a business' key customer-facing or back-office operations. As these production uses increase, the risks associated with the inability of a business to continue to use the AI solution – for example, if an insolvency event affecting the AI solution provider occurs – are garnering more attention during negotiations, with terms relating to ongoing due diligence, security of licence rights and access to data, business continuity and termination assistance becoming increasingly important. In response, Canadian organisations have begun to participate in risk management frameworks, including the National Institute of Standards and Technology AI Risk Management Framework which, although promulgated by a US Agency, was developed in collaboration with stakeholders worldwide, including Canadian public and private sector participants.

Assurances related to ethical AI

An important part of implementing AI in businesses is considering whether automated decision-making systems were developed ethically and in a manner that mitigates bias. Businesses should consider asking AI providers and developers of technologies to provide representations and warranties and other assurances that automated decision-making systems were developed in an ethical manner and so as to mitigate bias. Provisions have

included requiring the company to maintain and adhere to practices, policies, controls and procedures related to the ethical and responsible use of AI, including with reference to the Montreal Declaration.[47] Other measures have included expanding references to applicable laws to include guidance of regulators.

AI transparency

When implementing AI in businesses, emphasis should also be placed on AI transparency. This is particularly important as modern consumers are paying more attention than ever before to where and how products and services are made. As more organisations turn to the use of AI as part of their business, including the use of AI as part of consumer-facing products or services, it has become important and will continue to be important for users of AI to ensure that AI providers and developers provide transparency regarding how decisions are being made through the use of AI. This will require AI providers and developers to be able to explain the AI models and algorithms used in making decisions. Users of AI should consider asking for auditable records to be maintained with respect to the AI models and algorithms used in connection with any decision-making, and for the right to access such records and, where possible, understand the AI models and algorithms used in the event the user or consumer is required to explain such decision-making.

Civil liability

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 the first party 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.[48] 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.[49]
- 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. For example, while the US has seen lawsuits regarding the

liability of a self-driving system in a fatal accident, there have been no such lawsuits to date in Canada.[50] 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",[51] 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.

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.

The rationale for allocating risk in 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.

Discrimination and bias

In Canada, there has been little to no guidance from courts or tribunals on the application of human rights legislation to automated decision making. While there are no cases that touch on the application of AI, general principles of discrimination law suggest a potential for human rights claims.

In *Ewert v Canada*, 2018 SCC 30, the Supreme Court of Canada ruled on the use of actuarial risk-assessment tools in the corrections context. Mr. Ewert, a federal inmate and Métis man, challenged the use of actuarial risk-assessment tools to make decisions about his carceral needs and about his risk of recidivism. His concerns, raised in his initial grievance in 2000, were that these tools were "developed and tested on predominantly non-Indigenous populations and that there was no research confirming that they were valid when applied to Indigenous persons" (para. 12). He eventually sought a declaration in the Federal Court that the tests breached his rights to equality and to due process under the Canadian Charter of Rights and Freedoms,[52] and that they were also a breach of the Corrections and Conditional Release Act,[53] which requires the Correctional Service of Canada (CSC) to "take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible" (s. 24(1)).

While the *Charter* arguments were unsuccessful, the court held that CSC breached its obligations under the CCRA. The case did not explicitly cite algorithmic decision-making, but it grapples

with the issue where the data used to develop and train the algorithm, or the assumptions coded into the algorithm, create biases that can lead to inaccurate predictions about individuals who fall outside the dominant group that has influenced the data and the assumptions. As the CSC had long been aware of concerns regarding the possibility of psychological and actuarial tools "exhibiting cultural bias" (para. 49), the onus is placed on CSC to conduct research into how the tools impact cultural groups and verify the validity of them. The majority states that "this provision requires the CSC to ensure that its practices, however neutral they may appear to be, do not discriminate against Indigenous persons" (para. 54). Moving forward, it is unclear whether the applicability of *Ewert* to the commercial machine learning and AI context is diminished if the datasets that train the AI in question are deemed "fair".

When assessing the extent to which a dataset is fair, human rights principles would likely inform the analysis in courts. In the human rights context, is important to consider allocative harms. These occur when there is an unjustified unequal distribution of outcomes or resources on the basis of a protected ground, such as gender or race. Allocating or denying benefits based upon an individual's race, gender, sexuality, or other protected ground is degrading and dehumanising because it communicates that the individual is to be judged as a group, rather than as a person, and because such decisions are frequently based on stereotypical assumptions about groups historically disadvantaged by discrimination. Therefore, it is important that companies using or developing AI decision-making systems test whether or not the technology systematically denies a benefit to individuals who come from certain groups that can be identified based on a protected ground.

Conclusion

Canada continues to advance the discourse and development of a made-in-Canada approach to AI along with developing global standards. However, there is a potential that that the specifically Canadian legal and regulatory framework and the uncertainty that it creates threatens to impede Canada's progress. Conversely, if Canada can 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, Canada will be in a position to reap the rewards.

* * *

Endnotes

1. https://www.tortoisemedia.com/intelligence/global-ai/.
2. "Pan-Canadian AI Strategy Impact Assessment Report", Accenture & CIFAR, October, 2020, p. 6. 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.
3. https://briefed.in/report-tor-q4-2022.html?subscriber-vip24.
4. "Canada's new superclusters" SME research and statistics. [online] (February 18, 2019) http://www.ic.gc.ca/eic/site/093.nsf/eng/00008.html. See also: https://www.crunchbase.com/hub/canada-startups.
5. "WIPO Consultation on Artificial Intelligence and Intellectual Property - Submission from the Government of Canada" World Intellectual Property Organization. [online] (February 14, 2020) https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_canada.pdf.

6. https://one.oecd.org/document/DAF/COMP/M(2017)1/ANN3/FINAL/en/pdf.
7. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04342.html#sec03.
8. See Footnote 15 of https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04582.html#fn15.
9. Canada Business Corporations Act, RSC 1985, c C-44, s 102.
10. See generally: "Emerging Technologies: Understanding the Disruption Ahead" Institute of Corporate Directors. [online] (April 2019) https://www.icd.ca/ICD/media/documents/ICD_Emerging_Technologies_Report_EN.pdf.
11. "Building Data and AI Ethics Committees" Ronald Sandler and John Basl. [online] (August 20, 2019) https://www.accenture.com/ca-en/insights/software-platforms/building-data-ai-ethics-committees.
12. In 2021, Suryast – an AI generated painting inspired by Van Gogh's Starry Night was registered for copyright by the CIPO. The AI was one of the two registered co-authors on the work, with the other being a natural person, a Mr. Ankit Sahni.
13. https://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/report-16.
14. Personal Information and Electronic Documents Act (S.C. 2000, c. 5), s. 5(3).
15. "Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'acces a l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" Office of the Privacy Commissioner of Canada. [online] (February 2, 2021) https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#toc1;"Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. [online] (October 28, 2020) https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.
16. An "artificial intelligence system" is broadly defined under AIDA and captures any "technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions".
17. Law 25, An Act to modernise legislative provisions as regards the protection of personal information, 1st Sess, 42nd Leg, 2021, s. 110 (Law 25).
18. Law 25, s.160.
19. Law 25, s. 21.
20. Bill 54, s. 121.
21. Law 25, ss 80–81.
22. Law 25, s. 108.
23. Law 25, s. 107.
24. CPPA, s. 94.
25. CPPA, s. 128.
26. DPTA, being Part 2 of Bill C-27.
27. CPPA, s. 15.
28. CPPA, s. 72.
29. CPPA, s. 2(1), "de-identify", s. 2(3), ss. 20-22, s. 39, ss. 74–75. Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2nd Sess,

43rd Parl, 2020, cls 20 and 21 (CPPA). Bill C-11 also included a limited exception to concept for disclosing de-identified information for socially beneficial purposes.

30. CPPA, s. 75, s. 128. CPPA, cls 75 and 125. The Bill C-11 offence would have been punishable by fines of up to $25 million or 5% of gross global revenue (whichever is greater).
31. CPPA, s. 2(1), "automated decision system", s. 63(3), (4). CPPA, cls 62 and 63.
32. CPPA, s. 2(1), "anonymize", s. 6(5).
33. Final CANON Bill C-27 Working Group Document "Proposed amendments to de-identification and anonymization provisions in the Digital Charter Implementation Act, 2022 (Bill C-27)", December 7, 2022.
34. "Modernizing British Columbia's Private Sector Privacy Law". Special Committee to Review the Personal Information Protection Act [online] (December 2021) https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/2nd-session/pipa/report/SCPIPA-Report_2021-12-06.pdf.
35. "Consultation: Ontario's Trustworthy Artificial Intelligence (AI) Framework". Government of Ontario. [online] (May 2021) https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations.
36. "IPC Comments on the Ontario Government's Consultation on Ontario's Trustworthy Artificial Intelligence (AI) Framework". Information and Privacy Commissioner of Ontario [online] (June 2021), https://www.ipc.on.ca/wp-content/uploads/2021/06/2021-06-04-ipc-comments-on-ai-framework.pdf. See also "Privacy and humanity on the brink", Information and Privacy Commissioner of Ontario (Blog Post), July 21, 2022, online at <https://www.ipc.on.ca/privacy-and-humanity-on-the-brink/>.
37. "Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy". Government of Ontario [online] (June 2021) https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462.
38. Final CANON Bill C-27 Working Group Document "Proposed amendments to de-identification and anonymization provisions in the Digital Charter Implementation Act, 2022 (Bill C-27)", December 7, 2022, online at <https://deidentify.ca/wp-content/uploads/2022/12/CANON-Proposed-Amendments-to-Bill-C-27-Dec-7-2022.pdf>.
39. "Declaration on Ethics and Data Protection in Artificial Intelligence" 40th International Conference of Data Protection and Privacy Commissioners. [online] (October 23, 2018) https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.
40. "International Declaration Highlights Privacy Issues Related to Artificial Intelligence" Office of the Privacy Commissioner of Canada. [online] (November 21, 2018) https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181121_01/.
41. https://opendatabarome "Minister Morneau Launches Advisory Committee on Open Banking" Department of Finance Canada. [online] (September 26, 2018) https://www.fin.gc.ca/n18/18-085-eng.asp.ter.org/country-detail/?_year=2017&indicator=ODB&detail=CAN.
42. https://www.ontario.ca/page/beta-principles-ethical-use-ai-and-data-enhanced-technologies-ontario.
43. https://www.ontario.ca/page/artificial-intelligence-ai-guidance#section-1.
44. https://opendatabarometer.org/.
45. https://ciostrategycouncil.com/standards/.
46. https://ciostrategycouncil.com/standards/.
47. The Montreal Declaration was document developed by AI researchers in 2017 at an AI conference in Montreal that outlined 10 principles of how ethics should guide the

deployment and development of AI. The ensuing document has been widely adopted and endorsed by the wider AI community.

48. Civil Code of Québec, see arts 1468, 1469 and 1473, CCQ-1991.
49. Civil Code of Québec, CCQ-1991, art. 1473.
50. https://www.theguardian.com/technology/2022/nov/14/tesla-autopilot-landmark-case-man-v-machine.
51. Civil Code of Québec, CCQ-1991, art. 1465.
52. https://www.canlii.org/en/ca/laws/stat/schedule-b-to-the-canada-act-1982-uk-1982-c-11/latest/schedule-b-to-the-canada-act-1982-uk-1982-c-11.html.
53. CCRA, available at: https://www.canlii.org/en/ca/laws/stat/sc-1992-c-20/latest/sc-1992-c-20.html.

* * *

Acknowledgments

The contributions of the following Osler colleagues are gratefully acknowledged: Matthew Zvan (Articling Student); André Perey (Partner, Emerging and High Growth Companies); Wendy Gross (Partner, Technology); Michael Fekete (Partner, Technology); Sam Ip (Partner, Technology); Andrew MacDougall (Partner, Corporate Governance); Chelsea Rubin (Associate, Competition/Antitrust and Foreign Investment); Kuljit Bhogal (Associate, Privacy & Data Management); and Colleen Morawetz (Knowledge Management Lawyer, Privacy & Data Management).

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

Simon's practice concentrates on outsourcing, other complex services arrangements and procurement. 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. He leads a team providing innovative legal services models to the firm's high-growth technology clients pursuing a wide variety of cutting-edge technology and business models, including FinTech, AI, data analytics, Blockchain, AgTech and eHealth. Simon has been lead counsel on projects across a broad range of industry verticals, including the technology, banking, pension, investment, healthcare, energy, telecommunication and retail sectors. He also advises on selling to governments.

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).

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, including advising such clients on infrastructure, application development, rewards programmes, data processing, and payment processing-related services and transactions. 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.

Sam Ip
Tel: +1 416 862 5955 / Email: sip@osler.com

Sam is a member of the Technology Group and his practice includes technology procurement, contracting, and other commercial and corporate matters, with a focus on advising clients on complex and thorny issues related to the use of data, AI, blockchain technology and open source software.

Sam is also a licensed professional engineer and was the co-creator of Osler's free open source tool, Osler Code Detect (https://www.osler.com/en/tools/code-detect) and regularly helps organisations comply with ambiguous provisions found in many open source licences, developing policies that are actually used by engineers, and the negotiation of various open source issues as part of licensing and M&A transactions.

Osler, Hoskin & Harcourt LLP

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

China

Peng Cai
Zhong Lun Law Firm

Overview of the development and regulatory trends in AI, machine learning & big data

In 2022, AI technologies and applications are being rapidly iterated and evolved in China, particularly in data- and capital-intensive industries, such as the connected-vehicle industry and the industry of online live-streaming marketing. At the same time, the government's strict control and regulation of the platform economy has also led to large Internet platforms having to slow down their development of AI business scenarios, and the profitability prospects of AI companies concerned with B2B services were worrying.

However, it is reassuring to note that in late 2022, there was a shift in national policy towards the platform economy and that several local governments have introduced policies to strongly support the development of the AI industry. In particular, the "ChatGPT wave" blew across the country in early 2023, causing a widespread discussion on AI and machine learning within Chinese society, which will surely boost the development of the AI and big data industry in China significantly.

At the legal regulatory level, China continues the regulatory posture of multiple regulators for the industry of AI and data. As far as regulators are concerned, the Cybersecurity Administration of China ("**CAC**") has become the main regulator in the AI and data sector, and is the sole regulator on related core matters, including outbound data transfer, record-filing of deep synthesis and algorithms.

At the same time, AI technology companies also face more record-filing and compliance obligations. In the deep synthesis industry, for example, users, developers and technology proponents are supposed to comply to a series of assessment and filing duties.

In 2022, China has also strengthened the examination, evaluation and supervision system of ethics in science and technology, with the Central Government promoting the fundamental goal of "developing science and technology for social good and safe agile governance", while also making specific requests to the life sciences, medical and AI industries to establish organisational bodies for every market player such as the "science and technology ethics committee". We also note that regulators in certain sensitive sectors, such as finance, have also proposed standards for ethical guidelines for finance technology.

In summary, we believe that the Chinese government and lawmakers have made data security and data compliance a "top priority", and that data-intensive industries such as AI and deep synthesis will continue to face significant and serious compliance challenges.

Focal point of legislation

Following the completion of the fundamental legal structure in the field of data laws in 2021, 2022 witnessed the sprouting up of subordinate laws. These laws provided a possible rule for businesses to manipulate their data property and technologies, as well as to fulfil compliance obligations and bypass the risk of illegality.

China's AI legislation in 2022

For AI technology, the topics of scientific and technology ("**sci-tech**") ethics and AI-generated content ("**AIGC**") have been prominent lately, and new regulations for these sectors are urgently needed.

Sector of technology ethics

Sci-tech ethics serve as the values and code of conduct when conducting scientific research, technology development and other sci-tech activities, and is critical assurance for fostering the healthy development of science and technology. In 2022, China introduced the first national-level guidance document, *Opinions on Strengthening the Governance of Scientific and Technological Ethics* ("***Sci-tech ethics Opinions***"), to regulate sci-tech ethics.

The *Sci-tech ethics Opinions* outline the principles of sci-tech ethics, including enhancing human well-being, respecting life rights, adhering to fairness and justice, managing risks appropriately and being open and transparent. It requests for the bar to be raised for ethical norms in important fields such as bioscience, medicine and AI, so as to provide guidance to sci-tech institutions and researchers in their endeavours. Furthermore, it mandates the technological ethics (review) committee for organisations engaged in AI-related activities or research on AI technology.

Following the *Sci-tech ethics Opinions*, the People's Bank of China issued an industry guideline, *Guidelines for Science and Technology Ethics in Financial Sectors*, to give financial institutions specific instruction on how to execute ethical governance of science and technology.

Sector of AIGC

With the popularity of ChatGPT, AIGC is a topic that presents hopes and concerns. The *Administrative Provisions on Recommendation Algorithms in Internet-based Information Service* ("***Recommendation Algorithms Provisions***") was published by China in 2021, sparking extensive discussion. The *Recommendation Algorithms Provisions* categorise five types of algorithms, namely personalised pushing technology, ranking and selection technology, retrieval and filtering technology, dispatching and decision-making technology, and generation and synthesis technology. The first four types of algorithms use the discriminant model, a decision-making AI model that analyses, judges and predicts based on available data. The discriminating model is frequently used for autonomous driving and intelligent recommendations (short videos). Tech giants including Alibaba, TikTok and Meituan rushed to deploy algorithm compliance work, especially algorithm filing.

In 2022, a new rule was introduced to prevent the misuse of generative AI: the *Administrative Provisions on Deep Synthesis in Internet-based Information Services* ("***Deep Synthesis Provisions***"). The essence of generative AI is an inhuman enhancement and development of productivity that places an emphasis on the creation and generation of new content after extensive learning and induction. The widespread adoption of AIGC technology is anticipated to significantly increase productivity in the domains of marketing, design, architecture and content.

The *Deep Synthesis Provisions* are drafted in an open-ended manner. In general, businesses using AI, algorithms and related technologies in B2C or B2B models may be covered.

The *Deep Synthesis Provisions* set obligations on businesses according to their identities as follows: deep synthesis services providers; technology supporters for deep synthesis services; and deep synthesis services users. Each type of business is subject to different obligations, with deep synthesis service providers having the strictest requirements.

Data legislation in 2022

In 2022, a number of supplementary legislations were published, making it practically possible for businesses to implement data privacy compliance.

The legislation on outbound data transfers

Outbound data transfer must have been one of the hottest issues in China in 2022. As a background, CAC established three pathways for the outbound transfer of personal information under the *Personal Information Protection Law* ("***PIPL***"): security assessment organised by the national cyberspace authority; certification of personal information protection by a third party; and standard contract. Implementing regulations issued in 2022 partially operationalised the three pathways.

- Pathway I: Implementing rules for security assessment

The *Measures for the Security Assessment of Outbound Data Transfers* ("***Measures***") were released by CAC in 2022. It set forth an explicit threshold for data processors who must submit a notification for security assessment. Given that the grace period for the notification expired at the end of February 2023, unsurprisingly, a considerable amount of notifications will have been submitted in 2023.

- Pathway II: Certification of personal information protection

In 2022, up to five patches of provisions on the certification of personal information protection were published, revealing the basic mechanism of the certification. According to the *Announcement on the Implementation of Personal Information Protection Certification* jointly issued by the State Administration for Market Regulation and CAC, certification of personal information protection will be granted in accordance with both the *Information Security Technology – Personal Information Security Specification (GB/T 35273)* and the *Specification on Security Certification of Personal Information Cross-border Processing Activities (TC260-PG-20222A)*. In other words, businesses must obtain two certificates in order to proceed through pathway II. We understand that the China Cybersecurity Review Technology and Certification Center is the authorised body that undertakes the certification job and that there are a couple of programs in progress.

- Pathway III: Standard Contract Clause ("**SCC**")

The draft version of SCC was once brought by way of CAC in 2022. While being a draft, it offers a useful template for the data processor. Many businesses have already embraced it by modifying concluding data-processing agreements for their own purposes.

The legislation on building basic systems for data

Based on the fundamental legal construction established in 2021, the legislative process exhibits two features in 2022:

Firstly, both central and local governments have advocated for data exploitation. The *"14th Five-Year Plan" for the Development of the Digital Economy*, published by the State Council at the end of 2021, clarified the development objectives for creating a market system for data factors. At the end of 2022, the Communist Party of China Central Committee and the State Council jointly released the *Opinions on Building Basic Systems for Data to Better Play the Role of Data Factors* ("***Opinions***"), elaborating specific measures to build basic systems for the utilisation and exploitation of data resources for the economic sector.

According to the *Opinions*, China's basic system for data will entail the establishment of a data property system, data exchange and trading system, data-factor income-distribution system and data-factor governance system to cope with the new challenges arising with data. In the meantime, local governments such as Beijing, Shanghai, Guangdong, and others also introduced rules or policies to support the growth of local data-based digital economy. Data exploitation will be tightly interwoven with societal and economic growth thereafter.

Secondly, the convergence of sectoral laws on data and data privacy was remarkable in 2022.

- **Antitrust**: Because of network effects, a multi-sided market and free strategy that characterise the platform economy, it is challenging to estimate the market power of platform businesses using conventional metrics such as sales value or sales volume under Antitrust Law. In order to address these issues, the Supreme People's Court promulgated the *Provisions on Several Issues Concerning the Application of Law in the Trial of Monopoly Civil Dispute Cases (Draft for Public Comment)* ("***Antitrust Provisions***") in 2022, in which data and algorithms were absorbed as one of the factors in assessing market power. The *Antitrust Provisions* account "data assets" as a calculation index, reflecting the impact of data as a new element in the market. In the interim, it is vital to find solutions to questions such as how to identify and calculate data assets, and how to determine the overall market size.
- **Anti-unfair competition**: The *Anti-Unfair Competition Law (Draft Amendment)*, promulgated in 2022, defines "commercial data" and establishes rules for its utilisation. The term "commercial data" refers to data collected by business operators in accordance with the law that has commercial value and for which appropriate technical management measures have been taken. The concept of commercial data is defined in the *Anti-Unfair Competition Law (Draft Revision)*. The definition of commercial data suggests that future regulations on data utilisation may distinguish between commercial and non-commercial data.
- **Credit record**: The requirements of the *Cybersecurity Law* and the *PIPL* on system-protection capabilities and personal information protection leaders are incorporated into the *Administrative Measures for Credit Reporting Business* which came into effect in 2022, and *PIPL* was designated as the higher norms. A personal credit reporting agency, for instance, must have Level III or higher security-protection capabilities, and the business must nominate senior managers to serve as the information security officer and the personal information protection officer.
- **Customer protection**: A chapter on "Protecting the Right to Consumer Information Security" is included in the *Administrative Measures for the Protection of Consumer Rights and Interests by Banking and Insurance Institutions* (2022), and it accurately reflects and strengthens the requirements of *PIPL*.
- **Anti-spoofing**: The *Anti-Telecom and Online Fraud Law* (2022) lists the types of information that may be used by telecom and online fraud, such as logistics information, transaction information, loan information, medical information, matchmaking information, etc. Public security agencies shall simultaneously confirm the source of the personal information when handling a telecom and online fraud investigation.

Legislative trends

Legislative trends on data protection

To respond to the growth of the data-sector market, 16 central departments jointly issued the G*uiding Opinions on Promoting the Development of the Data Security Industry* ("***Guiding***

Opinion"). The *Guiding Opinion* encourages accelerating cross-industry integration and innovation of data security technologies and emerging technologies, such as AI, big data and blockchain, and calls for advancing research on technologies like lightweight secure transmission storage, privacy compliance detection and data abuse analysis. It also calls for enhancing the capabilities of data security awareness and risk analysis.

Also, the highly anticipated *Regulation on Network Data Security Management* was not officially released in 2022. It will most likely be made available in 2023. As far as the draft version concerned, it will significantly affect the rules on platform accountability, the protection of sensitive data, cybersecurity evaluations, etc.

Moreover, following the discussion of outbound data transfer above, 2023 is predicted to see the introduction of more specific and feasible rules for Pathways II and III.

Legislative trends in the AI Industry

According to the working meeting of the Central Political and Legal Commission,[1] the justice sector also pays close attention to the emerging data market. The meeting proposed that all central political and legal units should strengthen their awareness of legislation, put forward legislative suggestions in a timely manner around emerging fields such as digital economy, AI and unmanned driving, and formulate and improve judicial interpretations. More directive documents and judicial interpretations are anticipated to be introduced in 2023, as the legal resources to solve the conflicts that arise in the development of the digital market.

Following the national industrial policy, some local governments have also issued AI industry promotion policies. The *Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations* and the *Shanghai Regulations on Promoting the Development of the Artificial Intelligence Industry* are the two most typical. It is foreseeable that more local rules will be drafted in 2023 to promote the deep integration of AI with the economy, life and urban governance, as well as to encourage the inventive development of AI.

Observation and outlook on law enforcement

Justice

Application of AI in trials

Due to COVID-19, numerous trials in 2022 were held online. China's judiciary system introduced the people's court online litigation rules, online mediation rules, online operation rules and the *Opinions of the Supreme People's Court on Strengthening Blockchain Applications in the Judicial Field* to assist the ordinary running of the online trials.

In addition, at the end of 2022, the Supreme People's Court published the *Opinions on Regulating and Strengthening the Applications of Artificial Intelligence in the Judicial Fields*, with the goal of advancing the comprehensive integration of AI with adjudication and enforcement, litigation service, court management, as well as social governance facilitation. By 2025, China aims to build a more advanced functional system for the use of AI in the legal system, which will significantly reduce judges' heavy administrative workload.

Cases: Controversy judgments on the copyright of AIGC in China

A contentious debate has sparked worldwide on the copyright of AIGC. To discuss the topic in China, two crucial points shall be addressed as a prerequisite:

- China's copyrights only recognise creative works completed by natural persons, and content created and completed by non-natural persons is generally not identified as copyrighted works.
- Whether AIGC works are unique. Considering that AI fundamentally generates "new works" on the synthesis of existing data through the design of algorithms, models and

rules, without human intervention or little intervention, it is debatable whether AIGC works have been created with uniqueness in the literary, artistic and scientific fields.

Two judgments with diverse opinions have emerged in China's judicial practice. In a case involving Wolters Kluwer, China's famous legal database, the court believed that written works shall be created by natural persons. AIGC work lacking unique expression of the thoughts and emotions of either software developers or users does not have copyright attributes. As such, the legal analysis report generated through Wolters Kluwer is not protected by copyright.[2]

In another case concerning an AI news writer, the court held the view that software can never run automatically. The expression of the AIGC works is determined by the personalised choice of the software development team. It is the contribution of the software development team to determine the form of expression. Therefore, the AIGC news in question constitutes written works protected by China's Copyright Law as literary work.[3]

Administrative enforcement

Apps governance campaign

The year 2022 marked the fourth year of the app governance campaign in China. Apps, as the most easily perceivable Internet product, always draw great concern by the authorities. In addition to the central regulators, local governments such as Beijing, Shanghai and Guangdong also joined the campaign in 2022. Under strict oversight by multiple national departments, the personal information protection of leading apps has been improved steadily, while the trailing apps appear to lack motivation to achieve the requirement due to compliance costs.

The app enforcement campaign is anticipated to continue in 2023, with the aim of gradually shifting from standalone apps to software-development kits ("**SDKs**") and mini-programs.

Administrative power of CAC

In 2022, CAC published the *Provisions on Administrative Law Enforcement Procedures of Cyberspace Administration Departments (Draft for Comments)*, specifying the scope of administrative law enforcement of CAC expands from singular Internet information content to areas such as cybersecurity, data security and personal information protection, which to a certain extent solves the administrative jurisdiction conflicts among governmental departments in the field of cybersecurity and data privacy. In 2023, a more distinct division of administrative authority is anticipated.

Supervision on IPO

The listing market also showed concern for AI and big data regulation in 2022. Notably, many AI industry companies provided a very specific introduction to the AI mechanism and its commercial use, including data processing, cleaning and management capabilities, algorithm capability, training and reasoning.

In the meantime, regulatory attention has also been paid to the subject of data trade and data rights ownership. This has nearly always come up throughout their IPO process, especially for big data businesses.

Without question, data compliance issues will have a greater impact on a successful IPO as data governance becomes more significant.

Changes in legal liability

Draft amendment of Cybersecurity Law

In September 2022, CAC, together with relevant departments, drafted the *Notice on Seeking Public Comments on the Decision on Amending the Cybersecurity Law of the*

People's Republic of China (Exposure Draft) ("***Exposure Draft***"). The *Exposure Draft* mainly improved the legal liability system, consolidated the legal liability regulations and intensified the administrative penalties as follows:

- The *Exposure Draft* adjusted the maximum amount of fines for violations from the original CNY1 million to CNY50 million or 5% of the turnover of the previous year, which greatly increased the range of fines.
- The *Exposure Draft* added the legal liability of "employment prohibitions" for the person in-charge. The amendment not only raised the maximum fine imposed on the person in-charge to CNY1 million, but also granted the competent department the right to prohibit the direct person in-charge from engaging in any business activities for a certain period of time in serious administrative penalty cases. On one hand, the newly added legal liability can effectively urge the person in-charge to perform his/her duties with due diligence in cybersecurity management and operation; on the other hand, it can enhance the cybersecurity awareness of the person in-charge and improve the overall cybersecurity management level of network operators.

DiDi Global Inc. ("**DiDi**") case

On July 21, 2022, CAC issued an announcement of an administrative penalty decision against DiDi in accordance with the law, for its violations of the *Cybersecurity Law*, the *Data Security Law* and the *PIPL*, imposing a fine of CNY8.026 billion on DiDi, and a fine of CNY1 million each on both of the direct persons in-charge of DiDi. This is the first administrative penalty decision made by CAC in accordance with the *PIPL*.

In this case, Didi's illegal activities mainly included:

- **Violations of the *PIPL***: Excessive collection of personal information, mandatory collection of sensitive personal information, frequent right claims by the app and failure to fulfil the obligation to inform about the processing of personal information.
- **Violations of the *Cybersecurity Law* and the *Data Security Law***: The existence of data-processing activities that posed serious risks to the security of the country's critical information infrastructure and data security.

The heavy fines in the DiDi case have aroused widespread concern in society and sounded an alarm for the compliance of platform companies, warning them that they should fulfil their data compliance obligations in accordance with the requirements of relevant laws and regulations. The legal basis for CAC to hold DiDi liable is specified as follows:

- **Fine against DiDi**: The amount of the fine imposed by CAC on DiDi is mainly based on the relevant provisions in the *PIPL*, which imposes on the relevant entity a fine of less than 5% of its turnover of the previous year. Considering the seriousness of its violation, however, CAC imposed a heavier penalty on DiDi.
- **Fines against the person in-charge of DiDi**: The *Cybersecurity Law*, the *Data Security Law* and the *PIPL* all stipulate that the competent department has the right to fine the person in-charge; therefore, CAC imposed a maximum fine against the principal person in-charge of DiDi.

Accountability and immunity of platform algorithm

Big data and AI algorithms are complementary to the platform economy. In order to ensure the sound development of the platform economy, China has also made special provisions for the utilisation of algorithms by platform companies in 2022:

- **General provisions**: According to the *Recommendation Algorithms Provisions*, platforms shall be held legally liable if the algorithms they use do not comply with the codes of information services or infringe on the rights and interests of users, or

fail to fulfil the record-filing obligations, conduct false record-filings or fail to conduct algorithm security-assessments and fall under other circumstances in violation of compliance obligations.

- **Personal Information Protection sector**: According to the *PIPL*, platforms shall be held legally liable if they fail to ensure the transparency of algorithmic automatic decision-making and the fairness and impartiality of the results thereof, or if they use the algorithm to treat individuals in a discriminatory manner in terms of transaction conditions.
- **E-commerce sector**: According to the *E-commerce Law*, the legitimate rights and interests of consumers shall be respected and equally protected if the platforms use algorithms to provide search results of goods or services to consumers; otherwise, the platforms shall be held legally liable.
- **Antitrust sector**: According to the *Antitrust Law* and the *Antitrust Guidelines of the Antitrust Commission of the State Council on Platform Economy*, the platforms shall be held legally liable if they use algorithms to reach and implement a monopoly agreement and carry out algorithm-based discrimination.
- **Anti-unfair competition sector**: According to the *Anti-Unfair Competition Law (Draft Amendment)*, the platforms shall be held liable if they use algorithms to engage in unfair competition, infringe the rights and interests of users or other operators, and disturb the fair competition order on the market.

In addition, "technology neutrality" is a common defence when it comes to the use of platform algorithms. However, there are cases in that platforms should assume a higher duty of care for algorithm recommendation services, thus requiring the platforms to undertake the joint liability of infringement. Platform companies should effectively fulfil their compliance obligations, such as algorithm record-filing and algorithm security review, implement the responsibilities of entities for the algorithm security, and regularly review and evaluate the mechanism, model, data and application results of algorithms to reduce the risk of bearing legal liability.

From "preventing the disorderly expansion of capital" to "supporting development while normalising supervision", China has undergone a significant policy change in terms of platform governance by the end of 2022. Therefore, we believe that in 2023, the standard of regulation on the platform will change from "strict" to "normal", and the corresponding law enforcement standards and legal liabilities will also undergo some changes.

* * *

Endnotes

1. http://www.cac.gov.cn/2023-01/10/c_1674989052657262.htm.
2. (2019) Jing 73 Min Zhong No. 2030.
3. (2019) Yue 0305 Min Chu No. 14010.

Peng Cai
Tel: +86 10 5087 2786 / Email: caipeng@zhonglun.com

Peng Cai is an equity partner of the firm. His practice focuses on cybersecurity, data protection and intellectual property. He provides legal services to various industries, including TMT, manufacturing, finance and healthcare. With his deep involvement in legislation and extensive practice, he is dedicated to helping clients solve pressing challenges such as data and privacy, cybersecurity under strict supervision, IPOs, digital transformation, AI and metaverse, etc.

Mr. Cai is adept at mitigating data-security risks and tackling compliance challenges brought about by the Internet, big data and AI technologies. His expertise extends to areas including management of network security risks and data security, compliance management throughout the lifecycle of data, identification and control of personal information and privacy risks, design of compliance schemes for the cross-border transfer of data, design of global compliance schemes for data privacy, prevention of and response to data incidents, and advice for data audit for various businesses.

Zhong Lun Law Firm

22-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing100020, China
Tel: +86 10 5957 2288 / URL: www.zhonglun.com

Finland

Erkko Korhonen, Samuli Simojoki & Jon Jokelin
Borenius Attorneys Ltd

Trends

Finland was among the first countries to launch a national Artificial Intelligence Programme in 2017, whose objective was to shape Finland into a global leader in the application of artificial intelligence (AI). Finland has set itself a goal to become a trusted and safe pioneer in the field of digital economy by 2025. Finland is currently in a position to achieve its goal as a global trendsetter and forerunner within the EU in the creation of fair, consumer-oriented principles in the use of AI. This will be achieved by constructing a strong and distinctive digital economy where establishing close co-operation between the public and private sectors is of paramount importance.[1]

The Finnish Ministry of Economic Affairs and Employment has recognised the need to focus on retaining and attracting the top talent in the field. Finland is known for its highly motivated research groups that focus on emerging sectors, such as unsupervised learning, a vibrant start-up field and close co-operation between research institutions and companies. Additionally, the Finnish Center for Artificial Intelligence (FCAI) plays a large role in the process of enhancing Finland's strengths. The above-mentioned points have also been recognised as some of the strengths that should be marketed to the rest of the world.[2]

The goal set by the Finnish Government for the immediate future is for Finland to become known as a country where the opportunities offered by digitalisation and technological development are made full use of and implemented across administrative and industry boundaries. The aim is to increase the technological capacity of the public sector and to further develop public–private partnerships.[3] This includes addressing and creating a balance between the interests of individuals, companies and society in the use of new technology and AI in an innovative and ethically sustainable manner.[4]

In late 2020, the Ministry of Economic Affairs and Employment of Finland appointed a steering group to prepare an action plan for Finland to speed up the introduction of AI and to promote the so-called "fourth industrial revolution". The Artificial Intelligence 4.0 programme focuses on promoting the development and introduction of AI and other digital technologies, targeting SMEs in the manufacturing industry in particular. The final report of the programme, published in December 2022, identifies 11 concrete measures which aim to make Finland a frontrunner in twin transition by 2030.[5]

Another recent Government initiative in AI is the National Artificial Intelligence Programme, AuroraAI, which commenced in 2020 and was successfully completed in late 2022. The main output of the project was the AuroraAI network, an AI-powered technical solution that enables information exchange and interoperability between different services and platforms.[6]

The main piece of legislation within AI-related regulation is the proposal on the harmonised rules on AI and amending certain Union legislative acts (COM/2021/206 final, the "Proposal"). In its Proposal of 21 April 2021, the Commission proposes a legal framework to establish a European approach and to promote the development and deployment of AI for the protection of the public interest; in particular, health, security, and fundamental rights and freedoms. The Proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market.[7]

The Finnish view of the developmental steps of AI-related regulation in the EU has been broadly positive and the Finnish Government has supported the European-level initiatives for the most part. In late 2021, the Finnish Government published its first memorandum pertaining to the Proposal. In its memorandum, the Finnish Government expressed its strong support for the responsible development of AI in Finland and in Europe. In its observations, the Finnish Government gave emphasis to the perspective of fundamental rights in the use of AI-related systems. The Government noted that – when correctly used – AI solutions may enhance and contribute to the realisation of fundamental rights. However, it was acknowledged that there are still some unanswered questions in this context. For this reason, the Finnish Government considers it important to diligently assess the scope of applicability from the perspective of fundamental rights.[8]

The Finnish Government's view of the latest proposed amendments to the European AI regulation were presented in another memorandum in October 2022. Perhaps most importantly, the memorandum raised concerns about the definition of AI. Finland's aim is to exclude systems that automatically apply human-defined rules and operating instructions without exercising discretion or changing their operating logic from the scope of regulation. Furthermore, Finland considers it to be important that regulation on experimentation and testing of AI systems in real-life conditions is genuinely enabling, supports innovation and does not create disproportionate barriers to the AI systems' market entry.[9]

In 2023, the first legal provisions on AI-related liability were introduced in Finland. Regulation on public authorities' automated decision-making imposes the liability on the authority that uses automated decision-making tools. The regulation does not extend to civil liability yet, but still the new regulation can be seen to be progressive as it deviates from the valid EU laws. This topic is discussed in more detail below.

While AI is primarily seen as an opportunity for Finland, the concern of AI safety has also been acknowledged on a national level. One example of this is the Avoiding AI Biases project that formed part of the implementation of the 2021 Government plan. The project mapped the risks related to fundamental rights and non-discrimination involved in machine learning-based AI systems that are either currently in use or planned to be used in Finland. The mapping revealed that algorithmic discrimination has attracted reasonable attention, at least in the public sector. Based on the mapping carried out during the study, the researchers developed an assessment framework for non-discriminatory AI applications. The framework helps to identify and manage the risks of discrimination and to promote equality in the use of AI.[10]

In addition to the big data aspects, Finland might have the opportunity to become a pioneer in the field of "small data", where AI can be used even with a small amount of data. A current trend is to research and create more reliable and understandable technologies that

use less data, energy and computation.[11] Future opportunities lie in the B2B market, which has yet to be fully conquered. In the business sector, Finland could invest in the B2B market, which is twice as large as the B2C market. Therefore, in the future, Finland could develop small data AI solutions at the global frontlines while recognising the potential of the B2B market and developing solutions for using data in the market.[12]

The AI sector is striving to expand the interactive ecosystem in Finland. However, the funding is a big challenge. For example, the FCAI receives flagship funding intended for carrying out basic research, but it is not enough to run the ecosystem itself.

Ownership/protection

Protecting an AI algorithm in Finland

Traditionally, copyright has been considered the main safeguard for, e.g., software. For example, computer programs are primarily protected by copyright in Finland, but this protection is afforded, in practice, only to the expression of the computer program itself (i.e., its code).[13] On the other hand, algorithms are not, in principle, protected by copyright to any extent in Finland, regardless of the fact that they could be the sole reason for the existence and development of a computer program in the first place and contain inventive ideas and abstract principles. In fact, copyright does not efficiently prevent competitors from putting their own spin on an algorithm, which could, in principle, then result in any gained competitive edge crumbling to nothing.

As such, given the fact that copyright is not a fully effective means of protection for AI algorithms, the two other potential options that remain for their protection in Finland are the protection afforded to them as trade secrets or patenting them. Companies should therefore be aware that computer-implemented inventions can sometimes be patentable under the European Patent Convention and that, as such, this umbrella of protection can potentially be extended to cover an AI algorithm implemented via a computer program.

In order for this to be the case, however, the relevant computer program must have a further technical effect in addition to fulfilling other conditions, and such further technical effect needs to go beyond the normal function of the computer. Determining and assessing the technical effects that result from the use of the computer program (such as the ability to control a specific technical process with the use of AI) is therefore of key importance here.[14] In reality, AI algorithms can play a crucial role in solving several different technical problems. For example, the computational efficiency of an AI algorithm affecting the established technical effect can contribute to the technical character of the invention and thus to inventive step.[15]

AI algorithms generally have commercial value, and, in reality, the most valuable part of the computer program is often the algorithm.[16] Pursuant to the Finnish Trade Secrets Act (595/2018), which is based on the Trade Secrets Directive implemented in 2016, a trade secret is information that: 1) is confidential; 2) has commercial value due to its confidential nature; and 3) is subjected to reasonable measures to ensure its confidentiality. In the event that any information regarding an AI algorithm that is in the possession of a company meets these conditions, which could be relatively often, the relevant algorithm is protected as a trade secret regardless of how it is implemented or expressed (compared to the other forms of protection discussed above).

The Act also introduces the concept of a technical instruction. This concept is unique to Finnish law and is not based on the Directive. A technical instruction is a technical guideline or operations model that can be used in the course of business, and an algorithm

can also be considered to constitute a technical instruction.[17] The protection afforded to technical instructions is, in practice, triggered when the relevant technical instruction is disclosed confidentially in certain circumstances. If a party has been disclosed an algorithm confidentially in these circumstances, they are not permitted to use or disclose it further without authorisation. Therefore, even in circumstances where an AI algorithm is not, for one reason or another, afforded protection as a trade secret, the algorithm may be protected as a technical instruction and, as such, companies may consider utilising this concept in their IPR strategies.

What intellectual property issues may arise regarding ownership?

In the above-mentioned situations, companies must always keep in mind that the forms of protection cannot always be combined. Choosing between patenting an algorithm or protecting it as a trade secret, for example, is crucial since both forms of protection cannot always be employed at the same time. The fact that patent claims must be published, in actuality, could mean that an algorithm can no longer be considered to constitute the company's trade secret as it has been disclosed to the public and has consequently lost its confidential nature.

When it comes to patents, aspects such as the complex patenting processes and judicial proceedings that the algorithm might have to undergo, as well as the fact that the logic underlying the algorithm itself will become exposed, pose a real risk, especially for small and medium-sized enterprises, in a world where state borders do not play a significant role and where competitors can draw inspiration from the disclosed AI algorithm or potentially choose to ignore the patent itself. Infringements in general can be exceptionally difficult to detect and when a computer program is, e.g., stored in a cloud, it can be practically impossible for third parties to inspect the AI algorithm underlying the relevant computer program.

On the other hand, the protection that can be afforded to an AI algorithm as a trade secret can also become jeopardised, e.g., in situations where information regarding the AI algorithm must be disclosed pursuant to mandatory law.

The ownership of data

In addition to choosing the best form of protection available for their AI algorithms, it is at least equally important for companies to protect the data in their possession in one way or another, as AI and, consequently, machine learning require a significant amount of data in order to learn and develop. AI assigns a meaning to specific data sets when it produces information based on the said data. Another special consideration is that the data processed by AI can in itself be divided into personal and non-personal (or industrial) data.

However, there is no specific form of protection available for data in general in Finland, although data definitely has a significant impact on companies' business operations and, in more general terms, on the changes that are happening in the so-called "Industrial Internet". Companies do, naturally, strive to "own" or otherwise control the use of data in Finland as well. In this respect, one can note that when discussing the "ownership" of specific data, it could be more relevant to consider data to be subject to various kinds of rights of use, instead of it being considered something an entity can own, as was established in a fairly recent publication from the Finnish Ministry of Finance.[18]

In the absence of a specific form of protection, data can be protected, e.g., under copyright in the form of database protection rights or alternatively as a trade secret in Finland as discussed above. In addition, data may be protected with agreements. However, since copyright

protection for data is exceedingly arguable, and, for instance, the *sui generis* database right covers the arrangement of the contents of a database instead of the actual contents of the database, Finnish companies do, for the most part, strive to establish protection for their data as trade secrets or otherwise under contractual or technical arrangements.[19] One downside of contractual protection is that contracts can generally only provide protection *inter partes* and, thus, cannot bind any third parties.

Unlike with patents and copyright, the protection afforded to trade secrets is unlimited in duration, and trade secrets themselves can provide, in principle, a wider scope of protection for a company's data as a whole without the need to define exactly which assets are subject to protection. However, trade secrets also involve issues that relate to the potential disclosure of data and the inapplicability of trade secret provisions in the modern data industry.[20]

It is also relevant to question whether this kind of legal development that places so much emphasis on trade secrets supports the general goal of industrial and intellectual property rights, which is to foster innovation and the free flow of data in the EU. If data remains unavailable to other market operators, AI technology cannot be developed and improved as easily, in which case the market may become concentrated and competition may actually decrease.

The legal status of the "owner", or more appropriately in this context, the *holder* of data will be affected by the eventual adoption of the proposal for harmonised rules on fair access to and use of data (COM/2022/68 final, "Data Act"). The proposal for Data Act introduces a number of obligations on data holders, e.g., the obligation to make available or share data to users, third parties and authorities. The proposal for Data Act is currently pending in the EU legislative process and is expected to be enacted during the latter half of 2023.

Antitrust/competition laws

What happens when machines collude?

Over the last few years, there has been a lot of discussion surrounding cartels where the use of AI algorithms harmfully affects the pricing decisions made by companies, giving rise to collusion in the market. One of the key legal questions is whether the use of algorithms will result in a change in competition law, and if so, how, e.g., pricing algorithms should be regulated and which measures should be taken. In this context, we will discuss collusion caused by algorithms briefly in light of a recent report published by the Finnish Competition and Consumer Authority (the FCCA), which reflects the existing guidelines that are based on the latest developments in Finland.[21]

Firstly, the FCCA's report covers situations of explicit collusion, i.e., situations where anti-competitive conduct is carried out with the use of an algorithm, but the restriction of competition itself can be proven on the basis of an agreement concluded between the parties or a concerted practice.[22] Secondly, the report discusses collusion that relates to pricing services, which is somewhere in between explicit and tacit collusion in terms of severity. In these situations, competing companies apply the same pricing algorithm provided and maintained by a third service provider, which may lead to the creation of so-called hub-and-spoke cartels. The FCCA's report emphasises that, as the communication required by this kind of collusion takes place in a vertical relationship with the service provider, the lack of communication between competitors, in particular, poses a challenge in recognising and intervening in this kind of collusion.[23]

Thirdly, the report covers tacit collusion, i.e., algorithmic collusion. In these situations, the potential negative impact on competition is not based on the conduct of, e.g., the competing

corporations or that of the service provider mentioned above, but rather on the independent function of the algorithm. Pursuant to the FCCA's report, this kind of collusion can involve competitors using compatible algorithms when setting their prices, which can then result in their pricing becoming very similar without the competitors actually concluding any agreement or engaging in any concerted practice.[24]

These situations of tacit collusion are the most interesting and challenging when it comes to assessing them from the perspective of competition law, as current competition provisions do not apply to algorithmic collusion as such, due to the lack of communication between the competitors involved. Recognising, proving and investigating collusion in these cases therefore involves not only problems caused by, e.g., the complexity of the technology involved, but also problems relating to the current inapplicability of competition law provisions and interpretation practices.

As such, the key legal question at hand is how to intervene in tacit collusion caused specifically by, e.g., pricing algorithms. The FCCA's report does, in this respect, e.g., offer some criticism of the earlier suggestion that algorithmic collusion could be assessed from the perspective of competition law-based price signalling.[25] The report gives the impression that the FCCA emphasises that, going forward, what will be crucial is determining whether the aforementioned kinds of collusion can be intervened in by directing interpretation practices at the EU level or, alternatively, directly through law. Dealing with algorithms requires careful consideration in terms of selecting the right approach under competition law. As such, various different entities, such as companies, competition authorities, operators within the field of information technology and lawyers, should engage in active co-operation to establish a solution together.[26]

Board of directors/governance

The good corporate governance of listed companies is regulated in Finland by a combination of laws and decrees, including self-regulation and other best practices.

In the autumn of 2020, the Finnish Prime Minister's Office published a study on potential reforms to the Finnish Limited Liability Companies Act (624/2006) in terms of enhancing competitiveness. The purpose was to assess and identify whether the current regulatory framework is compatible with the changing digitalised business environment and whether amendments are required to update relevant legislation and to recognise options for "streamlining company law procedures". It was concluded that, in general, the Act is well equipped for adapting to the changing digitalised business environment and that there is no immediate need for overall reform.[27] The above-mentioned Act lays down the framework for companies' organisation and operative arrangements by establishing strong principles to be followed in their operational environment. Another central feature is its extensively non-mandatory nature. As a consequence, many of the provisions of the Act are default provisions and companies can, while observing certain restrictions laid down by law, depart from these provisions.

Although no need for comprehensive reform was found, the Act currently contains few provisions on digital practices, although these are generally utilised in corporate life. In order to clarify the legal situation, the addition of a general clause on digital practices was suggested. The objective is to further develop the regulation in a more technology-neutral direction and to clarify the use of digital procedures as an alternative approach.[28] The suggested amendments to the Act include, e.g., the possibility of digitising shares and the amendment of certain requirements regarding written-form and physical meeting places.

Regulations/government intervention

In 2019, the Finnish Government requested a group of experts to conduct a study on the potential of AI in the national regulatory environment, especially in support of public authorities' decision-making.[29] On this basis, the Government began to work on the preparation of legislation on automated decision-making in public administration, which entered into force in early 2023. The new legislation will clarify the old sector-specific, fragmented legislation.

The purpose of the regulation is to enable public authorities' automatic decision-making while also ensuring the legality of decisions and actions. Currently, EU legislation prohibits automated decision-making concerning natural persons, so the new Finnish legislation derogates from the EU law in this respect.[30]

The most significant changes to the old legislation are the new chapters on automated decision-making in the Administrative Procedure Act and the Act on Information Management in Public Administration. Under the Administration Procedure Act, an authority may make an automated decision on a case that does not involve matters which, in the Authority's prior discretion, would require a case-by-case assessment. It is essential to note that automatic decision-making tools would therefore not use discretion in decision-making. Thus, in that sense, the reform of the law does not allow for the use of overly advanced AI. Decision-making can therefore be automatic, but not autonomous. The Act on Information Management in Public Administration addresses liability issues. As was the case already before the new legislation, pursuant to the new chapter in above-mentioned Act, a machine or AI cannot be held legally responsible for its decisions. Automated decision-making must be treated as an instrument or tool for which the user is ultimately responsible. The long-lasted discussion on the liability issues relating to the use of AI has therefore come to a conclusion, for now, and this principle made its way to legislation.

AI is constantly enhancing the efficiency of most public services. Despite the new legislation, Aalto University's inclusive research project in which the aim is to help the state and municipalities in the Helsinki Metropolitan Area to develop reliable and safe applications based on AI and to comply with future EU regulations is still highly relevant. The purpose of the research project (Civic Agency in AI) is to enhance all AI tools used by the city of Helsinki.

The aim of the researchers is to present their work to both the Finnish Government and the EU, and ultimately to influence policy. The research project will be conducted by way of interviews, workshops and other suitable ways of gathering research material. The project has been funded for four years.[31]

Ethical issues have also played a central role in the dialogue revolving around AI and digitalisation in Finland, key topics being the protection of privacy, accountability for errors made by AI systems and the traceability and transparency of algorithm-based decision-making.[32] However, AI-related ethics should not only be seen as a factor that poses limitations on operations – it should also be viewed as a factor that increasingly creates opportunities.[33]

AI in the workplace

Digitalisation has also been considered to relate strongly to employment in Finland. Pursuant to a publication compiled by the Ministry of Economic Affairs and Employment, confidence and trust in the importance and significance of data as a source of growth have

remained strong among Finnish companies despite the challenges posed by the digitalisation process especially during the global pandemic.[34]

A good example of the opportunities created by AI and automation is the Industrial Internet, which can be used by companies in different industrial sectors to improve and optimise their operations. Today's industrial machinery is constantly generating data which, together with data from customers, can be used to optimise production volumes, for example. When all of this happens automatically, it may affect the position of the employees that perform the same tasks. This also creates a whole new set of opportunities for cloud service providers to offer companies data pools for such uses.[35]

It can be considered obvious that new AI applications that are developing at a rapid pace – such as the new version of OpenAI's ChatGPT – will have an impact on working life and replace jobs. However, at the time of writing, there are no concrete examples of this at the national level. Nor has the Government issued any policy or regulation so far on the use of AI in the workplace or how to limit it.

Civil liability

In September 2022, the European Commission issued a proposal for a Directive on adapting non-contractual civil liability rules to AI (AI Liability Directive),[36] which aims to make it easier to hold the tortfeasor liable by applying a reversed burden of proof in situations where it is difficult for the injured party to prove a causal link to the damage caused by AI. The AI Liability Directive also obliges the Member States to ensure that the courts are empowered to order a pretrial discovery on relevant evidence when a specific high-risk AI system is suspected of having caused damage. The Directive does not interfere with the national law in terms of who can be held liable for damage caused by AI, but it aims to prevent the AI user from hiding behind the AI they have used to avoid liability.[37] At the time of writing, the Directive is not yet in force and no national legislation has been adopted on its basis. As is the case with administrative decisions, liability cannot be legally attributed to the algorithm itself in Finland, even in a situation where the algorithm is the direct cause of the damage, as the legal entity doctrine has not been extended beyond natural and legal persons. For example, in most cases, a doctor is responsible for any diagnosis and treatment given, so in this respect the responsibility of the involved algorithm in decision-making itself is disregarded. Also, with regard to the activities of the authorities, even if the algorithm makes an actual administrative decision completely independently, the liability will lie with the official.[38, 39]

Criminal issues

The fundamental principles of Finnish criminal law are markedly tested when an AI robot or system directly commits a crime. This has been emphasised in a relatively recent publication which, in the context of the above, considers the criminal liability of an official.[40] By way of background, under the Criminal Code of Finland (39/1889), the criminal liability requires, in principle, that the crime has been committed intentionally or negligently. In the context of algorithmic decision-making, the emergence of criminal liability therefore requires a certain link between the official and the AI decision-making process, but the problem is that in AI-based solutions, even the system developer may not necessarily be able to determine what the AI-produced conclusion is based on, and therefore, in particular, officials in charge are simply not always able to monitor and familiarise themselves with the decision-making process of the AI. Thus, if AI directly "commits a crime" in Finland,

the AI algorithm itself cannot be held liable in the current legal situation, but the legal entity behind the algorithmic decision-making can be held liable, although as stated, for example, the relevant official must be firmly identified.

Discrimination and bias

Although specific legal frameworks or other guidance on AI algorithms are still awaited as clarified above, the Finnish Non-Discrimination Ombudsman can be mentioned as one of the more active parties in this regard in Finland. The Non-Discrimination Ombudsman has given its opinion and recommendations on discrimination caused by automatic algorithmic decision-making, which can most certainly be considered an error in the operation of the algorithm. Also, the Finnish Deputy Data Protection Ombudsman has addressed the possible discriminative issues in relation to automated decision-making in its decision on a predictive healthcare tool. The decision pertains to a tool that is designed to find and refer for treatment patients whose treatment should be specified. The Deputy Data Protection Ombudsman raises concerns that the algorithm might discriminate against patients who are excluded from specific proactive healthcare interventions based on the profiling performed by the algorithm.[41]

The Non-Discrimination Ombudsman has clearly stated that the Finnish Non-Discrimination Act (1325/2014) also applies to the use of AI. The Non-Discrimination Ombudsman takes into consideration the important findings related to AI-based discrimination, which is that when using AI technology, even without the authors or users intending or wishing it, AI may still indirectly end up producing discriminatory conclusions by combining (personal) data. In line with the current legal situation, the Non-Discrimination Ombudsman states on the issue of liability that the parties responsible for AI systems and the parties using them (such as public authorities, service providers and employers) are always responsible for ensuring that their activities are in accordance with the Finnish Non-Discrimination Act; thus, from this point of view, ensuring the appropriate conduct lies within the responsibility of the human behind the algorithm in Finland.[42]

However, as we are reminded of in the Finnish Innovation Fund Sitra's report, if AI-related systems are built to a high standard and impact assessments are properly carried out, and the AI systems are also frequently monitored, AI can make a significant contribution in achieving equality by basing decision-making on the premise of objectivity. Therefore, legislative requirements relating to equality in fact necessitate that data structures must be error-free and sufficiently comprehensive. In addition, accessibility is emphasised. However, despite the fact that decision-making is "outsourced" to AI, the authority should ensure that citizens still have equal access to services (i.e., maintaining traditional services alongside AI solutions, where necessary). In Finland, it should be noted that language requirements and the principle that services should be provided in both national languages may pose substantial difficulties in this context.[43]

The project called "Avoiding AI biases: a Finnish assessment framework for non-discriminatory AI applications" has developed an assessment framework for AI applications to be used in the Finnish Government's analysis, assessment and research activities. The purpose of the framework is to help to identify and manage the risks of discrimination, especially in public-sector AI systems, and to promote equality in the use of AI.[44]

National security and military

In 2020, the Finnish Ministry of Defence published its own Strategic Guidelines for Developing AI Solutions. The publication summarises the AI-related objectives in five

strategic guidelines: 1) the strategic level of defence administration plans for all aspects of digitalisation should be compatible and aligned; 2) research, development and maintenance of AI capabilities ought to be procured and resourced in an agile manner in order to realise the performance potential of rapid technological development; 3) in developing AI capabilities, critical competences are secured through recruitment and staff training as well as a network of AI partners; 4) the defence administration will develop an up-to-date technical infrastructure for the promotion of AI applications and identifies which data must be available; and 5) the defence administration complies with international legal and ethical obligations that are binding on the administrative branch in the construction and use of AI and participates actively in the drafting.[45] However, in its memorandum on the EU Act on Artificial Intelligence, the Finnish Government emphasises that AI systems developed and used for military purposes should be excluded from the scope of applicability of the Act.[46] The main AI policies in the administrative sector are based on the current Government Programme, the Government Defence Policy Report and the Government Resolution on Securing the Finnish Defence Technological and Industrial Base.

* * *

Endnotes

1. Leading the way into the age of artificial intelligence: Final report of Finland's Artificial Intelligence Programme 2019, publications of the Ministry of Economic Affairs and Employment 2019:41, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=y), p. 120, April 2021.
2. *Ibid*. p. 37 *ff*.
3. *Digitalisaation edistämisen ohjelma 2020–2023*, *Toimintasuunnitelma 2021* (in English: *The Programme for the Promotion of Digitalisation for the years 2020–2023, Action Plan 2021*), the Finnish Ministry of Finance VN/714/2020, available in Finnish at (https://vm.fi/documents/10623/30029448/Digiohjelman+toimintasuunnitelma+2021.pdf/5cdfa466-afd9-5175-9139-46958d4526c8/Digiohjelman+toimintasuunnitelma+2021.pdf?t=1614692585521), p. 3, April 2021.
4. Leading the way into the age of artificial intelligence: Final report of Finland's Artificial Intelligence Programme 2019, Publications of the Ministry of Economic Affairs and Employment 2019:41, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=y), p. 120, April 2021.
5. Artificial Intelligence 4.0 programme, Finland as a leader in twin transition – Final report of the Artificial Intelligence 4.0 programme, Publications of the Ministry of Economic Affairs and Employment 2022:63, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=y), March 2023.
6. Publication on the website of the Finnish Ministry of Finance, available in English at (https://vm.fi/en/national-artificial-intelligence-programme-auroraai), March 2023.
7. Proposal for Artificial Intelligence Act. (https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF) pp 2–3, March 2023.
8. Statement of the Finnish Government U 28/2021 vp, available only in Finnish at (https://www.eduskunta.fi/FI/vaski/Kirjelma/Sivut/U_28+2021.aspx), March 2023.

9. Memorandum of the Ministry of Economic Affairs and Employment (EU/664/2022), available only in Finnish at (https://www.eduskunta.fi/FI/vaski/Kirjelma/Documents/UJ_29+2022.pdf), March 2023.
10. Policy Brief of the Prime Minister's Office 2022:25, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164290/25-2022-Promoting%20equality%20in%20the%20use%20of%20Artificial%20Intelligence-an%20assessment%20framework%20for%20non-discriminatory%20AI.pdf?sequence=7&isAllowed=y), March 2023.
11. VTT's vision paper: Most promising technologies, Perspective on sustainable growth and effective innovation policy in Finland, Technical Research Centre of Finland, available in English at (https://www.vttresearch.com/sites/default/files/2022-06/VTT_Most_promising_technologies_2022.pdf).
12. Leading the way into the age of artificial intelligence: Final report of Finland's Artificial Intelligence Programme 2019, publications of the Ministry of Economic Affairs and Employment 2019:41, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=y), p. 53, April 2021.
13. *Cf*. Preamble 10 of the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.
14. Oesch, Rainer – Pihlajamaa, Heli – Sunila, Sami: *Patenttioikeus* (in English: *Patent Law*), 2014, Alma Talent Oy, available only in Finnish, p. 91.
15. Guidelines for Examination in the EPO (November 2019), Part G – Chapter II-14.
16. Vapaavuori, Tom: *Liikesalaisuudet ja salassapitosopimukset* (in English: *Trade Secrets and Non-Disclosure Agreements*), 2019, Alma Talent Oy, available only in Finnish, p. 55.
17. Government Proposal HE 49/2018, p. 95.
18. Finnish Ministry of Finance, *Eettistä tietopolitiikkaa tekoälyn aikakaudella -selonteko* (in English: *Report on Ethical Information Policy in the Era of AI*), available in Finnish at (https://vm.fi/documents/10623/7768305/Eettist%C3%A4+tietopolitiikkaa+teko%C3%A4lyn+aikakaudella+-selonteko.pdf/bf0ef101-5e11-175e-a87a-dea78359780c/Eettist%C3%A4+tietopolitiikkaa+teko%C3%A4lyn+aikakaudella+-selonteko.pdf.pdf/Eettist%C3%A4+tietopolitiikkaa+teko%C3%A4lyn+aikakaudella+-selonteko.pdf), p. 16, April 2021.
19. Ballardini, Rosa – Kuoppamäki, Petri – Pitkänen, Olli: *Regulating Industrial Internet Through IPR, Data Protection and Competition Law*, 2019, Wolters Kluwer, p. 67.
20. *Ibid*. p. 125.
21. FCCA reports 1/2021, Collusion situations caused by algorithms, available only in Finnish at: (https://www.kkv.fi/en/current-issues/press-releases/2021/5.2.2021-continuous-development-of-algorithms-requires-ensuring-the-functioning-of-competition-and-the-interests-of-consumers), April 2021.
22. *Ibid*. p. 21 *ff*.
23. *Ibid*. p. 29 *ff*.
24. *Ibid*. p. 40 *ff*.
25. *Ibid*. p. 53.
26. See, e.g., *Kuoppamäki, Petri: Algoritmiset kartellit ja kolluusio – kilpailuoikeuden haasteet ja mahdollisuudet* (in English: Algorithmic cartels and collusion – opportunities and challenges from the perspective of competition law), Defensor Legis 4/2020, available only in Finnish, p. 619.
27. Airaksinen, Manne – Rasinaho, Vesa – Alitalo, Anni – Oikarinen, Matias – Vammeljoki, Minna – Puukka, Johanna: Study on potential reforms to the Finnish Companies Act in

terms of competitiveness, published by the Prime Minister's Office on 24 August 2020, description sheet; the sheet is available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162390/VNTEAS_2020_39.pdf), otherwise available only in Finnish, April 2021.

28. *Ibid*. p. 59 and p. 73.
29. Koulu, Riikka – Mäihäniemi, Beata – Kyyrönen, Vesa – Hakkarainen, Jenni – Markkanen, Kalle: *Algoritmi päätöksentekijänä? Tekoälyn hyödyntämisen mahdollisuudet ja haasteet kansallisessa sääntely-ympäristössä* (in English: Algorithm as a decision-maker? The possibilities and challenges of artificial intelligence in the national regulatory environment), published by the Prime Minister's Office, 2019, available in Finnish at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161700/TEAS_44_19_Algoritmi%20paatoksentekijana.pdf), p. 13, April 2021.
30. *Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi* (HE145/2022 vp) (in English: Government proposal to Parliament on the automatic decision-making in public administration legislation) p. 30.
31. Artificial intelligence can make public service discriminatory or security risk – participatory research project aims for better services, available only in Finnish at (https://www.sttinfo.fi/tiedote/tekoaly-voi-tehda-julkisesta-palvelusta-syrjivan-tai-tietoturvariskin-osallistava-tutkimushanke-tahtaa-parempiin-palveluihin?publisherId=37936456&releaseId=69931837), April 2022.
32. Leading the way into the age of artificial intelligence: Final report of Finland's Artificial Intelligence Programme 2019, Publications of the Ministry of Economic Affairs and Employment 2019:41, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf?sequence=4&isAllowed=y), p. 35, April 2021.
33. *Ibid*. p. 106.
34. Paavola–Seppänen–Eloranta, available only in Finnish at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162669/TEM_2021_3.pdf?sequence=4&isAllowed=y), p. 11, April 2021.
35. *Ibid*. pp 100–104.
36. European Commission, Proposal for a Directive of the European Parliament and of the Council on Adapting Non-contractual Liability Rules to Artificial Intelligence, COM(2022) 496 final.
37. *Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston direktiiveiksi tuotevastuusta ja tekoälyyn liittyvästä vastuusta* (U 82/2022 vp), (in English: Finnish Government's letter to the Finnish Parliament on the European Commission's proposals for Directives of the European Parliament and of the Council on product liability and liability in relation to artificial intelligence) Finnish Government 9 July 2020, *Oikeuskansleri Pöysti peräänkuulutti avoimuutta tekoälytyökalujen käytössä* (https://valtioneuvosto.fi/sv/-/oikeuskansleri-poysti-peraankuulutti-avoimuutta-tekoalytyokalujen-kaytossa), April 2021.
38. *Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi* (HE 145/2022 vp), s. 166–167 (in English: The Finnish Government Proposal to Parliament for legislation on automatic decision-making in public administration).
39. Koulu–Mäihäniemi–Kyyrönen–Hakkarainen–Markkanen, p. 99 *ff*.
40. *Ibid*. p. 101 *ff*.
41. *Apulaistietosuojavaltuutetun päätös* (Dnro 6482/186/2020), (in English: The Finnish Deputy Data Protection Ombudsman's Decision, docket number 6482/186/2020),

available only in Finnish at (https://tietosuoja.fi/documents/6927448/105358665/ATSV+p%C3%A4%C3%A4t%C3%B6s+6482.186.2020.pdf/7349d849-005e-48be-1422-8fe6cb712f14/ATSV+p%C3%A4%C3%A4t%C3%B6s+6482.186.2020.pdf?t=1666858167880).

42. The Non-Discrimination Ombudsman, Artificial intelligence and equality (https://syrjinta.fi/en/artificial-intelligence-and-equality), April 2021.
43. The Finnish Innovation Fund Sitra, Possibilities of utilizing artificial intelligence in the public sector, available only in Finnish at (https://www.sitra.fi/julkaisut/tekoalyn-kayttomahdollisuudet-julkisella-sektorilla), pp 34–36, April 2022.
44. The Finnish Government's analysis, assessment and research activities, Promoting equality in the use of Artificial Intelligence – an assessment framework for non-discriminatory AI, a summary is available in English at (https://tietokayttoon.fi/documents/113169639/113170760/25-2022-Promoting+equality+in+the+use+of+Artificial+Intelligence-an+assessment+framework+for+non-discriminatory+AI.pdf/d2032617-9545-f064-d121-9dbfb92b96c9/25-2022-Promoting+equality+in+the+use+of+Artificial+Intelligence-an+assessment+framework+for+non-discriminatory+AI.pdf?version=1.0&t=1661236803455).
45. The Finnish Ministry of Defence, Strategic Guidelines for Developing AI Solutions, available in English at (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162372/Strategic_guidelines_for_developing_ai_solutions.pdf?sequence=1&isAllowed=y), March 2023.
46. Statement of the Finnish Government U 28/2021 vp, available only in Finnish at (https://www.eduskunta.fi/FI/vaski/Kirjelma/Sivut/U_28+2021.aspx), April 2022.

Erkko Korhonen
Tel: +358 20 713 3136 / Email: erkko.korhonen@borenius.com

Erkko advises clients on various technology transactions and arrangements, including ICT projects, outsourcing and cloud implementation. He also advises clients on issues relating to data economy as well as data protection and privacy in general (especially relating to GDPR compliance and e-privacy matters) in addition to e-commerce, telecommunications, media and marketing and consumer laws and practices. Erkko has been involved in several IP/ICT/data-driven M&A transactions, including advising clients on complex carve-out and separation arrangements and transitional services. In 2015 and 2016, Erkko completed a five-month period as a Visiting Foreign Lawyer at Pillsbury Winthrop Shaw Pittman LLP in Washington, D.C. and Los Angeles. Erkko co-heads the firm's Technology & Data team.

Samuli Simojoki
Tel: +358 20 713 3500 / Email: samuli.simojoki@borenius.com

Samuli has over 20 years of experience in technology law and is a trusted advisor for complex transactions in various fields of technology. He has participated in a multitude of projects relating to the new data economy and the use of data in different fields of business, including the health and energy sectors. Samuli also advises various leading Finnish growth companies, assists corporations on their dealings with growth companies and provides advice related to growth companies' financing transactions.

Samuli serves as a member or advisor on the boards of select Finnish technology and growth companies. Samuli is also the Chair of the International Bar Association's Media Law Committee.

Samuli is the Co-head of our Technology & Data team and the Chair of Borenius's Board.

Jon Jokelin
Tel: +358 20 713 3161 / Email: jon.jokelin@borenius.com

Jon joined Borenius as an associate in 2021. Before that, he worked as a trainee at Borenius and other Finnish law firms as well as at the District Court of Helsinki and Finnish Patent and Registration Office.

Jon advises our clients on matters related to technology and intellectual property law. Jon also focuses on corporate law-related questions, with a particular emphasis on growth companies. He also advises clients on financial services regulation and blockchain-related questions.

Borenius Attorneys Ltd

Eteläesplanadi 2, FI-00130 Helsinki, Finland
Tel: +358 20 713 33 / URL: www.borenius.com

France

Boriana Guimberteau
Stephenson Harwood

1. Trends

In recent years, society has been confronted with the increasing development of new technologies. In a digital era, European and national institutions must set new rules, best practices and recommendations to regulate Artificial Intelligence (AI), machine learning and big data in order to be competitive and to promote and protect innovation.

In March 2018, French President Emmanuel Macron announced that he wanted to make France the world leader in AI through the implementation of a national strategy. Four years later, France entered the second phase of the strategy, which runs from 2018 to 2025. Based on the Villani report,[1] it has three main objectives: attracting talent and investment in AI; disseminating AI and big data in the economy; and promoting an ethical AI system. Emmanuel Macron intends to carry on the efforts in this area since he unveiled the France 2030 investment plan in October 2021. Thirty billion euros are to be invested over five years to develop French industrial competitiveness and, through it, national solutions on AI and new technologies.

France is therefore particularly proactive and dynamic in the development of AI. Following the Villani report's ambition, the French government has, in particular, created the platform Health Data Hub in November 2019 to promote research and to financially support project leaders for selected projects. The platform helps research by enabling the access of a large amount of health data obtained from various health data systems including public health agencies. The platform collects and enables access to health data, henceforth promoting innovation in its use. It also contributes to the dissemination of standardisation norms for the exchange and use of health data. These missions, as well as some additional ones, are detailed in Article L. 1462-1 of the Public Health Code.

In parallel, France has also been actively promoting and ensuring an ethical AI system. As a reminder, France has always been interested in researching ethics as it was the first country to create a National Consultative Ethics Committee for Health and Life Sciences. If it was at the beginning only addressing health and science matters such as medically assisted procreation, the scope of the Committee quickly broadened to integrate new issues at stake caused by the increasing development of new technologies. In December 2019, the National Ethics Committee created a Digital Ethics Pilot Committee that has the purpose of addressing in a comprehensive way the ethical issues of digital and AI. The committee issued its first opinion in May 2020 on digital monitoring for pandemic management. Similarly, in December 2017, the CNIL released a study on ethics in AI entitled "*How can Humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*"[2] addressing the issue of AI and algorithms, recommending on that matter the creation of a platform auditing algorithms.

The French government is therefore very committed in ensuring the development of AI and machine learning, while ensuring that it has a framework. The CNIL is also a valuable institution in identifying risks.

In parallel, the European Union, driven by the ambition of becoming the world leader in AI technologies, has considered the digital evolutions induced by AI systems by adopting new regulations.

In October 2020, the European Parliament adopted three reports designed to address issues related to the development and increasing use of AI systems in relation to ethics,[3] liability[4] and intellectual property (IP) rights.[5] These reports pave the way for the establishment of European rules that will herald future legislation. To this end, they aim to create new legal frameworks embracing AI's specificities while promoting a dynamic and secured AI environment system.

As it is, the report on ethics sets new obligations that must be respected during the development and use of AI in terms of security, transparency, privacy, data protection, etc. In terms of liability, the report makes those who use high-risk AI liable for any damage resulting from its use. In the IP report, the EU recognises the importance of setting up a system of IP rights that provides sufficient guarantees to patent developers and promotes and secures innovation. Those three reports were closely followed up in 2021 by resolutions on AI in criminal matters, education, culture and audiovisual.[6]

In addition, the report on liability led to the presentation by the European Commission on 21 April 2021 of the *Artificial Intelligence Act*[7] which is a proposed horizontal regulatory framework on AI. The purpose of this draft is to set harmonised rules at the European level for the development, placement on the market and use of AI systems, as well as to address the risks brought out by AI. The *Artificial Intelligence Act* sets numerous obligations based on the level of risk the AI can cause, with some uses being strictly banished.

Alongside the AI Act, on 28 September 2022, the European Commission published a proposal for a Directive of the EU Parliament and Council "*on adapting non-contractual civil liability rules to artificial intelligence*", called the "AI Liability Directive".[8] This Directive aims to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies in the EU. Within the Directive, national courts would furthermore be given the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage. Indeed, the 2018 evaluation report of the Product Liability Directive[9] identified several shortcomings in relation to digital technologies in general and AI in particular.

A certain regulation of AI and machine learning is therefore beginning to emerge at the European level. New rules and obligations are being created to regulate the development and use of AI, ensuring competitiveness and securing innovation.

Regarding the protection of data, on 23 March 2022 the European Commission published a Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data, called "the Data Act".[10] This Regulation would apply alongside the General Data Protection Regulation of 27 April 2016[11] and introduces new rules on who can use and access all types of data (personal and non-personal) generated in the EU and in all economic sectors. This Regulation shall apply to AI systems.

2. Ownership/protection

According to the WIPO (World Intellectual Property Organization), AI is a "*discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention*".[12]

Big data refers to structured and unstructured data that is so large, fast or complex that it is difficult or impossible to process using traditional methods or storage.

Deep learning requires big data as it is necessary to isolate hidden patterns and to find answers without overfitting the data.[13]

Currently, there is no regulatory framework on AI, big data or machine learning, whether it be at the international, European or national levels. However, as mentioned before, the European Commission released in October 2020 a report on IP rights for the development of AI. It aimed at adopting an operational legal framework for the development of European AI and public policies treating the issues at stake and assessing all the IP rights related to them. In this respect, IP law may evolve in the future to take account of specificities of these new technologies.

However, if initiatives are conducted at the European level to consider the new challenges brought by AI, only the current rules of IP law can be applied to the protection of AI and its results. As AI encompasses a various range of elements (software, hardware, algorithms, computer programs, databases, etc.), different grounds of IP rights may be triggered.

2.1 Protection of AI tools

2.1.1 Copyright

Since 1985, computer programs have been protected under copyright law. The European Union has followed the lead since the European Directive n°91/250 CEE of 14 May 1991 on the legal protection of computer programs,[14] and later, harmonised the rules on the matter at the European level.

Software is therefore protected by copyright, whether it is the computer program itself (source and object codes), the program structure or the instruction programs that are addressed to the machine. In this respect, the French Supreme Court (*Court of Cassation*) had modified the definition of originality in a decision of 7 March 1986: the author must show a personalised effort going beyond the simple implementation of an automatic and constraining logic for the work to be original. Originality is therefore characterised by the author's intellectual contribution.

Consequently, the software part of an AI could be protected under copyright law as long as it fits the definition of originality. However, algorithms cannot be protected under copyright law as it is a "*succession of operations which only translates a logical statement of functionalities, devoid of all the functional specifications of the product concerned*".[15] It does not demonstrate the intellectual contribution of the author. In principle, copyright is granted to the creator of the work, and this, from its creation. In this sense, the author of the software will own the copyright. However, in the case of an employment contract, the rights related to the software will automatically be transferred to the employer.

2.1.2 Patents

Article L. 611-10 of the Intellectual Property Code (IP Code) explicitly excludes from patentable inventions algorithms, computer programs and mathematical models as they cannot be considered as inventions. However, AI elements can still be protected by patent law as a combination invention insofar as the invention meets the regular criteria of protection (novelty, inventive step, susceptible to industrial application) and is not based solely on algorithms and mathematical methods. In this case, AI elements, taken as a whole, could be patentable and protected under French patent law.

2.2 Protection of AI-generated content

AI can produce different results, some of which could be qualified as creations or inventions, the former falling within the scope of copyright law and the latter of patent law. Hence,

it strongly raises the question of authorship and ownership of the works and inventions it generates.

2.2.1 Copyright

Regarding copyright, many authors have considered the question of whether AI could benefit from the status of author of the generated content.

In France, authors recognise the personalist and humanist conception of copyright: the author is the person who creates the work. Historically, French copyright was created *in favorem auctoris*, i.e., in favour of the author. Since the philosophy of the Enlightenment placed individuals at the heart of its concerns, copyright was understood as a natural right, justified by the indefectible link between authors and their work. The work being an extension of their person, it is quite logical for them to be the rightful owners and to be protected accordingly.

The condition of eligibility also reflects this conception. To be protected, the work must be an original creation: this criterion is intrinsically linked to the author's person, since originality is the imprint of the author's personality. With this condition being found within the author's person, the results of AI cannot meet the conditions of copyright unless the AI is controlled by human intervention.

Furthermore, creation must be conscious and only a conscious being can engage in a creative process. By contrast, an AI is functioning based on its learning system. The requirement of a conscious human intervention implies that a machine cannot acquire the status of author.

The recognition of copyright protection to AI is therefore not likely under the applicable laws unless there is a human intervention, and the AI is used as a tool.

Consequently, if the current French IP law does not seem to apply to contents generated only by an AI, it could apply considering the degree of involvement of the AI tool's user. Nevertheless, in the absence of legal and/or regulatory provisions to date, it is case law that will be required to draw the contours of copyright protection applied to AI.

2.2.2 Patents

Patent law adopts a similar position to copyright law as it requires the identification of a natural person. Once again, the question of the AI as a potential inventor arises. In the IP Code, inventors are only referred to as natural persons. Indeed, according to Article L. 611-6, paragraphs 1 and 2 of the present code: "*The right to the industrial property title referred to in Article L611-1 shall belong to the inventor or his successor in title. If two or more persons have made an invention independently of each other, the right to the industrial property title shall belong to the person who can prove the earliest date of filing*." Therefore, an AI cannot be recognised as the inventor of the content obtained through its operation. The reasoning mentioned in copyright also applies to patent law.

One landmark case has, however, stirred debate by addressing the status of AI inventors. Quite recently, the inventor and scientist Stephen Thaler has submitted several patent applications listing DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) as an inventor. DABUS is an artificial neural network that has autonomously generated two inventions, including a beverage container based on fractal geometry. Those applications were rejected by numerous IP offices worldwide, on the ground that only a natural person could be an inventor.[16] Such requests were therefore explicitly in contradiction with the applicable law.

Some countries have taken a particularly innovative approach by recognising DABUS as an inventor. In 2021, South Africa even became the first country in the world to officially

recognise an AI as an inventor in a patent application. The Federal Court of Australia also approved the patent application listing DABUS as an inventor, Judge Jonathan Beach even declaring that: "it is a fallacy to argue […] that an inventor can only be a human."[17] Ultimately, such recognition was possible insofar as there had been human intervention in the process, as an individual created the AI.

2.3 Risk of IP infringement while using AI tools

While the very application of IP law to AI is not obvious, AI may also carry risks of potential infringement of prior IP rights. Indeed, since AI generally feeds on very large datasets, and in particular pre-existing content, it is possible to generate content infringing prior rights via the AI tool.

2.3.1 Responsibility of AI tools

In France, Article L.122-4 of the IP Code defines copyright infringement as the act of representing or reproducing a work in whole or in part without the author's permission. Nevertheless, Article L.122-5 of the same code provides for exception to this right of representation and reproduction, when the work has been disclosed: the author cannot, for example, prohibit private and free representations made exclusively within a family circle, or any copies and reproductions from a legal source and strictly reserved to private use.

The EU Directive 2019/790[18] on copyright and related rights in the digital single market has brought an additional exception. Indeed, Articles 3 and 4 of the Directive provide for the exception of "*Text and Data mining*". Such exception was transposed in French law with the Ordinance No.2021-1518 of 24 November 2021 in Articles L.122-5 and L.122-5-3 of the IP Code. Such Articles have entered into force on 1 January 2023.

Text and Data mining is defined in the Article 2 (2) of the said Directive as "*any authorised analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations*". AI tools are generally based on such systems. AI tools could therefore fall into the scope of Text and Data mining exception, provided that:

- the content that the tool contains has been made public; and
- it has been lawfully obtained.

Article L.122-5-3 of the IP Code, providing for this exception in French law, adds "*unless the author has objected in an appropriate manner, in particular by machine-readable processes for content made available to the public online*".

The content "*lawfully obtained*" means the reproduction or representation in whole or in part by the AI tool, of a public work, for which Text and Data mining has not been expressly forbidden by its author. Given the recent entry into force of the provisions, we will have to wait for case law to determine the contours of this exception.

2.3.2 Responsibility of the user of the AI tools

In addition to the liability of the AI tool, or more precisely of its developer/owner, the user of the AI tool is also exposed to several types of liability.

Indeed, generally, it is the user who discloses the content generated by the AI tool. The user could therefore engage his/her liability on the basis of French common law in the event of an illicit disclosure.

However, the disclosure of such content may also infringe IP rights. The liability of the user may result from the terms and conditions of the AI tool.

3. Antitrust/competition laws

The purpose of competition law is to ensure the regulation of markets and prevent anti-competitive practices. However, the development of AI could contribute to create new anti-competitive practices, cartels and abuses of dominant position.

To this end, in November 2019, the French Competition Authority and the German *Bundeskartellamt* have presented a joint study on algorithms and their implications for competition law enforcement while assessing the competitive risks associated with the use of algorithms.[19] The two competition authorities have endeavoured to jointly study the effects and potential risks of collusion that the use of algorithms can generate on competition and have considered the question of adapting the rules of competition law with the new practices permitted today by AI.

The price algorithms that are used to set the price lists applied by companies are more particularly targeted. To this extent, the study can be particularly useful to companies who want to ensure the compliancy of their algorithms with antitrust laws.

The algorithms that are used to support the commercial strategy and the pricing policy of companies could encourage competition breaches by hindering the free determination of market prices through the interplay of supply and demand. It could lead to the creation of barriers to market entry.

Algorithms could also be detrimental by enhancing collusion. In this matter, the report identifies three main risks:

- algorithms could be used to facilitate the implementation of traditional anticompetitive agreements (price fixing, customer sharing, etc.);
- a third party, for instance a software developer, could provide the same algorithm to several competitors which would cause pricing coordination; and
- algorithms could be used by companies to facilitate an alignment of the companies' behaviour.

In February 2020, the French Competition Authority published its study on competition policy regarding the challenges at stake within the digital economy. In its new contribution, the French Competition Authority reviews its analysis and recommendations to better regulate anti-competition practices and unfair competition caused by AI.

In April 2020, a Paper on Big Data and Cartels: The Impact of Digitalization in Cartel Enforcement was released by the ICN (International Competition Network) in order to identify the challenges raised by Big data and algorithms in cartel enforcement.[20] The report analyses AI as a collusion-creating tool, but also as an interesting one in detecting them.

Consequently, while no legal framework has been currently adopted to regulate the risks caused by AI, big data and machine learning, competition authorities in Europe and beyond are beginning to pay closer attention to the effects of AI and big data on competition.

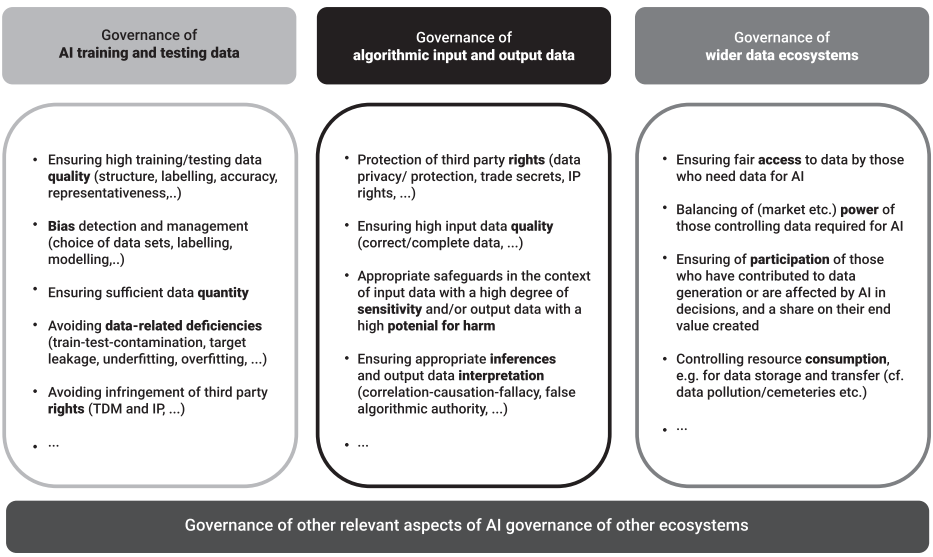
4. Boards of directors/governance

To enhance the benefits of AI while reducing the risks, governments must analyse the scope and depth of the existing risks and develop regulatory and governance processes and structures to address these challenges.

In France, the ACPR (*Autorité de Contrôle Prudentiel et de Résolution*) released a study "*Governance of Artificial Intelligence in Finance*"[21] in November 2020, according to which the following governance concerns need to be taken into account as early as the design phase of an algorithm: integration of AI into traditional business processes; impact of this integration on internal controls, specifically on the role assigned to humans in the new

processes; relevance of outsourcing (partially or fully) the design or maintenance phases; and lastly, the internal and external audit functions. According to the study, the most relevant elements of governance when introducing AI into business processes appear to be the operational procedures within those processes, the extension of segregation of duties to the management of AI algorithms, and the management of risks associated to AI. These elements are briefly described in this section.

It is also important to put in place data governance as it is the data which is used for the proper functioning with the AI. In this respect, in November 2020, the Global Partnership on AI (GPAI), which was established with a mission to support and guide the responsible adoption of AI, issued a report on Data Governance[22] which provides guidance on data governance depending on the different types of data:



5. Regulation/government intervention

5.1 GDPR and compliance

New technologies have considerably influenced the legislative landscape to the point that new regulations have to be implemented. As AI enables the processing of a large amount of personal data, the EU must ensure the respect of data subject's rights and privacy. In this respect, the increasing use of AI systems raises the question of their regulation as AI is continuously fed by an exponential amount of data during the machine learning phases. Certain precautions must be taken to protect the rights of data subjects.

Since 25 May 2018, and in addition to the French 1978 Data Protection Act, the principal data protection legislation within the EU has been the Regulation (EU) 2016/679 also known as the "General Data Protection Regulation" or "GDPR". Data must be collected and used in full compliance with the EU's GDPR.

In this respect, the GDPR imposes numerous obligations on companies, as they process European citizens' personal data. Companies engaged in big data, machine learning and AI must ensure that they respect these principles insofar as they process the personal data of European citizens:

- The processing of personal data carried out during AI phases must follow specified, explicit and legitimate purposes and can only be used for the purposes for which it was collected.
- The legal bases justifying the processing must be enlightened. Article 6 of the GDPR provides an exhaustive list of legal bases on which personal data may be processed.
- The data must be kept for a limited time, which must be specified.
- According to the principle of data minimisation, only the data that is strictly necessary for the processing must be collected.
- Personal data must be accurate and kept up to date.
- Transfers of European data outside the EU are prohibited or strictly controlled.
- Data subjects must be aware of their rights regarding the processing of their personal data.
- Personal data must be processed in a manner that ensures its appropriate security.
- The principles of privacy by design and privacy by default must be respected.

Consequently, companies dealing with AI tools and machine learning must follow these principles.

On 5 April 2022, the CNIL published a set of resources for the public and professionals dealing with the challenges of AI in relation to privacy and GDPR compliance.[23] Hence, the CNIL has made available to professionals a guide to ensure that companies using AI systems and processing personal data comply with the GDPR and the French Data Protection Act. As such, its main objective is to develop a regulatory framework for AI that respects human rights and helps in building European citizens' confidence in the system. Moreover, the guide provides an analysis tool allowing organisations to self-assess the maturity of their AI systems with regard to the GDPR and best practices in the field, in view of the future European regulation.

5.2 Tax law

The French 2020 Finance Act has authorised tax authorities, on an experimental basis and for a period of three years, to collect freely accessible data on social network websites and online platform operators. The Finance Act aims to prevent tax fraud and to improve prosecution of tax offences such as hidden activities and false domiciliation abroad of individuals (Article 154 of the 2020 Finance Act).

The CNIL, in its opinion of 12 September 2019, emphasised the need to respect the principle of minimisation as well as the principle of proportionality; only data that is necessary for the detection of tax fraud should be processed.

5.3 Open data

Big data also raises the question of its accessibility to the public. As numerous data is being collected, transparency in the process must be established.

Launched by the *French Digital Republic Act* in October 2016, the open data policy ensures a public data service by opening the dissemination of administrative data of economic, social, health or environmental interest.

For instance, in the field of Justice, the open data policy is characterised by the dissemination of public data applicable to court decisions. To this end, Articles 20 and 21 of the French

Digital Republic Act establish the availability of court decisions to the public free of charge and in electronic form. However, such dematerialised access necessarily implies the dissemination of a significant volume of personal data, including sometimes sensitive data, in the case of access to data relating to criminal convictions.

There is, therefore, a risk of conflict with the protection of personal data. However, this requires the prior removal of the first and last names of the individuals concerned, as well as any element allowing them to be identified.

5.4 Prevention of terrorism

The *law of July 30, 2021, on the prevention of terrorism acts and intelligence* comes to consider the digital evolution by integrating the new technologies and means of communication used by terrorists. As such, the intelligence services have new means of control and can now implement algorithmic monitoring of connection and browsing data on the Internet to identify potential terrorists. They can also intercept satellite communications.

Electronic communications operators, internet service providers and hosting companies are cooperating in the implementation of this surveillance. In this respect, a generalised obligation to retain connection data is now imposed on them, which is justified by the threat to national security. The law is therefore in line with the decision of the Council of State French Data Network of 21 April 2021.

The law, at the draft stage, had been the subject of three opinion notices of the CNIL dated 8 April, 15 April and 3 May 2021.

6. Criminal issues

In an increasingly connected environment, the scenario of an AI committing a crime no longer seems so aberrant. While an AI cannot commit crimes such as murders, it could indeed facilitate alternative forms of crime as it creates new criminal models.

In this sense, Europol, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and Trend Micro have recently released a report on the malicious uses and abuses of AI such as AI malware, AI-supported password guessing, and AI-aided encryption and social engineering attacks.[24] While some of the scenarios presented may appear quite theoretical, the report helps policymakers and law enforcers by listing existing and potential attacks with recommendations on how to mitigate these risks.

However, algorithms can also be used in criminal matters by the police, legal jurisdictions and public authorities. As AIs process vast quantities of personal data and analytics, it must be ensured that data subjects' rights regarding privacy and personal data are respected.

In October 2021, the European Parliament adopted a draft report on *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*.[25] It outlines the European views as well as recommendations on AI data processing by public authorities in the field of law enforcement and in the judiciary. Among other things, the draft report calls for greater algorithmic transparency, explainability, traceability and verification to guarantee the compliance of AI systems with fundamental rights. It also supports the *High-Level Expert Group on AI of the European Commission* in its desire of banning AI mass scale scoring of individuals by public authorities. The report emphasises that the security and safety aspects of AI systems used in law enforcement and by the judiciary need to be assessed carefully and be sufficiently sturdy to prevent the consequences of malicious attacks on AI systems.

To illustrate, in France, 2017, the CNIL had issued a warning to the city services of Valencienne for deploying an illegal videosurveillance policy. The city had installed

around 300 cameras alongside computer vision software that aimed to detect and analyse "abnormal behaviour". The CNIL issued a warning, stating that the regulations were not respected, and that the device was disproportionate. The system was installed outside of any legal framework and without seeking the opinion of the CNIL, which is mandatory in such cases. The video protection system includes a certain number of functions (automatic number plate reading device, detection of rapid movements, counting the number of people, etc.) and many cameras were directly monitoring public space. The CNIL found that the system was illegal, given its numerous malfunctions, also due to the lack of a study on other "less intrusive" means of securing the city.

In 2021, the CNIL submitted a draft position on so-called "intelligent" or "augmented" video devices in places open to the public in order to accompany their deployment and to ensure the respect of data subjects' rights.[26] In this report, the CNIL noted that use for civil security, health or traffic flow purposes, which are of little harm to individuals, is not authorised by the current regulations as it is not possible in practice to respect the right of opposition. The CNIL therefore considers that it is up to the public authorities to decide whether to enable such processing.

Also, given the increase of cyberattacks, the EU Directive "NIS2" of 14 December 2022 aims to strengthen security requirements, streamline reporting obligations, and introduce stricter supervisory and enforcement mechanisms.[27] The Directive entered into force on 16 January 2023 and the Member States have until 17 October 2024 to transpose it in national legislation. It broadens the scope of application of the previous "NIS" Directive, and for example requires companies to implement cyber risk management measures, including risk mitigation requirements and due diligence of third-party suppliers and services.

Finally, a Proposal for a Regulation[28] of the EU Parliament and Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 was published on 15 September 2022, called "Cyber Resilience Act". This proposal for a Regulation was drafted in reaction to the increase of successful cyberattacks on hardware and software products, leading to an estimated global annual cost of cybercrime of 5.5 trillion euros by 2021. It mainly aims to create conditions for the development of secure products with digital elements, by ensuring that manufacturers take security seriously throughout a product's life and create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

7. Discrimination and bias

According to the European Parliament, AI technology must be trained using unbiased data sets to prevent discrimination.[29]

In a press release dated 16 March 2021, the European Parliament indeed informed about the risks of the use of AI in the education, culture and audiovisual sector, notably the potential impact on the "*backbone of fundamental rights [and] values of our society*".

The Culture and Education Committee then called for AI technologies to be regulated and trained so as to protect non-discrimination, gender equality, pluralism, as well as cultural and linguistic diversity.

In this regard, the European Parliament affirmed that the Commission "*must establish a clear ethical framework for how AI technologies are used in EU media to ensure people have access to culturally and linguistically diverse content*". This should be the role of the proposed AI Act, and the AI Liability Directive.[30]

In the context of the increased use of AI-based technologies, in particular to improve decision-making processes, it is necessary to ensure that all Europeans can benefit from these new technologies in full respect of EU values and principles.

In this regard, the EU has proposed a Directive, alongside the proposed AI Act, which aims to raise a common set of rules for a non-contractual liability regime, called the "EU Artificial Intelligence Liability Directive". The purpose of the proposed Directive is to modernise the current liability regime.

For example, such proposition creates a rebuttable "*presumption of causality*" to ease the burden of proof for victims to establish harm caused by an AI system. It would furthermore give national courts the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage.[31]

8. National security and military

In terms of military use of AI, the European Parliament has raised awareness, in a press release dated 20 January 2021. In fact, it considers that:

"*AI can replace neither human decision-making nor human contact;*
EU strategy prohibiting lethal autonomous weapon systems is needed."

As per more general security concerns, in particular regarding the risk of mass surveillance and deepfakes by public authorities "*the increased use of AI systems in public services (...) should not replace human contact or lead to discrimination*". More specifically in the health sector, the European Parliament warns on the necessity to highly protect the patients' personal data.

Moreover, EU Member States warn on the threats to the fundamental rights and state sovereignty arising from the use of AI technology in massive civil and military surveillance (for example, highly intrusive social scoring applications should be banned).[32]

In France, the Ministry of the Armed Forces is developing its relations with the French scientific community in the field of AI and is supporting projects that could lead to new technologies of interest to national Defence. The development of AI will aim to significantly increase the strategic autonomy and the operational and technological superiority of the armed forces.[33]

* * *

Endnotes

1. https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf.
2. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.
3. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf.
4. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf.
5. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf.
6. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2017(INI)&l=en.
7. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-958501aa75ed71a1.0001.02/DOC_1&format=PDF.
8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.
9. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374.
10. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068.
11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

12. WIPO/IP/AI/2/GE/20/1 REV., "WPO conversation on intellectual property (IP) and artificial intelligence (AI)", May 21, 2020, §11.
13. Wayne Thompson SAS Research & Development, *Big Data: What it is and why it matters | SAS*.
14. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0250&from=EN.
15. Cour d'appel de Caen, 18 March 2015, Ministère public / Skype Ltd and Skype Software Sarl.
16. In 2019, the European Patent Office (EPO) rejected the patent applications submitted in the name of DABUS, followed by the USPTO in 2021 and the IPO the same year. Thaler appeal in UK was also dismissed.
17. *Federal Court of Australia, Thaler v. Commissioner of Patents* [2021] FCA 879, §12
18. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0790.
19. https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=5.
20. https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/06/CWG-Big-Data-scoping-paper.pdf.
21. https://acpr.banque-france.fr/sites/default/files/medias/documents/20200612_ai_governance_finance.pdf.
22. https://gpai.ai/projects/data-governance/gpai-data-governance-work-framework-paper.pdf.
23. https://www.cnil.fr/fr/intelligence-artificielle/la-cnil-publie-ressources-grand-public-professionnels.
24. https://unicri.it/sites/default/files/2020-11/Abuse_ai.pdf.
25. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf.
26. https://www.cnil.fr/sites/default/files/atoms/files/projet-position-cnil-relative-conditions-deploiement-des-cameras-dites-intelligentes-ou-augmentees-espaces-publics_consultation-publique.pdf.
27. https://eur-lex.europa.eu/eli/dir/2022/2555.
28. https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454.
29. https://www.europarl.europa.eu/news/en/press-room/20210311IPR99709/ai-technologies-must-prevent-discrimination-and-protect-diversity.
30. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.
31. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.
32. https ://www.europarl.europa.eu/news/en/press-room/20210114IPR95627/guidelines-for-military-and-non-military-use-of-artificial-intelligence.
33. https://www.entreprises.gouv.fr/fr/numerique/enjeux/l-intelligence-artificielle-et-monde-de-la-defense#:~:text=Le%20d%C3%A9veloppement%20de%20nos%20capacit%C3%A9s,artificielle%20de%20d%C3%A9fense%20(CCIAD).

Boriana Guimberteau
Tel: +33 1 44 15 82 78 / Email: boriana.guimberteau@shlegal.com

Boriana Guimberteau is a partner in the Paris office of the law firm Stephenson Harwood where she heads the Intellectual Property practice. She has strong experience in the full spectrum of IP rights with a focus on trademarks and unfair competition. She regularly acts before the specialised French and European jurisdictions and offices. Her expertise also covers non-traditional trademarks and copyright issues, and innovative technologies like blockchain and NFTs.

Boriana started her career as in-house counsel at LVMH (Perfumery division). Before joining Stephenson Harwood, she spent 17 years with the French firm FTPA co-heading the IP department. Boriana is a member of INTA's Brands & Innovation Committee and was once again recognised by the most recent *World Trademark Review*'s *WTR 1000* for her prosecution and enforcement work.

Stephenson Harwood

48, rue Cambon, 75001 Paris, France
Tel: +33 1 44 15 80 00 / URL: www.shlegal.com

Germany

Moritz Mehner, Dr. Martin Böttger & Dr. Christoph Krück
SKW Schwarz

Trends

The field of Artificial Intelligence (AI) and Big Data is expected to continue to evolve rapidly in 2023, with advances in areas such as natural language processing, computer vision and machine learning (ML), where algorithms are being used to analyse vast amounts of data and uncover insights that were previously impossible to detect.

One area where AI is already having a major impact is in the development of language models like OpenAI's ChatGPT, which can generate human-like text by analysing large amounts of language data. Even in the legal industry, ChatGPT and other language models could be used to automate tasks like drafting legal documents and contracts, conducting legal research and even assisting with case analysis and strategy. In fact, ChatGPT has the potential to be used in a wide range of industries, from healthcare to finance to retail, and is set to disrupt how we may work as a society in the near future. With the latest development from GPT-3.5 to GPT-4, published in March 2023, OpenAI has succeeded in taking the next important step within a very short time. GPT-4 is not only capable of visually recognising objects, i.e., when pictures of flowers are seen, the tool recognises the object flowers, but GPT-4 also formulates what can happen to the object when an action is performed on the object.

Another trend to watch in 2023 is the increasing use of Big Data analytics to drive business decisions. As more data is generated from a growing number of sources, organisations are looking for ways to use this data to gain a competitive advantage. ML algorithms are being used to analyse large datasets and uncover insights that can be used to improve operations, target marketing efforts and develop new products and services. In connection with advancing AI models, the enormous amounts of available data become meaningfully usable for the first time.

Of course, as with any rapidly evolving technology, there are also concerns about the potential risks and ethical implications of AI and Big Data. For example, some researchers have warned that AI could be used to automate biased decision-making, or to create sophisticated fake news and propaganda.

AI continues to push into new application areas through skills that most people thought would be the exclusive domain of humans. As companies consider adopting these skills, they could benefit from thinking about how their customers will interact with them and how that will affect their trust. The functionality offered by new AI tools could, and probably will, turn the whole business upside-down and change it forever in some industries; but a lack of trust could ultimately ruin those ambitions.

The ban on ChatGPT in Italy has shown that there is a great need for explanation and regulation in the near future. It is essential for the further development and use of these

technologies that a regulatory framework is created that knows how to contain risks without squandering the technologies' great opportunities.

Ownership/protection

Big Data:

In principle, the German legal system does not know a legal ownership of data itself. In its final report of their conference in 2017, the German Minister of Justice of all 16 German states explicitly denied such an ownership right or the economical need of such a right to data itself; the current legal provisions are considered effective to meet the industries' interests and requirements.

The German legal system offers a multilayered framework of legal provisions under which data, access to data or the integrity of data may be protected:

Intellectual property rights:

In particular, data can also be protected under German **copyright law**. However, this depends solely on the respective content of the data. For the protection of data itself as a copyrighted work, the mandatorily required act of intellectual creation by a natural person within the meaning of the German Copyright Act (*UrhG*) is regularly absent due to its characteristic being the result or intermediate state of a machine process. Insofar as the content of the corresponding data constitutes a copyrighted work within the meaning of UrhG, it will be fully protected accordingly.

As a result of the implementation of the European Directive RL 96/9/EC, **database works** are protected under copyright under Section 4 UrhG, as well as the database creator under Sections 87a *et seq*. UrhG with a right of protection *sui generis*. The creation of a database work also requires a personal intellectual creation in the form of the systematic or methodical arrangement of the data as the database. In the case of electronic databases, this will depend on the individual case. The decisive factor in the creation is the conception of the selection and linking of the data. A systematic/methodical arrangement of data that is decisively determined or specified by an algorithm or other software will also fail to be an intellectual creation by a natural person. The execution of the arrangement can in principle be carried out by the "machine", without this speaking against a personal intellectual creation.

A similar case-by-case consideration is also necessary in the case of the ***sui generis* property right of the database creator** under Section 87a *et seq*. of UrhG. This is primarily a protection of investment. The creator of a database who makes a substantial investment in the creation or maintenance of the database is granted the exclusive right to reproduce, distribute and publicly display the database in its entirety or a substantial part thereof, pursuant to Section 87b UrhG. A personal act of intellectual creation is not required for this protection. Accordingly, it is not necessary to evaluate the individual case for an act of intellectual creation by a natural person, but the existence of a substantial investment. As a rule, one can also assume with regard to Section 87a *et seq*. UrhG in the case of machine-generated data that this usually represents a standardised by-product of the actual operation of the machine or software rather than a specific investment for the creation of a database.

In addition to this specific copyright content of data, it regularly may also contain **names, company designations, trademarks, logos and likenesses of personalities** and be of commercial value. Therefore, the requirements and prerequisites of trademark law, name law (Section 12 of the German Civil Code (*BGB*) is also regularly applicable to aliases and pseudonyms) and personal rights must always be observed when exploiting data. However,

this regularly does not play a role in the possibility to protect data, but rather plays a considerable role in the commercial exploitation by the respective party exploiting the data.

Lastly, ownership rights of course exist regarding the physical storage device/facility that empowers the owner respectively. However, this only relates to the physical items and facilities and not the data contained therein.

Legal access and/or integrity protection:

The central provisions in the **German Criminal Code** (*StGB*) are Sections 202a, 202b, 202c, 202d StGB (data access protection) as well as Section 303a StGB (data integrity protection) regarding the protection of databases. According to the legal general opinion, these are considered protective laws within the meaning of Section 823 (2) of the BGB and can therefore also give rise to claims under civil law against third parties.

Section 202a of the StGB makes it a criminal offence to obtain **unauthorised access** for oneself or another to data that is specially secured against unauthorised access by overcoming the access security. Section 202a of the StGB thus requires special security against unauthorised access – technical and organisational measures to protect data thus play an important role as elementary prerequisites for its legal protection (this is also the case in the German Business Secret Act (*GeschGehG*)). This usually excludes a large number of the relevant cases in which a person from within a company who regularly handles the relevant data "leaks" the data or passes it on "under the table" to third parties or provides them with access.

Section 303a of the StGB protects the **integrity of data against deletion, rendering unusable, suppression and modification** – not only in the stored state, but also during transmission of the data. Interference is only punishable if it is unlawful. This is already the case if there is unlawful interference with another's right, such as a right of disposal or possession.

The GeschGehG, introduced in 2019, may also grant protective rights to certain data. The GeschGehG mainly protects **business secrets** against unauthorised access, use and/or disclosure. Data may be considered a business secret, if (mandatory requirements) the information contained in the data is not publicly known and thereby has an economic value, is protected in its secrecy by appropriate technical and organisational measures and a legitimate interest in keeping it secret is shown. To fulfil these requirements and enable respective protection under the GeschGehG, entities are usually required to have a cohesive policy in place to appropriately protect business secrets from an operational as well as legal perspective.

Next to this legal framework provided under German laws, a key legal instrument in successfully protecting and simultaneously exploiting data is the correct use of contractual agreements. While such contractual relationships regularly only have a legal effect between the contracting parties, they should cover the complete value chain of the data to be exploited and make sure to meet the legal requirements to grant the protection as outlined above.

Reliable data business therefore depends on the overall effective legal framework and internal compliance policy.

Lastly, EU regulation also introduced an **allowance for text and data mining** in Section 44b UrhG. Text and data mining is understood as the automated analysis of single or multiple digital or digitised works to extract information, particularly about patterns, trends and correlations. Reproductions of lawfully accessible works for such text and data mining are permitted. An owner may reserve his rights to exclude his copyrighted works from such lawful text and data mining (i.e. with a digital watermark); such a reservation needs to be machine-readable.

AI:

AI applications are, by their nature, regularly protected as **software** under Section 69a *et. seq*. UrhG. Preparatory design work leading up to the development will also be protected; however, ideas and principles will not be. Protection under a software patent may be considered in case the software is firmly connected to a specific technical or mechanical feature or process.

On the other hand, as with machine-generated databanks above, any works that are generated by an AI application will regularly lack the necessary act of intellectual creation by a human being to be considered a copyright-protected work under the UrhG. There are, however, situations imaginable in which a human being creates copyright-protected work with the help of an AI application. It will come down to the individual case and the assessment if the respective process can still be considered an act of intellectual creation under the control by a human being with the help of an AI application, or if the human actions are not detrimental enough for the final result. As a general rule, the results – meaning generated works – of AI applications will not be protected under copyright laws in Germany. Therefore, there is also no comparable ownership right to these generated works.

While the result of AI applications will regularly not be protected under German copyright laws, the training of the AI application with existing copyright-protected works may very well constitute an infringement of the respective author's copyright. In practice, it is currently a major issue to actually prove that an AI application has been trained using copyright-protected works. However, the first international cases for obvious infringements by AI application can be found. Also, Section 44b UrhG for text and data mining may also apply, depending on the individual case – see above.

Antitrust/competition laws

AI & Big Data in competition law

German competition law can become relevant in case scraping technology is used for the respective learning processes.

Scraping can, under specific circumstances, constitute a so-called "targeted obstruction" of a competitor pursuant to Section 4 No. 4 of the German Act against Unfair Commercial Practices (*UWG*).

However, a breach of terms and conditions alone does not suffice according to the German Federal Court of Justice (*BGH*), but a "targeted obstruction" requires in addition that security measures are being circumvented against the will of the creator/provider of the database/content (e.g., automatic circumvention of a "Captcha-Tool").

Thus, whether security measures are circumvented in relation to AI, ML & Big Data will have to be assessed based on the specific database and scraping technology.

In case of a breach of the UWG, the creator of the protected material has the right to a cease-and-desist claim and claims for damages.

AI & Big Data in antitrust law

Antitrust law in Germany is governed by the German Competition Act (*GWB*). Establishing a market dominance under Section 18 GWB cannot simply be based on market shares or "data power" in case of Big Data or digital platforms.

As part of recent reforms, additional factors for the assessment were included in Section 18 GWB, *inter alia*, direct and indirect network effects, access to competition-relevant data

and the principle that the assumption of a market shall not be invalidated by the fact that a good or service is provided free of charge (i.e., in case the service is "only" paid with personal data).

Section 19 GWB prohibits the abuse of a dominant position. The "essential facilities doctrine" forms one group of cases in the context of the so-called refusal of business. This concerns cases in which companies control access to information, services or infrastructure and prevent access for other competitors in order to improve their own market position.

It is being discussed whether the mass amounts of data held by large Internet companies should be classified as such an "essential facility". However, the European Court of Justice requires "exceptional circumstances" as a prerequisite for access, and other arguments speak against this; in the case of personal data, data protection law itself can be a barrier, since personal data cannot be transferred to competitors in general without the consent of the data subject.

Board of directors/governance

In connection with the handling of Big Data and AI, managing directors and members of a management board (in the following referred to as directors) must take appropriate measures to ensure that the public law regulations applicable to their company are observed.

Those regulations include, *inter alia*, general provisions such as data protection regulations (GDPR) and the GeschGehG for the protection of business secrets, but also sector-specific laws such as Section 75c of the German Fifth Social Code (*SGB V*) (hospital sector), the German Federal Office for Information Security Act (*BSIG*) (for providers of critical infrastructure) and at a European level the upcoming Digital Operations Resilience Act (a regulation on resilience against cyber risks for financial companies) and the Artificial Intelligence Act (AI Act).

However, for the company director, the area of "Responsible AI" will become increasingly important. In the future, the director will also have to comply with the "AI Regulation" that was presented as a draft by the EU Commission on April 2021 and which, when coming into force, will regulate the handling of AI systems across all sectors of business and industry.

Against this background, the directors' personal due diligence obligations with regard to legal and business (including technical) risks are governed by applicable corporate laws and internal corporate governance rules. The admissible ratio between entrepreneurial risks and opportunities of a company depends, with regard to Big Data and AI, on the technical development and the technical and legal risks discernible.

As a rule, directors have to act with the care of a prudent and diligent businessman (*cf.* for example, Section 43 of the German Limited Liability Companies Act (*GmbHG*) and Section 93 of the German Stock Corporation Act (*AktG*)). This means the directors have to act diligently themselves and monitor the behaviour of the company's employees. In addition, directors also have a general compliance duty. This means that suitable organisational measures must be taken to avoid liability and control risk in the event of a potential risk.

Accordingly, measures taken by the management are generally at the director's reasonable discretion. A central aspect in this context is the so-called business judgment rule, which is codified in the AktG, but is correspondingly also applicable to other types of companies. According to this rule, the manager is acting diligently if, when making an entrepreneurial decision, he or she could reasonably assume to be acting for the company's benefit on the basis of appropriate information.

In this context, for the area of AI, it is critical that the director in his or her organisation ensures that the limited capabilities of AI are realistically assessed, the scope of application is clearly defined, intellectual property and privacy laws are complied with, and the results delivered by AI are subject to critical and constant human monitoring and review. The director cannot, in the current state of the art, readily rely on the results provided by any AI systems, as those results are fundamentally based on statistical considerations rather than on a thorough assessment of the individual circumstances.

Furthermore, the director must generally set up a compliance system that enables the company to avoid and control legal and business risks.

This, of course, also applies to the areas of Big Data and AI. The directors (themselves and through suitable employees) must, for example, identify and take measures to prevent IT and digital risks, e.g., by installing defensive devices, restricted access rights and access controls, shut-down mechanisms and by applying the need-to-know principle or taking other adequate organisational precautions. Such devices or mechanisms must be incorporated into a legal set of rules (so-called (IT) compliance guidelines) that must be brought to the workforce's attention and represent a binding work instruction.

In the area of Responsible AI, the currently available draft of the AI Regulation can serve as a source of orientation. The draft regulates, *inter alia*, AI safety, conduct, documentation and transparency obligations, risk-management requirements and sanction options for the authorities.

The director can delegate a certain part of his or her responsibility in the IT compliance area.

This can be affected vertically, i.e., by involving specialised employees at subordinate levels (e.g., CSO, CCO). But, at the same time, the necessary know-how and processes for effective monitoring of employees must also be ensured at the horizontal (senior management) level, namely by adequate company (and group) by-laws for the directors/management board.

However, even delegation typically does not fully release a director from his or her ongoing monitoring duties. In particular, in the case of rapidly advancing technical developments, such as in the area of Big Data or AI, a managing director must establish effective reporting chains and ensure he or she obtains a regular picture of the employees' (and responsible co-directors') activities.

Further, it is clear that a complete delegation of business decisions to AI systems is currently not permitted.

If the director violates his or her supervisory duties, he or she may be subject to personal liability claims for damages incurred by the company, directly or through claims raised by third parties. In the case of administrative offences within the company, a director is already considered responsible regardless of his or her own fault (and can even be personally fined) if there is no proper compliance system in place or if, for example, the measures pursuant to Art. 32 GDPR are not sufficiently implemented (Section 130 German Act on Offences (*OWiG*)).

Directors will need to be particularly critical of whether insurance policies in place cover the company's Big Data and AI activities. This applies in particular to Directors and Officers' Insurance policies. It is therefore recommended to discuss the director's measures and the company's compliance system with the insurance company when using or distributing Big Data or AI products.

Regulations/government intervention

Big Data

There is no regulation of the phenomenon of "Big Data" as such. The question of regulation is given some structure when three phases are considered: data collection; data storage; and data analysis.

Under the GDPR regime, data collection, storage and analysis are subject only to the extent that personal data are involved. In this respect, the upcoming Regulation on harmonised rules on fair access to and use of data (Data Act), which might become applicable in 2024 or 2025 in the EU, could apply. The Data Act will regulate certain aspects regarding the processing of non-personal data as well.

In the context of the GDPR, the principles of processing personal data according to Art. 5 GDPR are relevant for Big Data applications, especially the principles of purpose limitation, data minimisation and storage limitation.

The transparency requirement when obtaining valid consent for the processing of personal data using Big Data and/or AI analytics may pose challenges.

Sector-specific regulations may also play a role: in the area of payments and open banking, in addition to the GDPR, the Second Payment Services Directive may also need to be taken into account, if applicable; or in the field of scoring, the EU Solvency II Directive and its implementation in the German Insurance Supervision Act (*VAG*). Telematics services, such as the automatic assessment of insurance premiums, must be seen in the light of the prohibition of automated decisions under Art. 22 (2) GDPR.

AI

On an EU legislative level there is a new legal framework regarding AI in the pipeline: the Regulation of the European Parliament and of the Council laying down harmonised rules for the AI Act. It is likely that the law will be in place by 2024.

The AI Act focuses primarily on rules around data quality, transparency, human oversight and accountability and also aims to address ethical questions.

First of all, companies must address the question of whether the AI Act applies to their technologies and businesses' operations, since the scope of application is rather broad and will capture a broad spectrum of software products.

Most of the extensive compliance obligations apply to providers of AI-systems. Nevertheless, users of such systems also have to comply with certain obligations, in particular if they control the data input.

Companies outside the EU are also well advised to deal with the upcoming regulation, since on the one hand, the so-called "Brussels effect" is expected, i.e., countries outside the EU will adopt the EU approach in the long term and the rules might form a global standard, similar to the GDPR. And on the other hand, and more importantly, the scope of the AI Act already applies to providers that place AI systems on the EU market or put them into operation in the EU, regardless of whether these providers are established in the EU, as well as to providers and users of AI systems that are established or located in a third country, if the result produced by the system is used in the EU.

The AI Act classifies AI systems depending on their overall risk in several categories: unacceptable risk; high risk; and low risk, where each category is narrowed down to certain subject matters and each category faces a different regulatory approach. AI-systems that bear an unacceptable risk are prohibited, high-risk systems are subject to rigorous

compliance obligations and some AI-systems, classified as low-risk, have to comply only with transparency obligations.

The AI Act contains a large number of compliance regulations that must be observed during operation and even during development, and that may result in quite high fines if violated. Providers must essentially set up a risk-management system that documents and manages risks across the AI system's entire lifecycle.

High-risk AI systems, for example, have to comply with the following compliance obligations: risk management systems for the entire lifecycle; governance for training and testing data (data has to be representative, error free, complete and without biases); documentation; record-keeping possibilities to ensure traceability and monitoring; transparency; human oversight; accuracy; robustness; and cybersecurity.

Implementation of AI/Big Data/ML into businesses

The rapid evolution of technology in recent years has propelled the integration of AI, Big Data and ML into various business sectors, including finance, healthcare and retail, among others. By leveraging these tools, companies are now able to analyse vast amounts of data, improve decision-making processes, streamline their operations and gain a competitive edge. However, as businesses embrace these technological advancements, it is crucial for them to comply with legal requirements and implement policies to minimise legal risks associated with data protection.

Possible-use cases:

AI algorithms, particularly ML models, can process and analyse big amounts of data from diverse sources. When linked to Big Data, AI models can identify patterns, trends and anomalies that may be difficult or impossible for humans to detect. Possible-use cases encompass customer service with chatbots and virtual assistants, streamlining sales and marketing through data analysis or assisting human resources with recruitment, employee engagement and training. Additionally, AI bolsters fraud detection, cybersecurity and process automation, enabling businesses to focus on more complex tasks.

What companies should be aware of:

In addition to legal issues surrounding ownership and protection, antitrust and competition laws, labour and data protection laws also play a role. To enable legally compliant use of new technologies, it is further recommended to introduce company policies. Some key considerations when developing company policies include establishing ethical guidelines, data governance, and training and awareness.

Companies are recommended to create a set of ethical principles that guide the development and deployment of AI and ML systems, ensuring they are transparent, accountable and do not discriminate. Businesses should also implement a data governance framework that outlines the roles and responsibilities of different stakeholders in managing data assets, ensuring data quality and complying with data protection regulations. Finally, it is inevitable for companies to provide regular training and education to employees on data protection laws, ethical AI practices and the responsible use of AI, Big Data and ML.

The implementation of AI, Big Data and ML offers tremendous potential for businesses across various industries. However, it is essential to adopt a responsible approach, comply with legal requirements and implement policies that ensure ethical and transparent use of these technologies.

Discrimination and bias

AI applications in employment:

Robo-recruiting and other AI applications in the field of employment will also be regularly governed by the Anti-Discrimination Act in Germany. The established legal opinion in the legal literature in Germany suggests that any such AI applications need to be training with data mirroring the applicable "reality of society", especially in respect to all discriminatory aspects set by the Anti-Discrimination Act (racial or ethnic origin, gender, religion or belief, disability, age or sexual identity). Burden of proof in case of a challenge by an employee may fall back to the employer (if the employee makes a plausible indication of such discrimination) who uses AI application and ultimately by the developer or the distributor of the AI application.

Anti-discrimination principle in the German Constitution:

The same anti-discrimination principle is set in the German constitution and directly binds all states and the public sector. Any use of AI application in this field will have to adhere to this principle.

Conclusion

The question of legal regulation and applicable laws depends in relation to AI and Big Data on the specific technology and the individual case. In fact, AI and Big Data must always be considered together when evaluating and using them in a company.

In the EU, on a regulatory level, European-wide harmonised rules are being considered (GDPR, AI Act) which is also highly preferable to establish a robust and effective legal framework.

As is often the case in the field of technology, and also therefore with AI, the technological development will be faster than the legislation. This also means that early adopters will have to move in a certain grey area from a legal perspective for some time. For this reason, early consideration of the legal frameworks and installing compliance systems is particularly relevant.

* * *

Acknowledgments

The authors would like to give special thanks to their co-authors Christine Wärl and Helena Kasper for their contributions in the preparation of this chapter.

Christine Wärl advises national and international clients on mergers and acquisitions and other corporate transactions. She also advises on general commercial and corporate law.

Helena Kasper advises national and international clients on the legally compliant design of data-processing procedures and business concepts. In these areas, she is active in the real estate, online stores, technology and production sectors, among others. She supports companies in all data protection issues, with a focus on international data transfer and the digitalisation of business processes. Helena also advises on IT law issues and is a member of the SKW Schwarz Innovation Lab, specialising in the digitalisation of legal services (Legal Tech).

Moritz Mehner
Tel: +49 89 2864 0206 / Email: m.mehner@skwschwarz.de

Moritz Mehner, transferring his many years of private enthusiasm for esport, data economy and new technologies to his professional life, focuses on the legal matters surrounding these sectors. This includes advising on and drafting of both classic and new (SaaS, Cloud, PaaS) software and licensing agreements, issues relating to ownership and copyright, regulatory requirements and commercial exploitation.

His legal work additionally concentrates on designing and implementing solutions to legal problems associated with digitising innovative business models in the fields of data economy, IoT, Blockchain and cloud computing; utilising his experience from working two-and-a-half years on the business side in the data economy before becoming a lawyer in 2018.

Finally, Moritz is experienced in matters of data protection, in particular the practical application of the GDPR.

Dr. Martin Böttger
Tel: +49 89 2864 0461 / Email: m.boettger@skwschwarz.de

Dr. Martin Böttger mainly advises on M&A, private equity and venture capital mid-cap transactions, in capital markets law alongside general corporate and commercial law matters. Martin has particular expertise in the sectors of IT/software, life sciences, high-tech and real estate, as well as sports and brand companies.

His clients include institutional and private investors, international corporations, SMEs and start-ups. Martin has advised on the structuring and implementation of several private-equity financed buy-and-build platforms.

In addition, Martin represents family offices, private clients, foundations, athletes, clubs and associations in the areas of financing, legal structuring, asset management and sports law.

Dr. Christoph Krück
Tel: +49 89 28640268 / Email: c.krueck@skwschwarz.de

Dr. Christoph Krück specialises in IT law and digital business as well as data privacy. One focus is on advising online platforms on issues of internet and platform regulation as well as on youth, consumer and competition law. Furthermore, he advises companies on the drafting and negotiation of terms of use, general terms and conditions, licensing, SaaS, Cloud and other technology and IT contracts.

With regard to data privacy, he advises on the general requirements of the GDPR and is particularly focused on issues relating to the internet, as well as Big Data and platform structures. In addition, he closely monitors the developments concerning regulation of AI, blockchain and algorithms.

Dr. Christoph studied in Leipzig and completed his legal clerkship in Berlin with stages at the Federal Ministry of Economics and Technology and in a law firm in Massachusetts, USA. He wrote his doctoral thesis on aspects of German competition law in comparison to Spanish law.

SKW Schwarz

Wittelsbacherplatz 1, 80333 Munich, Germany
Tel: +49 89 286400 / URL: www.skwschwarz.de/en

India

Nehaa Chaudhari, Aman Taneja & Namratha Murugeshan
Ikigai Law / Ikigai Business Consulting

Introduction and trends

In 2022, revenue generated through Artificial Intelligence (**AI**) in India stood at USD 12 billion.[1] Increasing efforts by the Indian government to promote the digital economy and usher in a 'digital techade'[2] has made AI an important subject matter of legal and policy consideration. While government intervention has focused on areas such as making data-sets available[3] and drafting an IndiaAI roadmap that focuses on promoting research and innovation in the AI start-up community,[4] legal and regulatory intervention have not yet been introduced in India. However, this might change with the proposed Digital India Act (**DIA**), on which the government started public consultations in March 2023.[5] The DIA intends to bring AI regulation within its scope.[6] The government has indicated that it is considering defining and regulating high-risk AI,[7] creating frameworks for AI accountability and the ethical use of AI-based tools.[8]

In India's union budget for 2023–24, India's finance minister called for 'Making AI in India and Making AI work for India'.[9] The budget also announced[10] the setting up of three 'Centres of Excellence' for research on AI in premier educational institutions,[11] promoting industry partnerships for research and development of scalable solutions in agriculture, health and sustainable cities and enabling access to anonymised data through the National Data Governance Policy.[12]

There is a big focus on identifying AI applications for public good, transforming sectors such as healthcare,[13] education[14] and agriculture,[15] and incentivising the adoption and promotion of capacity building in AI.[16] Prominently, the Ministry of Electronics and Information Technology (**MeiTY**), the NITI Aayog (the government's apex public policy think tank), the Telecom Regulatory Authority of India (**TRAI**) and the Department of Telecommunications (**DoT**) are government agencies and sectoral regulators actively involved in this space. Industry-led efforts include NASSCOM's Responsible AI Resource Kit that aims to seed the adoption of responsible AI at scale[17] and NASSCOM's programme 'Future Skills Prime' in collaboration with MeiTY, which is focused on upskilling IT professionals in various areas of emerging technologies, including AI.[18] The government has also launched several programmes such as 'Responsible AI for Youth'[19] and 'Youth for Unnati and Vikas with AI'[20] which aim to promote AI technology and social skills, and to enable Indian youth to become designers and users of AI. These are aimed at familiarising students with AI skills and to enable them to contribute to AI advancement through social impact solutions and through democratised access to AI tools.[21]

The Indian government is also keen to be a key participant in the conversation on AI adoption and regulation at an international level. The Global Partnership on Artificial Intelligence

(**GPAI**) is a multi-stakeholder initiative which aims to bridge the gap between theory and practice on AI by supporting cutting-edge research and applied activities on AI-related priorities, and specifically to support responsible and human-centric development and use.[22] India became chair of the GPAI in November 2022 for a three-year term.[23] The government has stated that it recognises AI as a kinetic enabler for taking forward current investments in technology and innovation. This follows India assuming presidency of the G20 forum.[24] Under its G20 presidency, India has emphasised the need for data-driven development and for converting data to intelligence through the use of AI and Big Data analytics.[25]

The trends highlight the government's efforts to make India a 'global innovation and research brand'[26] and the government's willingness to be open to innovative and experimental use of AI across various sectors for various use cases, while also adequately considering guardrails for such innovation, which are discussed in the sections below.

Ownership/protection

With advancements in AI technology, AI software can produce content on its own – ranging from complex texts on virtually any topic, blogs and short stories, to images, drawings and even poetry and music. Progress in Machine Learning has enabled AI to leverage experience to 'learn' and function in a manner that is very minimally reliant on human intervention. This presents a conundrum in ascribing ownership and protecting "works" created by AI. This is because this shifting ground, from AI being a creation, to AI becoming a creator, is presently not accounted for in Indian law.

Copyrightability of AI software

The requirement of a human creator and a minimum degree of creativity for copyright protection to accrue leaves open questions concerning ownership and authorship of works created by AI.

The ownership question pertaining AI arises at two levels – first, ownership of AI algorithms itself and second, ownership of AI-created works.

As far as AI software/algorithms are concerned, their copyright protection will be governed in India by the Copyright Act, 1957 (**Copyright Act**). According to the Act, computer programs and software are considered literary works,[27] and as such, they are eligible for copyright protection. Hence, AI software/algorithms are capable of copyright protection under the Copyright Act. Under the Act, the owner of a copyright in an AI software has the exclusive right to reproduce, distribute and perform the software.[28] To obtain copyright protection for an AI software, the software must be original,[29] a creative expression and not a mere idea or concept[30] and be of copyrightable subject matter, in this case being "literary works".[31]

The creator of the software/algorithm will have to prove these requirements to obtain copyright protection. Registration of copyright is not mandatory but is useful from an enforcement perspective. In case of infringement, copyright owners in India can enforce both civil remedies (by filing a suit for copyright infringement for an injunction/pecuniary remedies/rendition of account of profits)[32] as well as pursue criminal action (which include imprisonment/fines[33] as well as search and seizure).[34]

Copyright over AI-generated works

Though the AI software is itself copyrightable as a computer program, the dilemma arises in who will be the author and/or owner of any works generated by such AI software.

As discussed above, the Copyright Act provides that for the grant of copyright protection, any work must be original, i.e. originating from an author.[35] While the Act does not provide

for a standard of originality, judicial precedent has clarified that the baseline requirement is that the work must involve a minimum degree of creativity and should not be a product that is not merely a result of labour.[36] It is unclear whether outputs produced by AI tools would satisfy the requirement of "creativity" if they are viewed as mere synthesis of data from existing sources.

Another aspect is that copyright law has until now only recognised natural persons as authors of a copyrighted work. Hence, for AI-created works to gain copyright protection, it becomes necessary that a natural person is attached to any authorship claim. The Copyright Act stipulates that the author of literary, dramatic, musical or artistic works which are computer-generated is the "person who causes the work to be created".[37]

Hence, the question of authorship depends on the interpretation of the word "person". The Delhi High Court has taken a conservative approach wherein it stated the Central Board of Secondary Education (**CBSE**), being an artificial person, cannot claim authorship in a set of question papers.[38] This was reinforced in 2019 wherein the Delhi High Court rejected a copyright claim over a list compiled by a computer, on the grounds, *inter alia*, of lack of human intervention.[39]

Interestingly, in 2020, the Copyright Office had registered an AI tool "*Raghav*" and a natural person as co-authors of an artwork produced by the AI tool. This was the first time that an AI tool was being recognised as an author of a copyrighted work. However, subsequently, the Copyright Office issued a withdrawal notice, stating that the onus was on the applicant to inform the Copyright Office about the legal status of the AI tool.[40] This instance has cast some doubt over the ability of AI systems being recognised as authors of works.

Patentability of AI-related inventions

The Patents Act 1970 (**Patents Act**) stipulates that for an invention to be patentable, it must satisfy three requirements: novelty; inventive step; and industrial application.[41] The Patents Act does not allow the patenting of computer programs *per se* or algorithms. The Joint Parliamentary Committee has expressed the intent behind adding the words "*per se*" and stated that "*the words "per se" have been inserted because sometimes the computer program may include certain other things, ancillary thereto or developed thereon. The intention here is not to reject them for grant of a patent if they are inventions. However, the computer programs as such are not intended to be granted a patent*".[42]

However, Courts have clarified that a software-based invention that has a "technical effect" or a "technical contribution" may be patentable. Recently in 2020, the IPAB granted a patent for a "*Method and Device for Accessing Information Sources and Services on the Web*". The applicant's application for a patent had initially been rejected on the ground of being a computer program. However, he filed a writ before the Delhi High Court, arguing that there was a technical effect and a technical advancement involved and it was not a mere software simply loaded on to a computer. The Delhi High Court observed that "*innovation in the field of artificial intelligence, blockchain technologies and other digital products would be based on computer programs; however, the same would not become non-patentable inventions simply for that reason. It is rare to see a product which is not based on a computer program*".[43] It went on to state that "*patent applications in these fields would have to be examined to see if they result in a "technical contribution*".[44] This precedent is viewed as having provided a boost to software patents in India. The Patents Office has also published three sets of guidelines for computer-related inventions. In the 2013 Guidelines,[45] the meaning of "technical effect" has been elaborated as a "*solution to a technical problem, which the invention taken as a whole, tends to overcome. For example*

higher speed, improved user interface, more economical use of memory etc.". Further, the 2013 Guidelines also state in considering a patent application what has to be seen is how integrated the novel hardware is with the computer program.[46] These are important considerations to be kept in mind for developers of AI algorithms seeking to apply for a patent for their technology/software.

In recent years, there has been a significant increase in the number of software patent filings in India. A report by NASCOM sheds some light on the recent trends in software patents; Indian companies have filed 138,000 tech patents in India from 2015 to 2021. Over 50% of the patents filed during 2015–2021 were related to emerging technologies with AI leading in terms of total patents. AI patents more than doubled in the period 2015–2021 compared to 2015–2019. Twenty-one per cent of the technology patents filed were related to software applications and healthcare.[47]

Patentability of AI-generated inventions

Under the Patents Act, an application for a patent can be filed by "*any person* claiming to be the first and true inventor of the invention".[48] A 'patentee' is defined as "*the person* entered on the patent office register as the grantee or owner of the patent.[49] Reading of the above provisions of the Patents Act indicates that only a human can apply to be the inventor under the Patents Act. Hence, AI may not be eligible to apply as an inventor under the current law.

The Parliamentary Standing Committee on the "*Review of the Intellectual Property Rights Regime in India*" has observed that the requirement to have a human inventor for innovating computer-related inventions (innovations by AI and machine learning) hinders the patenting of AI-induced innovations in India.[50] Based on this recommendation, we may see further legislative examination of these provisions in the near future.

Trade secret protection

Trade secrets are usually information having commercial value which are not in the public domain. The Trade Related Aspects of Intellectual Property Rights (**TRIPs**) Agreement allows members the flexibility to frame laws to prevent the unauthorised disclosure and use of "certain information" which is kept secret, has a commercial value and the owner of the information takes reasonable steps to keep it secret.[51] India, though a signatory to TRIPS, does not have a separate law for trade secrets, which are instead protected through judicial rulings under provisions and aspects of contract law, torts, copyright law and common law principles of equity. Organisations may initiate an action based on breach of contract, (in case a Non-Disclosure Agreement or equivalent agreement was signed), a tort action on breach of confidentiality, misappropriation of trade secrets, infringement of copyright (in case the information was also protected through copyright) or even criminal offences, such as theft and criminal breach of trust. In India, trade secret protection has been recognised for information such as confidential client/customer lists[52] and technical drawings of a business.[53]

When trade secrets consist of works that are also the subject matter of copyright protection, principles of authorship and ownership applicable to copyright would apply. Courts have observed that trade secret law protects different elements of compiled business data, with copyright protecting the expression in the compilations and trade secret law protecting the underlying data.[54]

In the case of AI, trade secret protection can be particularly important as it can help to safeguard valuable proprietary algorithms, models and data sets that are crucial for the functioning of AI systems.

AI algorithms may be protected as trade secrets if they meet the criteria laid down by Courts. Courts have recognised trade secret to mean "*a formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information – including a formula, pattern, compilation, program, device, method, technique, or process that derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and is the subject of reasonable efforts, under the circumstances, to maintain its secrecy*".[55] Trade secret protection is sometimes broader and more flexible than other intellectual property protections such as copyright and patents and can be obtained without any application/registration, thereby making it an attractive option for AI developers.

In light of the above, it is clear that there is sufficient IP protection for AI technologies in India, and we may see more changes. The legal framework surrounding AI and AI-based systems needs to be evaluated to allow protection of both AI solutions and AI-generated works. This will not only incentivise innovation but also encourage creators of AI tools and technology, leading to development of better AI technology.

Antitrust/competition laws

The Competition Act 2002 and its attendant rules help in preventing practices which have adverse effects on competition in India and the Competition Commission of India (**CCI**) is the regulatory body responsible for not only its enforcement but also promoting and sustaining competition in the market. The recent emphasis by the government on creating public digital infrastructure for the betterment of citizens has laid bare the new realities of the digital economy and the need to regulate digital markets. This fact is reinforced by the 53rd Report of the Parliamentary Standing Committee (**The Report**) which deliberated on the need to bring in amendments aimed at digital markets. The report focuses on the anti-competitive practices of big tech companies. The Report notes that *ex-post* regulations in digital markets have not been sufficient to regulate anti-competitive practices. In order to address the same, it proposes *ex-ante* regulations. The Report recommends considering an approach that is similar to the Digital Markets Act adopted by the European Union. Large players in the digital markets that serve as 'intermediaries' or 'gatekeepers' will be recognised as 'Systemically Important Digital Intermediaries' (**SIDI**) based on revenue, market capitalisation and active business, and end users. The Committee recommended that the Digital Competition Act be framed as a separate legislation for regulating anti-competitive conduct in digital markets. The Government, on this basis, recently constituted a Committee on Digital Competition Law (**CDCL**) to examine the recommendation outlined in the Report.

The Report's recommendations differ from the recommendations made by the Competition Law Review Committee (**CLRC**) in 2019.[56] The CLRC noted the existing competition law was capable of handling anti-competitive practices that arise in the technology space. The CLRC concluded that the existing regulation was sufficient to address competition in the digital economy, with periodic reviews. The CLRC also suggested that the existing framework had the flexibility to deal with competition concerns of the digital market.[57]

With the rise of AI and its increasing use in various sectors, including e-commerce, healthcare and finance, competition law in India is also evolving to address the unique challenges presented by AI. To address these concerns, the CCI has been exploring the use of AI and other emerging technologies to detect and investigate anti-competitive practices.

Particularly, CCI, in its recent outreach activities, has expressed an interest in setting up a Digital Markets and Data Unit which will act as a centre within CCI to assess digital markets in India.[58]

One of the key concerns with the use of AI is the potential for it to be used to facilitate anti-competitive practices. For example, AI algorithms could be used to facilitate price-fixing, bid-rigging or other forms of collusion between firms.[59] This is a particular concern in industries where a few large players dominate the market, such as the telecoms or retail sectors.

Enterprises that have access to large repositories of data as a consequence of their market power have been noted to marginalise other competitors who are unable to capture the market due to lack of access to data.[60] There is also an increasing scrutiny against e-commerce entities for use of algorithms that provide preferential treatment to either the entity's own products or certain select sellers.[61]

The fast-paced nature of technological developments and the growing dependency on digital economy would compel the competition law framework to scrutinise the relationship between data, AI and market power. This increased scrutiny[62] would target regulating the use of AI applications and related algorithms to consolidate market power and subsequently engaging in anti-competitive activities.

Board of directors/governance

With increasing use of AI, the possibility and role of AI in company management and corporate governance have become prominent. At a preliminary level, there are increasing instances of AI involvement in decision-making by companies.[63] Such an involvement of AI offers companies a competitive advantage by helping strengthen decision-making processes by increasing the efficiency and effectiveness of decision-making, risk management and compliance.[64]

Within the Indian legal framework on corporate governance, there are no bars on the use of assistive technologies to aid decision-making by the board. This allows AI to increase the quality of information on which decision-making is based. With respect to having AI involvement with the possibility of replacing natural persons in the board of directors, several challenges persist. Particularly, how AI would fit into the fiduciary relationship that the Board shares with its constituencies and the duty of care they need to possess while engaging in decision-making. While AI presents plenty of opportunity in aiding decision-making, it cannot presently act as a replacement to the fiduciary duties that the Board of Directors have.

Even for AI involvement in aiding decision-making, it is necessary that the Board of Directors implement measures for data privacy, transparency in functioning of the AI and cybersecurity, and against algorithmic bias. The increasing deployment of AI raises questions concerning attribution of civil and criminal liability for any damages or harms that arise. The present use of AI technology is not error-free, and it is important to identify frameworks of liability concerning AI use. However, traditional approaches of understanding liability cannot be directly adapted to AI systems due to two reasons: unpredictability; and casual agency without legal agency.[65] Unpredictability of AI systems makes it difficult to understand the level of human intervention in the decision-making processes adopted by AI. Hence, the discourse on attribution of liability to AI systems comes down to whether a separate legal status can be granted to AI systems. The legal regime in India is yet to consider the question of whether legal agency can be granted to AI and where in the autonomous decision-making process can the liability of natural persons be identified. However, presently, the areas of government intervention captured above

focus on increasing accountability and transparency of AI systems as much as promoting its use. This indicates a cautious and preventive approach towards questions of liability wherein developers of AI systems failing to meet the identified standards of accountability may be held responsible for the consequences that arise.

Regulations/government intervention

Recognising the potential of AI in augmenting capacity in sectors such as healthcare, education and in boosting overall economic growth, India has been moving towards building an overall regulatory framework and ecosystem for AI's governance. The overarching principles and potential regulatory approaches can be identified in the proposed policy frameworks, strategy documents, discussion papers and committee reports released by the government.

MeitY and NITI Aayog have been at the forefront of directing the AI policy regime in India. They have pitched several mission plans that anticipate and harness the growth of AI in India. Up until 2020, both entities had overlapping mandates with respect to pushing the AI agenda forward in India. A committee was then set up to resolve this overlap, post which it was decided that MeitY will be responsible for the implementation of India's AI mission, a Rs. 7000 crore (approximately USD 85 billion) project, while Niti Aayog would offer planning and support to the same.[66]

A. Intervention by MeitY

In 2018, MeitY constituted four committees to promote AI initiatives in India and develop an AI policy framework. Each committee focused on a different mandate including: platforms and data on AI; leveraging AI for identifying national missions in key sectors; mapping technological capabilities; and key policy enablers. These committees released their reports in July 2019. Broadly, the key takeaways from these reports included:

- enriching the National Artificial Intelligence Resource Platform (**NAIRP**), which will bring together all publicly shareable data, information, tools, literature for collaboration on AI and enable solutions for international cooperation;[67]
- leveraging AI technology in areas of healthcare, road safety and detection of financial fraud;[68]
- promoting ethical and responsible use of AI and investing in the development of bias-free datasets for building fairness, transparency and accountability features in AI systems;[69] and
- creating necessary resources for testing and certification of AI systems, providing incentives for compliance and spreading awareness on ethical issues concerning AI.[70]

The committees also recognised creating a good foundation of technologies, intellectual property and algorithms as key for the adoption of AI.[71]

In 2019 MeiTY had set up an expert committee to deliberate on a data governance framework for India. In 2020, this committee released the 'Report by the Committee of Experts on Non-Personal Data Governance Framework'.[72] Apart from suggesting the creation of a separate national legislation and a separate authority to oversee governance of non-personal data, the committee also recommended mandatory sharing of non-personal data which may be useful for Indian entrepreneurs to develop new and innovative services or products to benefit citizens.

Following which, MeiTY released the draft National Data Governance Framework Policy (**NDGFP**) in May 2022. In the 2023 Union Budget, the government announced its intention to launch the finalised version this policy.[73] This policy intends to maximise access to and use of anonymised, non-personal public-sector data in India to deliver citizen-centric

services. It seeks to promote research, innovation and growth of India's AI and data-driven ecosystem. The NDGFP applies to all government entities and is primarily focused on government data. It applies to all data collected and managed by any government entity. The policy notes that, with its adoption, it will launch the non-personal data-based 'India Dataset' program that addresses the methods and rules to ensure that non-personal data and anonymised data from both government and private entities are safely accessible for research and innovation.[74] Indian researchers and start-ups who want to use non-personal data sets are also governed by the Policy and the standards laid down by it. The NDGFP sets up the Indian Data Management Office (**IDMO**) which is responsible for laying down rules and standards on data handling. It will prescribe implementation strategies and data-sharing toolkits for stakeholders to comply with its standards. The IDMO will be a body under MeitY.

B. Intervention by TRAI

In December 2022, the Telecommunication Engineering Centre (**TEC**) under the federal Department of Telecommunication released the *Draft Standard on Fairness Assessment and Rating of Artificial Intelligence Systems*. This voluntary standard seeks to enhance trust in AI systems by promoting bias assessment and enabling a standardised procedure for conducting it. This standard is intended to aid fair assessment of AI systems and provide a reference scale for their comparison. This standard follows the NITI Aayog's recommendation on 'Responsible AI', which seeks to ensure principles of equality, inclusivity and non-discrimination are adopted in the deployment of AI.[75] Through this, the standard provides principle-based assessment metrics for AI technologies. This standard is intended to be used by AI system developers for self-assessment for arriving at a set of fairness scores and for auditing and testing AI systems and issuing fairness certificates. The standard also prescribes the structure for the fairness evaluation outcome report, which is to be prepared after the AI system has been evaluated in accordance with the standard.

In August 2022, the Telecom Regulatory Authority of India (**TRAI**) released a *Consultation Paper on Leveraging Artificial Intelligence and Big Data in Telecommunication Sector.* This emphasises the need for standardising the meaning of overlapping principles like 'Trustworthy AI/Responsible AI/Explainable AI' and identifying a definition for AI. It suggests the creation of an authority that will create guidelines for data sharing between industry and the government and between government agencies. It also suggests that the industry should work to harness data generated from each node of their networks for further AI innovations. This includes setting up data hubs and industry sharing data with the government. The paper also suggests how accreditation of AI products and solutions will help in public procurement of AI.

Thus far, the TRAI's intervention focuses on suggesting principle-based mechanisms to address AI-related risks and promote responsible and trustworthy AI systems.

C. Intervention by NITI Aayog

In February 2021, the NITI Aayog released the *Approach Document for India, Part 1: Principles for Responsible AI*.[76] This document is meant to serve as a roadmap for greater adoption of AI in India. It establishes ethics principles for the design, development and deployment of responsible AI. The document suggests the adopting of a 'graded risk-based approach' to different AI use cases across different sectors. The document lists two societal concerns – psychological profiling and the adverse impact of AI/automation on existing jobs. It argues in favour of regulations for specific use cases of AI and supports a risk-based approach to AI regulation wherein only high-risk use cases would be subject to harder regulations. The document also mentions the requirement of a law for AI in India. In August

2021, the NITI Aayog released the *Approach Document for India, Part 2: Operationalizing Principles for Responsible AI*.[77] This document discusses the role of the government, private sector and research institutions in implementing the principles discussed in Part 1 of the series. This document suggests that under a risk-based approach for regulating AI, the potential for harm should determine how stringent regulatory intervention should be. It supports self-regulation for low-risk cases and adopting a sandbox framework for cases where the risk is unknown. Distinct from Part 1, this document suggests that existing legislation and sectoral regulation is sufficient for governing AI in the present. The document proposes the creation of a Council for Ethics and Technology that works as an advisory think-tank for the operationalisation of a 'Responsible AI for All' framework. The document suggests that the government's role should include developing policies for responsible AI adoption and promoting 'inclusive and non-discriminatory AI' to balance the interests of preserving privacy and accumulating data for innovation.

In November 2022, the NITI Aayog that serves as a think tank of the government released the *Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology.*[78] The paper uses the Ministry of Civil Aviation's 'Digi Yatra Programme' as a case study to identify risks and mitigation strategies of using facial recognition technology (**FRT**). It recommends mitigation strategies based on responsible AI principles, which include safety and reliability, inclusivity and non-discrimination, equality, privacy and security, transparency, accountability, and protection and reinforcement of positive human values. It also recommends the backing of robust data protection regulation for FRT technology, explainable algorithms, independent systems audits of FRT algorithms and human-in-the-loop review aspects of AI algorithms in FRT.

Sectoral Guidance

Healthcare

In March 2023, the Indian Council for Medical Research released the 'Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare'.[79] The guidelines recognise the transformative potential of AI in healthcare, with focus on accessibility, affordability and improving the quality of care. The guidelines acknowledge the need for an ethically sound policy framework to guide the development and application of AI in the healthcare sector. It recognises the need for accountability and responsibility at all stages of deployment of AI in healthcare.

Finance

With financial technologies finding an increasing stronghold in India's banking sector, the use cases for AI[80] in the sector have also increased. Of importance is the use of AI technology in the credit delivery process.[81] Use cases of AI in digital lending span throughout the lifecycle of the lending process – right from credit assessment to customer identification, customer onboarding, loan application processing, risk assessment and fraud detection.[82] With the intention to regulate increasing use of digital technologies in the financial sector, the Reserve Bank of India (**RBI**), which is India's central bank and regulatory body responsible for the regulation of the Indian banking system, issued its 'Guidelines on Digital Lending'[83] that aim to reduce the influence of unregulated fintech entities in the lender–borrower relationship. The guidelines state that creditworthiness assessments done using technology (which can include AI technology) must be carried out in an auditable way, to ensure that transparency and contestability of decisions is maintained. Further, RBI's '*Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps Digital*

Lending'[84] that was released prior to the guidelines, broadly recommends the use of 'glass-box models' to enhance transparency and acceptability of algorithms, documentation of the rationale for algorithmic features aiding lending decisions and the auditability of use of algorithms.

E-commerce

In 2022, the Department of Consumer Affairs released the framework for safeguarding and protecting consumer interest from fake and deceptive reviews in e-commerce.[85] The *Online Consumer Reviews: Principles and Requirements for their Collection, Moderation and Publication*[86] is a voluntary guideline document, that recognises the use of automated tools for moderation of reviews. Particularly, it recognises automated moderation through filtering and rejection of content based on a pre-determined set of criteria that establishes content suitability for publication.[87]

Advisory against deep fakes

Recently, in February 2023, MeiTY issued an advisory[88] to target and remove false information in the form of deep fakes. This advisory was issued to Chief Compliance Officers of social media platforms such as Twitter, Facebook, Instagram and WhatsApp. The advisory requires social media platforms to ensure that they take 'reasonable and practicable' measures to take down deep fakes from their platforms within 24 hours of receiving a complaint.

Conclusion

The present vision for AI regulation focuses on flexible, policy-based approaches that are intended to promote the increasing use of AI in a transparent, responsible and fair manner. The overarching principles adopted by the government in its various programmes and policy papers on AI indicate the foundational principles of this framework to be safety, non-discrimination, transparency and accountability. However, some uncertainties remain pertaining to protection to be accorded to AI creations, the role of AI in corporate governance and liabilities accruing from AI-based decision-making. Considering this, it is necessary that the evolving regulatory framework of AI also focus on clarifying these existing ambiguities while promoting increased AI adoption.

* * *

Endnotes

1. Analytics India Magazine, *The State of AI in India 2022*. Available at https://analyticsindiamag.com/the-state-of-ai-in-india-2022/#:~:text=AI%20market%20size%20in%20India,have%20been%20making%20towards%20digitalisation.
2. Digital India Campaign – Catalyzing New India's Techade. Available at https://www.mygov.in/campaigns/digital-india/.
3. Money Control News, *Govt to launch 'largest' AI-based datasets programme by April: Rajeev Chandrasekhar,* March 9, 2023. Available at: https://www.moneycontrol.com/news/business/govt-to-launch-largest-ai-based-datasets-programme-by-april-rajeev-chandrasekhar-10222371.html.
4. Deccan Herald, *MeiTY forms task force to draft IndiaAI roadmap by April End,* March 14, 2023. Available at https://www.deccanherald.com/national/north-and-central/meity-forms-task-force-to-draft-indiaai-roadmap-by-april-end-1199960.html.

5. Varun Ramdar, *Digital India Act Consultations: The promise of a whole-of-government approach bodes well for digital economy,* Money Control, March 14, 2023. Available at https://www.moneycontrol.com/news/opinion/digital-india-act-consultations-the-promise-of-a-whole-of-government-approach-bodes-well-for-digital-economy-10248621.html.
6. Ministry of Electronics and Information Technology, *Proposed Digital India Act, 2023,* presented on March 9, 2023. Available at https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf.
7. *Id,* p. 19.
8. *Id,* p. 23.
9. Budget 2023–24, Speech of Nirmala Sitharaman, Minister of Finance, delivered on February 1, 2023. Available at https://www.indiabudget.gov.in/doc/budget_speech.pdf#page=18.
10. Chethan Thathoo, *Budget 2023–24: Decoding the Government's Artificial Intelligence Pitch,* Inc 42, February 2, 2023. Available at https://inc42.com/buzz/budget-2023-24-decoding-the-governments-artificial-intelligence-pitch/.
11. Budget 2023–24, Speech of Nirmala Sitharaman, Minister of Finance, delivered on February 1, 2023. Available at https://www.indiabudget.gov.in/doc/budget_speech.pdf.
12. *Id,* p. 18.
13. Mohit Nair and Arathi Sethumadhavan, *AI in healthcare: India's trillion-dollar opportunity*, World Economic Forum October 18, 2022. Available at https://www.weforum.org/agenda/2022/10/ai-in-healthcare-india-trillion-dollar/.
14. Parul Saxena, *AI impact on India: AI in education is changing India's learning landscape*, IndiaAI, January 10, 2022. Available at https://indiaai.gov.in/article/ai-impact-on-india-ai-in-education-is-changing-india-s-learning-landscape.
15. Naman Agrawal and Himanshu Agrawal, *Intelligent inputs revolutionising agriculture,* NITI Aayog Science Reporter, February 2021. Available at https://www.niti.gov.in/sites/default/files/2021-09/IntelligentInputsRevolutionisingAgriculture.pdf.
16. Ministry of Electronics and Information Technology, *Artificial Intelligence*, Press Information Bureau, March 30, 2022. Available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1811372.
17. IndiaAI, NASSCOM Responsible AI Resource Kit. Available at https://indiaai.gov.in/responsible-ai/homepage.
18. Ministry of Electronics and Information Technology, Future Skills Prime. Available at https://futureskillsprime.in/about-us.
19. Ministry of Electronics and Information Technology, *Empowering youth to be future ready*. Available at https://responsibleaiforyouth.negd.in/home.
20. *Id.*
21. Analytics India Magazine, *The State of AI in India 2022*. Available at https://analyticsindiamag.com/the-state-of-ai-in-india-2022/#:~:text=AI%20market%20size%20in%20India,have%20been%20making%20towards%20digitalisation.
22. The Global Partnership on Artificial Intelligence. Available at https://gpai.ai/about/.
23. Ministry of Electronics and Information Technology, *After assuming the G20 presidency, Shri Narendra Modi Government to assume the Chair of Global Partnership of AI (GPAI)*, Press Information Bureau, November 20, 2022. Available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=1877503.
24. Ministry of External Affairs, *G-20 and India's Presidency*, Press Information Bureau, December 10, 2022. Available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882356.

25. Samir Saran and Anirban Sarma, *India will prioritise data for development at G20,* Observer Research Foundation, December 14, 2022. Available at https://www.orfonline.org/research/india-at-g20-will-herald-data-for-development/.
26. IndiaAI, *India AI will become a global innovation and research brand: MoS Rajeev Chandrasekhar,* March 14, 2023. Available at https://indiaai.gov.in/news/india-ai-will-become-a-global-innovation-and-research-brand-mos-rajeev-chandrasekhar.
27. Section 2(o), the Copyright Act 1957.
28. Section 14(b), the Copyright Act 1957.
29. Section 13(1)(a), the Copyright Act 1957.
30. *R.G Anand v M/s Delux Films & Ors.* AIR 1978 SC 1613.
31. Section 13(1)(1a), the Copyright Act 1957.
32. Section 55, the Copyright Act 1957.
33. Section 63, the Copyright Act 1957.
34. Section 64, the Copyright Act 1957; *Eastern Book Company and Ors. v. D.B. Modak and Ors.* (2008) 1 SCC 1.
35. Section 13(1)(a), the Copyright Act 1957.
36. *Eastern Book Company v D.B. Modak* 2002 PTC 641.
37. Section 2(d)(vi), the Copyright Act 1957.
38. *Rupendra Kashyap v Jiwan Publishing House Pvt. Ltd.* 1994 (28) DRJ 286.
39. *Navigators Logistics Ltd. v Kashif Qureshi & Ors.* 254 (2018) DLT 307.
40. https://www.managingip.com/article/2a5d0jj2zjo7fajsjwwlc/exclusive-indian-copyright-office-issues-withdrawal-notice-to-ai-co-author.
41. Section 2(j), the Patents Act 1970.
42. https://ipindia.gov.in/writereaddata/Portal/IPOGuidelinesManuals/1_86_1_Revised__Guidelines_for_Examination_of_Computer-related_Inventions_CRI__.pdf.
43. *Ferid Allani vs Union Of India & Ors.*, W.P. (C) 7/2014 and CM Appl. 40736/2019.
44. *Ferid Allani vs Union Of India & Ors.*, W.P. (C) 7/2014 and CM Appl. 40736/2019.
45. Guidelines for Examination of Computer Related Inventions (CRIs) 2013. Available at https://ipindia.gov.in/writereaddata/Portal/IPOGuidelinesManuals/1_36_1_2-draft-Guidelines-cris-28june2013.pdf.
46. Para 5.4.5, Guidelines for Examination of Computer Related Inventions (CRIs) 2013. Available at https://ipindia.gov.in/writereaddata/Portal/IPOGuidelinesManuals/1_36_1_2-draft-Guidelines-cris-28june2013.pdf.
47. NASSCOM, India Patents Report Innovations from India: Transcending Barriers. Available at https://nasscom.in/system/files/publication/Emerging-Patente-April-2022-V8.pdf.
48. Section 6(1)(a), the Patents Act 1970.
49. Section 2(1)(p), the Patents Act 1970.
50. Para 8.3, Parliamentary Standing Committee on Commerce, 161st Report – Review of the Intellectual Property Rights Regime in India, July 23, 2021. Available at https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/13/141/161_2021_7_15.pdf.
51. Article 39(2), The Trade Related Aspects of Intellectual Property Rights (TRIPs) Agreement. Available at https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm.
52. *Mr. Diljeet Titus, Advocate vs Mr. Alfred A. Adebare And Ors.* 2006 (32) PTC 609 Del.
53. *John Richard Brady and Ors. v Chemical Process Equipments Pvt Limited & Anr* (AIR 1987 DEL 372).

54. *Burlington Home Shopping Pvt. Ltd. vs Rajnish Chibber* 61 (1995) DLT 6.
55. *Tata Motors Limited & Anr v State of Bengal*, G.A. No. 3876 of 2008 on January 12, 2010.
56. Ministry of Corporate Affairs, *Government constitutes Competition Law Review Committee to review the Competition Act,* Press Information Bureau, September 30, 2018. Available at https://pib.gov.in/newsite/PrintRelease.aspx?relid=183835.
57. Ministry of Corporate Affairs, *Report of Competition Law Review Committee,* July 2019. Available at https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf.
58. National Conference on Economics of Competition Law, Special Address by Dr. Sangeeta Verma, March 3, 2023. Available at https://cci.gov.in/advocacy/publications/speeches/details/115/0.
59. In Re: Alleged Cartelization in the Airlines Industry, *Suo Motu* Case No. 03 of 20.
60. *Delhi Vyapar Mahasangh v Flipkart Internet Private Limited and Amazon Seller Services Private Limited*, Case No 40/2019, Order dated January 13, 2020.
61. *Delhi Vyapar Mahasangh v Flipkart Internet Private Limited and Amazon Seller Services Private Limited*, Case No 40/2019, Order dated January 13, 2020.
62. Competition Commission of India, Address by Chairperson dated May 20, 2022. Available at https://cci.gov.in/advocacy/publications/speeches/details/102/0.
63. Initiative For Applied Artificial Intelligence, *AI for Boards: Gearing up for the future of business*. Available at https://aai.frb.io/assets/logos/211018_AIforboards_E_Screen.pdf.
64. Deloitte, *State of AI in India*, December 2021. Available at https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/in-State-of-AI-in-India-noexp.pdf#page=7.
65. Peter M Asaro, *The Liability Problem for Autonomous Artificial Agents,* Association for the Advancement of Artificial Intelligence, 2015. Available at https://peterasaro.org/writing/Asaro,%20Ethics%20Auto%20Agents,%20AAAI.pdf.
66. Surabhi Agarwal and Yogima Seth Sharma, *MeitY to implement AI mission, while NITI Aayog will help in planning,* Economic Times, December 25, 2020. Available at https://economictimes.indiatimes.com/tech/tech-bytes/meity-to-implement-ai-mission-while-niti-aayog-will-help-in-planning/articleshow/79950502.cms?from=mdr.
67. Ministry of Electronics and Information Technology, *Report of Committee A on Platforms and Data on Artificial Intelligence,* July 2019. Available at https://www.meity.gov.in/writereaddata/files/Committes_A-Report_on_Platforms.pdf.
68. Ministry of Electronics and Information Technology, *Report of Committee C on Mapping Technological Capabilities, Key Policy Enablers Required Across Sectors, Skilling and Re-Skilling, R&D,* July 2019. Available at https://www.meity.gov.in/writereaddata/files/Committes_C-Report-on_RnD.pdf.
69. *Id.*
70. Ministry of Electronics and Information Technology, *Report of D on Cyber Security, Safety, Legal and Ethical Issues,* July 2019. Available at https://www.meity.gov.in/writereaddata/files/Committes_D-Cyber-n-Legal-and-Ethical.pdf.
71. Ministry of Electronics and Information Technology, *Report of Committee C on Mapping Technological Capabilities, Key Policy Enablers Required Across Sectors, Skilling and Re-Skilling, R&D,* July 2019. Available at https://www.meity.gov.in/writereaddata/files/Committes_C-Report-on_RnD.pdf.
72. Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-personal Data Governance Framework,* December 2020. Available at

https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.
73. Gargi Sarkar, *Union Budget 2023–24: Government to Launch National Data Governance Policy,* Inc42, February 1, 2023. Available at https://inc42.com/buzz/union-budget-2023-24-government-to-launch-national-data-governance-policy/.
74. Ministry of Electronics and Information Technology, *Draft National Data Governance Framework Policy,* May 2022. Available at https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf.
75. NITI Aayog, *Responsible AI for All: Approach Document for India, Part 1 – Principles for Responsible AI,* February 2021. Available at https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.
76. *Id.*
77. NITI Aayog, *Responsible AI for All: Approach Document for India, Part 2 – Operationalizing Principles for Responsible AI*, August 2021. Available at https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf.
78. NITI Aayog, *Responsible AI for All, Adopting the Framework*: *A Use Case Approach on Facial Recognition Technology,* November 2022. Available at https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf.
79. Indian Council of Medical Research, *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare*, March 2023. Available at https://main.icmr.nic.in/sites/default/files/upload_documents/Ethical_Guidelines_AI_Healthcare_2023.pdf.
80. Tejamoy Ghosh, *How Fintech players are leveraging AI/ML to bridge the gap in MSME lending*, The Times of India, May 25, 2022. Available at https://timesofindia.indiatimes.com/blogs/voices/how-fintech-players-are-leveraging-ai-ml-to-bridge-the-gap-in-msme-lending/.
81. Anubhutie Singh and Srikara Prasad, *Artificial Intelligence in Digital Credit in India*, Dvara Research, April 13, 2020. Available at https://www.dvara.com/research/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/.
82. *Id*.
83. Reserve Bank of India, *Guidelines on Digital Lending*, September 2, 2022. Available at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF. (Accessibility may be limited outside of India.)
84. Reserve Bank of India, *Report of the Working Group on Digital Lending Including Lending through Online Platforms and Mobile Apps*, November 18, 2021. Available at https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF. (Accessibility may be limited outside of India.)
85. Ministry of Consumer Affairs, *Centre launched framework for safeguarding and protecting consumer interest from fake and deceptive reviews in e-commerce*, Press Information Bureau, November 21, 2022. Available at https://pib.gov.in/PressReleasePage.aspx?PRID=1877733.
86. Bureau of Indian Standards, *Online Consumer Reviews – Principles and Requirements for their Collection, Moderation and Publication,* November 2022. Available at https://www.medianama.com/wp-content/uploads/2022/12/19000_2022.pdf.
87. *Id,* p. 11, point 6.5.3.
88. Dia Rekhi, *Weed out 'deep fakes', MeitY tells social media platforms,* Economic Times, February 22, 2023. Available at https://economictimes.indiatimes.com/tech/

technology/weed-out-deep-fakes-meity-tells-social-platforms/articleshow/98131043.cms?from=mdr.

* * *

Acknowledgments

The authors would like to thank Dhruv Bhatnagar, Pallavi Sondhi and Pranav Mody for their contributions to the preparation of this chapter.

Nehaa Chaudhari
Tel: +91 853 0166 662 / Email: nehaa@ikigailaw.com

Nehaa heads Ikigai's public policy practice. She is a *Chambers and Partners* ranked lawyer for TMT. *The Legal 500* has consistently ranked her as one of India's best lawyers for data protection. Nehaa helps her clients understand, strategise and skillfully navigate India's regulatory and policy ecosystem. She works with several international technology giants, global venture capital firms, Indian and global industry associations, some of India's most innovative start-ups (including unicorns) and think tanks. She also advises the Indian government on technology law and policy.

Earlier, Nehaa worked with the Centre for Internet and Society, India (CIS), and the Berkman Klein Center at Harvard University. At CIS, she was the only Indian civil society representative in international copyright and broadcasting treaty negotiations at the World Intellectual Property Organization. She was also a member of various Indian government committees on these areas. Nehaa has taught at the NALSAR University of Law, NLU, Delhi, and IIM, Indore. She has authored a module on intellectual property rights for UNESCO. She has spoken on television news and events around the world.

Aman Taneja
Tel: +91 997 1765 114 / Email: aman@ikigailaw.com

Aman is an IP and technology lawyer. He has expertise in dealing with all aspects of online content regulation, including issues of intermediary liability, the regulation of curated content platforms and advertising regulations. He also leads a lot of the firm's work on emerging tech areas such as AI, drones and food tech. Prior to joining Ikigai, he worked for four years with the litigation team at Anand and Anand, New Delhi. He was part of the firm's IT and e-commerce law practice group. He also did a short stint with the IT legal team at Shell. Aman received the Netherlands Fellowship Programme scholarship to pursue his Master's degree in law and technology from Tilburg University. His views on Indian law and policy have been carried by media houses and publications such as *The Indian Express*, *The Times of India*, *MediaNama*, *Tech Circle*, *India Ahead TV* and *Mojo Story*.

Namratha Murugeshan
Tel: +91 876 2452 148 / Email: namratha@ikigailaw.com

Namratha is a lawyer and policy researcher. Her areas of interest include AI and emerging technologies. At Ikigai, she works on policy and regulatory issues concerning AI, e-commerce regulation and competition regulation. Prior to joining Ikigai, she worked at the Vidhi Centre for Legal Policy as a research fellow and has previously worked as a legislative assistant to a Member of the Indian Parliament.

Ikigai Law / Ikigai Business Consulting

D-295, Defence Colony, New Delhi, India – 110024
URL: www.ikigailaw.com / Email: contact@ikigailaw.com

Ireland

David Cullen
William Fry LLP

Introduction

Ireland has a long-standing track record as a key location for many of the world's leading technology companies. It will undoubtedly be at the forefront of artificial intelligence (**AI**)-driven investment. Crucial to this has been the fact that the governance of AI, machine learning and big data fall within Ireland's existing laws. This is in part due to a national strategy of ensuring up-to-date laws in a technology hub and in part due to the use of technology neutral terminology to avoid what might otherwise be speedy obsolescence in regulating such a fast-moving sector. AI has been identified by the Irish Government as an area in which it intends to be an international leader. There will also be alignment with important international standards, such as those derived from EU laws, such as the AI Act, the AI Liability Directive (**AILD**), the Data Act, the Data Governance Act and the Machine Products Regulation.

Ireland published its National AI Strategy in July 2021, which includes: an "*AI Ambassador*", who champions AI as a "*positive for change*"; an Enterprise Digital Advisory Forum, which assists with industry adoption of AI; and two European Digital Innovation Hubs (**EDIHs**). These EDIHs are the first of four hubs for the promotion of Ireland as a prominent AI development location, and part of Ireland's membership in a pan-European network.

Several notable AI-related trends have emerged.

Trends

Will the Irish regulatory framework governing AI reconcile with appropriate ethics in society as contained in the EU Commission's AI Strategy?

The launch of AI chatbots (such as ChatGPT) and other AI tools (such as Midjourney, an art generator) indicates a keen appetite for the everyday use of emerging technologies by the wider public in Ireland and elsewhere, with users taking advantage of their capabilities in natural language processing, generative capability and machine learning to perform a wide variety of tasks – to solve problems, access information, produce artistic works and streamline business processes. The rapid pace at which these products and services have become ubiquitous, hugely popular, and increasingly important to many organisations' business strategies has been notable. In tandem, however, issues have been raised about the potential for deployment of deep-learning models by bad actors or for unethical purposes.

A structure that places emphasis on both legal and ethical considerations is essential, not just from a commercial perspective, but also as a cornerstone of positive public engagement in which consumers can trust AI systems. Ireland's legal and regulatory approach to AI will align with the ethical proposals set out in the EU Commission's AI Strategy. By placing

people at the core of AI, it provides a clear path for Ireland and the EU to "*safeguard the respect for our core societal values*" and become "*a leader in cutting-edge AI that can be trusted throughout the world*".

In a William Fry survey, we asked C-suite industry leaders from over 300 firms worldwide if they shared concerns when it came to ethical issues that arise in relation to the deployment of AI. Seventy-eight per cent agreed that they did, while 83% believed that regulation would help businesses adjust to AI's future impact.

The system under the EU's AI Regulation (**AI Act**) to identify and categorise unacceptable-risk AI systems, high-risk AI systems and minimal-risk AI systems, provides a good framework for dealing with the ethical considerations raised in the current debate in Ireland. In particular, the AI Act's regulation of high-risk AI systems by establishing rules and obligations for developers, deployers and users of AI technologies, including an outright ban on AI systems that are harmful to humans, should assist to fulfil this purpose. This will be particularly influential given that almost two-thirds of Irish businesses in Ireland are expected in a significant way to use AI or machine learning this year, while other surveys show that Ireland has the highest share of enterprises in Europe using AI.

Enforcement by the Irish Data Protection Commission (**DPC**)

There are a multitude of laws in place to regulate various aspects of data use and more coming soon. With the volume of data used by AI systems, compliance with these laws is essential in order to maintain reputational integrity and avoid the extensive fines that organisations can receive under laws such as the General Data Protection Regulation (**GDPR**). AI companies should note that risk assessments will be needed to ascertain the relevant category applicable to the AI system and, if it is a high-risk system, an impact assessment may be required. We explore the relevant aspects of Ireland's data protection laws further below.

In 2022, the DPC imposed a fine of €405 million on Meta Platforms Ireland Limited (**Meta**) in relation to its Instagram services for breaching the privacy rights of teenagers. It also imposed a further fine of €265 million on Meta in relation to its Facebook services for failing to comply with its obligations to implement technical and organisational measures to ensure compliance with data protection obligations by design and by default.[1] There are similar obligations (and fines) under the AI Act.

In Ireland and elsewhere in Europe, data protection authorities are reviewing the ways in which AI organisations are processing personal data and their compliance with the GDPR. Recently, the Italian data protection authority temporarily banned a widely used chatbot developed by AI over privacy concerns, including that it had unlawfully collected personal data from its users and had no system in place to verify the age of its users. The company could face a fine of up to €20 million or 4% of its annual turnover. The DPC has stated that it will work with the other European data protection authorities to address concerns over the amount of data that is used and processed by AI systems at an EU level.

We also expect to see an increased commercial and regulatory focus on the issue of text and data mining (**TDM**). This is an aspect of AI technology in which large amounts of data are selected and analysed for purposes such as extraction, pattern recognition and semantic analysis.

While exceptions are allowed for reproduction of copyright works for the purposes of TDM under the Copyright and related rights in the Digital Single Market Directive (**CDSM**),[2] this legislation specifically disallows the processing of personal data unless it complies with the GDPR and data protection law.

It remains to be seen whether third-party content providers, operating with large datasets and potentially without legal basis, under Article 6 of the GDPR if they have not obtained authors' consent, could find themselves facing an enforcement action by the relevant supervisory authority.[3]

Contractual issues: legal liability will continue to be a sticking point in future AI contracts

Allocation of risk and liability is possibly the most significant contractual issue arising between customers and vendors. As we see an increase in organisations utilising AI as part of their product or service offering, liability needs to be thoroughly considered in contracts for the use and purchase of systems using AI. When dealing with consumers, additional care is required. Consumer Protection Legislation, including the Sale of Goods and Supply of Services Act 1980, and the Product Liability Act 1991, imply terms in consumer contracts preventing the exclusion of liability. Also, when vendors are considering limiting their liability under a contract, they should note that Irish law follows the common law doctrine of privity of contract. This means that it will not be possible for third parties to make a claim under the contract against the vendor. Instead, another legal route must be followed, such as a claim under the tort of negligence.

Liability clauses

Businesses that deploy emerging technologies as part of the product or service they provide to end users should be cognisant to the fact that where the use of their product or service causes harm to third parties, the way in which liability is apportioned under their contract with end users will dictate the commercial risk to which they are exposed.

Clear legal drafting is particularly important where it is the case that there is a lack of explainability in the use of AI systems. Liability clauses must be drafted in a transparent manner, for example, by clearly setting out the intended parameters of the system's use, or in the case of generative AI, by clearly excluding liability for infringements of third-party IP rights. The elements of an AI system that are in a supplier's control should be set out as part of this transparency exercise. While how a contract will be drafted will likely depend on the strength of each party's bargaining power, suppliers will benefit from stating in granular detail the circumstances which will give rise to liability. Customers, on the other hand, should conduct fact-finding exercises to assess liability and to consider whether particular outcomes really are solely in the control of autonomous systems, for example, or whether these are actually issues which form part of a supplier's control.

Ownership/protection

Ireland's Intellectual Property (**IP**) regime is facing novel issues resulting from the deployment of emerging technologies. Certain provisions of Irish law arguably go further than IP law *acquis* of the EU. As a result, Ireland potentially offers unique protection to an organisation's AI or deep-learning models in certain circumstances. One of the challenges under modern IP legal theory is that authorship is being seen as increasingly hard to reconcile with the concepts of machine learning or autonomous systems, i.e., where works are created without the instructions of humans.

Copyright

Ireland's copyright regime is contained in the Copyright and Related Rights Act 2000 (**CRRA**), which protects copyright in a "*computer program*", specifying "*a program which is original in that it is the author's own intellectual creation and includes any design materials used for the preparation of the program*".

A "*computer-generated*" work under Section 2 of the CRRA is one that is generated by a computer in circumstances where the author of the work is not an individual. The author of this type of work is the person by whom the arrangements necessary for the creation of the work are undertaken. Section 21(f) states: "*In this Act, "**author**" means the person who creates a work and includes: … (f) in the case of a work which is computer-generated, the person by whom the arrangements necessary for the creation of the work are undertaken.*"

While an absence of case law means that the legislation is yet to be tested, it is notable that this Irish provision departs from the EU copyright position, which requires human authorship for copyright to vest in a work. The legislation appears to derive from the idea of a legal entity model, i.e., one that infers the existence of natural persons behind a legal entity instructing it.

TDM

The CDSM and Irish Regulations implementing it provide for an exception to the reproduction copyright in works for the purposes of TDM, even if for commercial purposes, if the rights in such works have not been expressly reserved "*in an appropriate manner*" with regard to TDM. This "*appropriate manner*" includes, for online works, metadata and terms and conditions for a website or a service, and if not available online, it must be communicated to everyone who has lawful access to the work. The UK High Court proceedings initiated by Getty Images against Stable Diffusion will test the UK's "*fair dealing*" exception to copyright infringement. If a similar case is initiated in Europe or Ireland, the reproduction exception in the CDSM will likely play a significant role, along with Ireland's equivalent *"fair dealing"* exception under the CRRA.[4]

Patents/trade secrets/confidentiality

Patents in Irish law are governed by the Patents Act 1992 as amended (**Patents Act**). A patent shall be patentable if "*it is susceptible of industrial application, is new and involves an inventive step*".[5] However, computer programs are not considered to be an invention,[6] meaning much of the scope for patentability relating to emerging technologies are untested under Irish law.

Similarly, there is no decision that a machine can be classified as an inventor for the purposes of the Irish Patents Act. "*Inventor*" is defined as "*the actual deviser of an invention*", which appears to leave the question open; however, Section 80, relating to co-ownership of patents, refers to co-owners as "*two or more persons*" [*emphasis added*]. This aligns with the decisions of the European Patent Office (**EPO**) in J8/20 and J9/20, in which the Legal Appeal Board of the EPO confirmed the EU position under the European Patent Convention (**EPC**) that an inventor must be a person with legal capacity.

Due to the difficulties in patenting abstract ideas, acquiring meaningful patents on AI systems is not straightforward. Some companies are using trade secret protection to protect their AI-related IP. Trade secrets are governed by common law and the European Union (Protection of Trade Secrets) Regulations 2018, whose provisions mirror the definition of "*trade secret*" contained in the equivalent EU Directive (2016/943).

There may be some protection as an algorithm. Under Irish law, in order for an algorithm to be classified as a trade secret, there are three essential criteria:

- it must be actually secret;
- it must have actual or potential commercial value; and
- there must be reasonable efforts made to keep it a secret.

Antitrust/competition laws

Data as raw material for deploying AI, and the control of its supply as raw material, could potentially generate a market-distorting advantage if left unregulated.

AI-related anti-competitive behaviour

Indications of the adaption of Ireland's regulatory regime to potential market abuses are becoming visible. Strict information requirements are imposed on businesses when entering "*off-premises*" or "*distance*" consumer contracts, requiring businesses to inform consumers where "*the price of the goods, digital content, digital service or service was personalised on the basis of automated decision-making*".[7] This aligns with the position of the Irish Competition and Consumer Protection Commission, which has previously stated that in the case of personalised pricing algorithms, there should be specific information requirements which mirror the European Commission's New Deal for Consumers.

Domestic regulation

The Competition Act 2002 (as amended) prohibits anti-competitive behaviour by undertakings in Irish law. Section 4 of the Competition Act 2002 is based, by analogy, on Article 101 of the Treaty on the Functioning of the European Union (**TFEU**) and is concerned with situations where undertakings come together to create anti-competitive agreements, conduct concerted practices or take anti-competitive decisions. Section 5 prohibits undertakings from abusing a dominant position in trade for any goods or services. This provision is based on Article 102 of the TFEU. Whether Irish law or the TFEU is relevant will depend on the territorial impact of the arrangements.

It is possible that the issue of "*algorithmic pricing*" i.e., the automated re-calibration of prices based on internal and external factors such as market data or competitors' prices, may constitute potential anti-competitive behaviour or a concerted practice.

Board of directors/governance

A major trend for Irish businesses is the integration of AI into their business models. To date, Irish enterprises have been engaging AI mainly for purposes such as business administrative processes, production processes and ICT security. Other uses include marketing and sales purposes, human resource management and management of enterprises. As AI becomes increasingly embedded in the business operations of many companies, directors will need to be aware of their new obligations to ensure compliance with the law when deploying AI in their businesses. This applies not only to upcoming EU legislation, but also how the integration of this technology interacts with their existing duties as directors under the Companies Act 2014.

The current draft of the AI Act provides for fines of €30 million or 6% of global turnover, whichever is higher.[8] To comply with the AI Act, board members will need to be aware of the broad definition afforded to AI under it and first assess whether the systems they are providing or using fall within its scope. Risk assessments will also need to be carried out to ascertain whether an AI system is deemed to have an unacceptable level of risk, or if it creates a high or medium/low risk, as the Act prescribes differing rules in respect of each case. If it is decided that high-risk AI systems are being used or provided, a regulatory regime which should include regular formal risk assessments, data processing impact assessments, detailed record keeping and requirements around human oversight will need to be implemented.

Directors will need to consider these issues themselves: due to the emphasis on collective as well as individual duties, it will not be sufficient to delegate the task to a designated committee

or individual.[9] Additionally, under the Companies Act 2014, directors are under a fiduciary duty to act in good faith in the best interests of the company, act honestly and responsibly in relation to conducting the affairs of the company, and exercise due care, skill and diligence. As AI systems have transformative power for businesses, a decision by a board of directors for (or against) deploying AI will be relevant to assessing the performance of their duties. Directors who choose to implement AI will need to be scrupulous to mitigate the risks of AI, such as bias, issues in the structure and quality of data, and lack of explainability in the model, to ensure that the decision is taken in the best interest of the company.

Data protection

Ireland's domestic data protection legislation is central to the use and application of AI. The Data Protection Act 2018 (**DPA 2018**) and the European Communities (Electronic Communications Network and Services) (Privacy and Electronic Communications) Regulations 2011 provide for data privacy in electronic communications. The DPA 2018 implemented certain operational and discretionary national matters as required by the GDPR.

The GDPR

Several provisions of the GDPR apply to the governance of AI in Ireland. The GDPR imposes strict rules in relation to the use of personal data for AI systems. Article 35 requires those processing personal data "*using new technologies*" to carry out an assessment of the impact of the processing where that processing is "*likely to result in a high risk to the rights and freedoms of natural persons*". Those developing AI to process personal data will need to assess whether their AI systems are high-risk, in which case a data protection impact assessment would need to be carried out.

Controllers are required to implement appropriate technical and organisational measures to ensure that they achieve data privacy by design and by default.[10] It is crucial that developers of AI consider these obligations and embed data privacy features into their systems at the outset and only process data necessary for each specific purpose of the processing.

There is also a prohibition on individuals being subject to a decision based solely on automated processing, which is relevant to "*profiling*".[11]

There is an overarching principle of transparency in the GDPR which obliges controllers to be clear about the processing of personal data undertaken.[12] AI organisations should be alert to the complexities of AI-based processing. It is crucial for developers to consider transparency at the outset as it can be difficult to achieve transparency when the processing of AI systems cannot be fully anticipated.

Irish context

The GDPR permits for certain derogations. Irish law is permitted to restrict the scope of data subjects' rights and controllers' related obligations in several articles of the GDPR in certain circumstances.[13] The DPA 2018 provides that this can be done when processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes[14] or where processing for purely journalistic purposes or academic, artistic or literary expression.[15]

Member States are required to set a minimum age at which online service providers can rely on a child's own consent to process their personal data.[16] The DPA 2018 sets this age of this digital consent at 16. Organisations using AI may need to seek the consent of a child's parent or guardian, where that child is under the age of 16, in order to rely on consent as the legal basis for processing a child's personal data.

Open data & data sharing

Ireland has implemented the European Union (Open Data and Re-use of Public Sector Information) Regulations 2021, to give effect to the EU Open Data Directive 2019/1024. The purpose of the regulations is to make machine learning, AI and the Internet of Things (**IoT**) more accessible, to address emerging blocks to publicly funded information and to stimulate digital innovation, particularly in relation to AI.

The data sharing regime requires high-value datasets to be made available for re-use free of charge in machine-readable formats and via APIs and, where applicable, as a bulk download.

Civil liability

Liability is expected to be a key consideration for businesses that deploy AI.

Products liability

Under the Liability for Defective Products Act 1991, the definition of a "*product*" includes all movables including movables incorporated into another product or into an immovable. Products incorporating AI are included in this definition of a "*product*" and covered by the legislation. The type of damage that is captured under the Act comprises of "*death or personal injury*" or damage to any item of property, other than the defective product itself, provided that the property is a type intended to be used for private consumption or was used by the injured person for private use or consumption. However, given the passage of time since the drafting of the legislation, while the Liability for Defective Products Act 1991 can be applied to products incorporating AI, it is not fit for purpose to adequately deal with the intricacies of such products due to advancements in digital technologies and how AI affects the operation of products.

While the current framework does apply to products that incorporate AI, Ireland will transpose laws to give effect to the EU Commission's proposed specific AI liability framework to address the issue of damage caused by AI systems, including its proposal for an AILD and a Product Liability Directive (**PLD**).

AILD

The AILD will set down uniform rules for certain areas of non-contractual civil liability for damage caused where AI systems are involved, and substantially increase the liability risk for businesses which incorporate AI systems into their products and/or services. If damage is caused by a system which incorporates AI, a victim of damage will not need to prove that the damage was caused by the AI system, but rather, the deployer/owner of the AI system will have to prove that the AI system did not cause damage. There will be a rebuttable presumption that the AI system caused the damage. This means that businesses providing products or services incorporating AI systems will need to reconsider their contracts, particularly in relation to warranties, indemnities, and caps and exclusions from liability. Insurers may also need to reassess how they insure businesses incorporating AI systems.

Revised PLD

The PLD modernises the rules and is designed to provide an effective compensation system at an EU level to those that suffer physical injury or damage to property as a result of defective AI. The PLD takes into account changes in how products are produced, distributed and operated, expanding the concept of "*product*", as outlined under the Liability for

Defective Products Act 1991, to include "*digital manufacturing files and software*". All digital products will be covered, and the rules are modified to work for new and emerging technologies. The PLD covers cyber weaknesses and updates to software and AI systems. Cyber-security issues and failure to provide necessary software updates will be considered "*defects*" for the purposes of product liability cases.

Criminal issues

In relation to policing in Ireland, the DPC has in the past expressed concern over the certain proposed uses of facial recognition systems in relation to the *Garda Síochána* (Digital Recording) Bill 2021. Similarly, the proposed *Garda Síochána* (Recording Devices) Bill 2022 has come under scrutiny for posing risks to privacy and data protection from the Irish Council for Civil Liberties, with concerns raised that the lack of effective safeguards and legal bases for processing special-category data means that the 2022 Bill is not in compliance with the DPA 2018 or the GDPR.

While the 2021 bill provided for "smart" body-cameras to be worn by members of the *Garda Síochána* (Irish police), which can facilitate automatic facial recognition and automatic profiling and tracking of individuals, the 2022 bill also includes expanded CCTV use and access to third-party CCTV and drones. The DPC noted that there was no legislative basis within the DPA 2018 for this type of processing of special-category data.

Several national data protection authorities in Europe have taken issue with mass surveillance and the use of biometric data. In 2022, the French, Italian and Greek data protection authorities each respectively imposed a €20 million fine on an AI company that sells facial-recognition software to law enforcement agencies in the USA for breaches of the GDPR (unlawful processing of personal data and a failure to respect individuals' rights under the GDPR). The GDPR was applicable even though the company did not offer its services in the EU because the company monitored the behaviour of people in the EU. The data protection authorities also imposed a ban on the further collection of data and on the further processing of the biometric data of individuals in France, Italy and Greece and to delete any existing data held on these individuals. The DPC will likely take the same position as its European counterparts if a similar complaint is filed in Ireland.

Discrimination and bias

Discrimination in AI can stem from biased training data, skewed algorithms, lack of diversity in data, and the unconscious biases of those implementing and deploying the AI itself. Ireland's anti-discrimination regime is well established and implements the Equal Treatment Directive 76/207. The Equal Status Acts 2000–2018 prohibit discrimination in the provision of goods and services, accommodation and education. These laws can be used to protect individuals from discrimination in certain instances such as where AI is utilised in the selection of tenants in residential properties, or in the case of applicants for schools and colleges.

In the employment sphere, the Employment Equality Act 1998 was enacted to affirm the European principles of non-discrimination. In Ireland this applies to discrimination on the grounds of gender, marital status, family status, sexual orientation, religion, age, disability, race and membership of the traveller community. These nine equality grounds, by law, must be respected in the recruitment process of employees. It is possible that this protection could extend to instances in which the initial stages in a recruitment process have little human interaction and/or are dependent on AI.

Further, Ireland's Gender Pay Gap Information Act 2021 requires employers to publish details on pay differences between male and female employees. This may impact organisations' utilisation of AI to accurately track pay in companies and report real data to identify problems in companies and remove latent bias.

National security and military

In the EU, suppliers of technology systems that are susceptible to influence by foreign actors or states may pose a threat to national security. This can occur where a body acting in bad faith attempts to gain access to a technology provider's customer data for surveillance or intelligence purposes. Ireland, amongst other EU Member States, has witnessed the presence of companies who have been deemed to be subject to this type of influence, predominantly in the communications sphere, and who may pose a surveillance or intelligence threat. The Irish Government has recently moved to introduce the Communications Regulation Bill 2022, which will allow it to ban companies from supplying technology to mobile networks where they are deemed to pose a "*threat to national security*". It will also give Government ministers powers to designate parts of a communications network as being "critical or sensitive" and exclude network technology from "*high-risk vendors*" being used in those critical areas. The Bill is currently still in draft stage.

In addition, Ireland implements sanctions, or restrictive measures, in accordance with the EU's Common Foreign and Security Policy (Article 215 TFEU), as well as in relation to "*preventing and combating terrorism and related activities*" (Article 75 TFEU).

Conclusion

Many companies are keen to harness the potential of AI to improve their product or service offering, to help employees to focus on business-critical tasks, to speed up processes or to cut costs. Ireland is a leading hub in Europe with respect to the share of enterprises using AI, with two thirds of Irish businesses and IT leaders predicted to implement AI in their organisations by the end of this year. Ireland's forward-looking national strategy for AI, along with its unique status as the sole English-speaking common law jurisdiction in the EU and its low corporate tax rate, has ensured that the country is a welcoming home for businesses hoping to capitalise on the benefits of this technology.

* * *

Endnotes

1. Article 25 GDPR (EU) 2016/679.
2. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 3. April 2019 on copyright and related rights in the Digital Single Market (CDSM Directive), transposed into Irish law by Regulation 4 of S.I. No. 567/2021 - European Union (Copyright and Related Rights in the Digital Single Market) Regulations 2021 (Irish CDSMD Regulations).
3. Article 17 CDSM.
4. Section 51(1) CRRA.
5. Section 9(1) Patents Act 1992.
6. Section 9(2) Patents Act 1992.
7. Schedule 3 Consumer Rights Act 2022.
8. Article 71(3) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL

INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS.

9. Ahern, Deirdre "The Impact of AI on Corporate Law and Corporate Governance", *The Cambridge Handbook of Private Law and Artificial Intelligence*, 11 November 2021. Accessed 5 April 2023. http://www.tara.tcd.ie/bitstream/handle/2262/101064/AI%20AND%20CORPORATE%20LAW%20.pdf?sequence=1&isAllowed=y.
10. Article 25 GDPR.
11. Article 25 GDPR.
12. Article 5 GDPR.
13. Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) GDPR.
14. Section 61 DPA 2018.
15. Section 43 DPA 2018.
16. Article 8 GDPR.

David Cullen
Tel: +353 1 639 5000 / Email: David.Cullen@williamfry.com

David is a Partner and Head of William Fry's Technology Group, specialising in complex technology matters and the strategic protection and development of intellectual property, in particular for online and digital markets. David has represented multinational clients on: the development, implementation and operation of several national IT infrastructure projects; all aspects of data protection and privacy, dealing with large scale data and security breaches and cybersecurity; corporate data protection/privacy-related projects including advising on various matters involving the Office of the Data Protection Commissioner, audits, PIAs, preparation for GDPR, group implementation of policies and review of existing policies & procedures; and negotiation of complex commercial contracts including outsourcing and naming rights agreements.

William Fry LLP

2 Grand Canal Square, Dublin 2, D02 A342, Ireland
Tel: +353 639 5000 / URL: www.williamfry.com

Italy

Massimo Donna
Paradigma – Law & Strategy

Trends

Adoption

In 2022, overall artificial intelligence ("**AI**") investments have topped 500 million Euros, a 32% increase from 2021. As expected, the lion's share of AI investments has been generated by larger corporations, 61% of which have stated to have AI programmes in place, whilst only 15% of small and medium-sized enterprises ("**SMEs**") can declare as much. As for the specific applications which have been the bulk of AI investments as of late, a survey has shown that they include Intelligent Data Processing, Natural Language Processing, Chatbots, Recommendation Systems, Computer Vision and Robotic Process Automation. Such a promising AI adoption trend is in line with and very relevant to Italy's overall economic performance. In fact, in 2022, Italy sealed the end of the COVID-19 pandemic by posting significant GDP growth, also thanks to the successful deployment of the European Recovery Fund.

AI Strategic Programme

In this context, it is noteworthy that Italy used part of such funds to roll out its Strategic Programme on Artificial Intelligence, which was approved by the Italian Government on 24 November 2021 and periodically adjusted. The Strategic Programme is aimed at boosting AI research in Italy by promoting its general understanding and appeal to younger generations, with the final goal of making Italy an important AI hub. Of course, the AI that Italy is seeking to promote has all the characteristics that the EU has been clarifying over the past few years, i.e. it is human-centred, trustworthy and sustainable and shall be deployed in all of the Country's strategic sectors such as industry and manufacturing, the education system, agri-food, hospitality, health, infrastructure, etc. AI is also considered a fundamental tenet of the modernisation of Italy's public administration.

By adopting and rolling out the Strategic Programme, Italy is making a robust effort to catch up with some of its partners within the EU, which have traditionally invested more in AI. In fact, whilst over the past few years concern was growing that Italy's industrial core was not being swift enough in adjusting to the AI and robotics revolution, the COVID-19 crisis has truly been a litmus test for the Country's industrial preparedness, and the outcome is surprisingly positive.

To fully appreciate where the development of AI solutions currently stands in Italy, it should be remembered that Italy's entrepreneurial landscape is very different from that of its European neighbours. In fact, most Italian businesses are SMEs that 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. Indeed, the latest data show that Italy is sixth worldwide for the number of installed industrial robots, and that patent registrations relevant to AI-related inventions have decidedly picked up lately.

The Strategic Programme emerges off the back of several previous efforts to boost AI. In fact, in 2020, the Italian Government set up a group of experts tasked with setting out the AI strategy for Italy and ensuring that the positive adoption trend does not falter going forward. The outcome of such an ambitious project was a report released in October 2020, which identifies the underlying principles upon which the Italian AI strategy should be built and the main areas on which government action or guidance should be focused, and makes several policy recommendations. So, as for the industries where AI use should be boosted, the Italian AI Strategy Report ("**IASR**") identifies manufacturing and the Internet of Things ("**IoT**"), finance, healthcare, transportation, food, energy and the defence sector. The public sector should also play an important role in the implementation of the Italian AI strategy, on the one hand by making the great trove of data it collects available through the Open Data initiative, but also by increasingly using AI for its institutional tasks.

Whilst some of the recommendations appear immediately actionable, others may be interpreted as calling for excessive *ex ante* regulation, as we will see in the following sections.

Also, the urgency with which the IASR appears to be encouraging industrial SMEs to join forces and enter into Data Sharing Agreements to leverage their joint data resources does not seem to factor in the actual data scale necessary to effectively trigger the algorithmic leverage.

Concerns

The Italian Regulators' concerns were heightened by the introduction of ChatGPT, an AI chatbot developed by OpenAI and launched in November 2022, which is built on top of OpenAI's GPT-3.5 and GPT-4 families of large language models and was also developed by using both supervised and reinforcement learning techniques. On 31 March 2023 the Italian Data Protection Authority ("**DPA**") stunned the tech community – and the public in general – by imposing a temporary ban on all data processing carried out by OpenAI, the firm behind ChatGPT.

In fact, the Italian regulator found no legal basis for the processing of the personal data as training data, and pointed out that data subjects in Italy were never provided with an information notice as required under article 13 GDPR.

The DPA explained that the information provided by ChatGPT is often incorrect, which amounts to inaccurate data processing. The exposure to such incorrect data could imperil minors, especially in consideration of the fact that Open AI has failed to verify ChatGPT users' age.

The ban was imposed with immediate effect, and the regulator pointed out that breaching it may trigger a criminal sanction of up to three-years' prison time, as well as the sanctions under article 83 GDPR.

The regulator granted OpenAI 20 days to justify its conduct and to indicate which measures have been taken to comply with the DPA ban. On 28 April 2023, the DPA announced that the ban on ChatGPT had been lifted as a result of OpenAI introducing certain measures to enhance data protection. In particular, OpenAI, among other things, posted a new, more detailed information notice on its website, made it easier for European users to oppose the

processing of their personal data for AI learning purposes, and set up an age-verification button. Many commentators criticised the AI ban as, in their opinion, it achieved very limited results on the data protection front, whilst at the same time cutting Italy out of the AI scene for a month at a time when that technology is developing at a breakneck pace.

In general, lately Italian regulators have been concerned as regards AI's potential biased and discriminatory outcomes, and its ability to allow granular levels of surveillance and influence. The expectation of the imminent adoption of the EU AI Act (the proposed Regulation on AI) has, of course, deterred national lawmakers from adopting any country-specific legislation that may conflict with EU law. However, it should be noted that the proposed AI Act is already stirring some controversy in Italy, with particular reference to "General Purpose AI", i.e. AI with multiple possible uses in different contexts. In fact, it has been pointed out that since the EU AI Act's classification of systems as high-risk AI (which triggers heavier regulatory requirements) is based on the AI's "intended use", this might allow general purpose AI's users to elude the requirements and obligations attached to AI systems.

Ownership/protection

In the absence of a statutory definition, it was left to the Administrative Court to define AI. In fact, the Italian Supreme Administrative Court, on 25 November 2021, ruled that whilst an algorithm is a "*finite set of instructions, well defined and unambiguous, that can be mechanically performed to obtain a determined result*", AI is when "*an algorithm includes machine-learning mechanisms and creates a system which not only executes the software and criteria (as in a "traditional" algorithm), but that constantly processes data inference criteria and takes efficient decisions based on such processing, according to an automatic learning mechanism*". The definition is certainly not waterproof from a technical or legal standpoint, but it is still note-worthy.

Most recently, the discussions around the intellectual property ("**IP**") 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; (iii) whether the training or deployment of AI may breach third-party IP rights; and (iv) whether AI inventions are eligible for patenting.

(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 also be granted under articles 98 and 99 of the Industrial Property Code (*Codice della Proprietà Industriale*), which protect know-how. In fact, provided 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. Certain commentators argue than not only data-sets but also algorithms themselves

could be protected 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, the first few weeks of 2023 have seen the release of the latest version of ChatGPT as well as other similar Generative AI applications, which can be used to carry out an extremely broad range of tasks and activities, including the creation of AI-generated artwork. In this respect, whilst Italian law is clear in requiring that copyright holders be natural persons, it is still debated whether artwork created by a natural person leveraging the power of AI can be copyright protected. In this respect, a very recent ruling of the Italian Supreme Court stated, incidentally, that an artist can invoke copyright protection in respect of an artwork created with the support of software; however, in such a case, the degree of the software's contribution should be specifically assessed. In other words, the Supreme Court's ruling could be interpreted as a first timid nod to the possibility that an artwork created by way of prompting an AI chatbot could be eligible for copyright protection, provided that the prompt is specific (and *per se* creative). Also, 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 from 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, whilst in other jurisdictions artists have already sued AI solution providers claiming breach of copyright, we are not aware of any such case being brought to Court in Italy yet.

(iv) As for whether AI inventions are eligible for patenting, the European Patent Office ("**EPO**") DABUS decisions, by which it was ruled that only inventions where the stated inventor is a natural person are eligible for patent application, have – for the time being – discouraged any opinion to the contrary at national level. On 21 December 2021, such decision was confirmed by the EPO Legal Board of Appeal.

In a context in which case law has not yet had the opportunity to validate most commentators' theories on AI's IP implications, in 2019, Italian Administrative Courts had a chance to rule on the relationship between algorithmic transparency and IP. 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 that supplied the

algorithm to prepare a brief explanation as to 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. It is interesting to note that, subsequently, CONSOB, the financial markets regulator, proposed a more nuanced solution to the need to balance consumers' protection and AI's IP. In fact, in its June 2022 publication "*Artificial Intelligence in Asset and Wealth Management*", the watchdog has proposed that financial intermediaries, rather than being forced to disclose the algorithms and data-sets that they utilise to the general public, should only be obliged to share them with the financial regulator.

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 permitted 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 ("**EFD**") 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 EFD 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 EFD 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 EFD 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 DPA (*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 shown 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, whilst 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 enforcing 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.

Quite notably, the IASR appears to be trying to revive the "Data as Essential Facility Doctrine", but only with regard to data gathered by IoS and Industry 4.0 solution providers in compliance with the relevant solutions' purchase or licensing agreements. It appears, therefore, that the IASR is not advocating regarding consumer data as an essential facility. We expect that the regulators' focus on data will increase as a consequence of the coming into force of the Data Governance Act, the Digital Services Act and the Digital Markets Act.

More recently, both the UK Competition and Markets Authority and the US Federal Trade Commission have announced that they will examine the AI market, as the expensiveness of the technology behind AI risks compressing competition. At the time of writing, no such standing has been taken by the FCA.

Board of directors/governance

Company Directors are under the obligation to perform their duties with diligence and appropriate technical skills. Pursuant to article 2086 of the Civil Code, Company Directors must set up an organisational, administrative and financial corporate organisation adequate to the relevant business's size and characteristics, also with a view to providing timely warning of the company's financial conditions and detecting possible upcoming insolvency. Under article 2381 of the Civil Code, the Board of Directors – which may include both executive and non-executive Directors – must jointly assess the corporate organisation as it was set up by the executive Directors. In this context, as AI solutions become more available, Company Directors are increasingly expected to make use of AI to ensure that such structure is adequate, both by acquiring sufficient familiarity with AI and by ensuring

that the Company's Chief Information Officer, Chief Data Officer and Chief Technical Officer are regularly consulted or even appointed as Board members.

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, including 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 have been 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 to the applicable legislation and, if not, act swiftly to remedy the situation.

Recently, some legal commentators have argued that since Company Directors are under the obligation to make their decisions based on adequate information, such obligation may include an implicit obligation to act based upon AI-based decision-support tools. For example, when the Board of Directors is convened to decide whether the company should enter into a certain long-term contractual commitment with a third party, such third party's credit score becomes of paramount importance, and the Directors may be liable *vis-à-vis* shareholders and creditors if it were proved that their decision was based on a credit score determined by using weaker methods than state-of-the-art AI.

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, the IASR appears to have adopted a different approach, as it highlighted the need for AI-specific legislation. For example,

among other things, the IASR appears to recommend that commercial agreements having AI solutions as objects should be forced to include statutory standard contractual clauses.

Finally, 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 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 a 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 notion that AI should be regarded as a "dangerous activity" is also promoted by the IASR authors, who also suggest adjusting the liability regime of AI developers and marketers to that of animal owners. However, other commentators have been reluctant to extend the "animal intelligence" liability regime to AI.

Legal commentators have been increasingly questioning whether "AI Agents" could be granted rights and be burdened with obligations, in other words whether, in addition to natural persons and legal persons, *ad hoc* "robotic persons" should have been introduced in the Italian legal system. In fact, as increasing AI adoption has deepened concern over potential liabilities, some thought that such concerns could be addressed by holding AI responsible by way of granting it a robotic-person status, which would be similar to that that slaves used to enjoy in Ancient Rome. Although fascinating in principle, such proposals have been promptly criticised on the grounds that AI Agents would not be owning assets and, therefore, it would be pointless to hold them liable.

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 has decreased below a certain point.

It is hard to assess whether the above creative legal thinking will be backed by the 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

Predictive policing and crime prevention

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 large 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 unacceptably 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 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? Whilst 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 is 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.

Predictive justice

In Italy, as in other jurisdictions, AI-based or AI-enhanced proceedings have sometimes been considered a possible step forward towards more unbiased criminal justice. However, at the time of writing there are still (too) many issues preventing the swift entering of algorithms in criminal justice; the main obstacle being everyone's right to be sentenced by way of a motivated legal decision, which right would be breached by the black-box nature of most AI algorithms. In fact, the internal workings of algorithms may not only be made obscure by algorithm vendors to protect their IP, but in some cases might have evolved autonomously using machine-learning techniques, to an extent that not even the algorithm creator can grant access to its workings.

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 can 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.

CONSOB, the Financial Markets watchdog, has also warned that financial intermediaries using AI to carry out adequacy assessments could end up discriminating against clients, for example based on their ethnicity, if algorithms and data-sets were not checked and verified appropriately.

National security and military

The Italian military has traditionally been both a NATO pillar and instrumental to UN peace-keeping and peace-enforcing missions worldwide.

The Ministry of Defence has published a document detailing the latest AI-based solutions which have been adopted or are in the process of being assessed by the Italian armed forces.

In parallel, Leonardo S.p.A., an Italian-headquartered, state-co-owned multinational defence contractor, has increased its focus on AI applications on a number of fronts. In fact, to this end, Leonardo has installed the Davinci-1, a "supercomputer" ranked among the 100 most powerful worldwide, at its Genoa (Italy) site. The Davinci-1 will allow Leonardo to consolidate and boost its leadership in fields such as autonomous intelligent systems, high-performance computing, electrification of aeronautical platforms and quantum technologies.

The increased military focus on AI solutions has started to prompt early debates among legal scholars who, for the time being, appear to be focused on human AI and robotic enhancements and their potential constitutional impact.

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 matters, including financial innovation, blockchain and cybersecurity as well as technology-driven M&A. Massimo routinely lectures on a range of technology law matters.

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 & Taiki Matsuda
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 ageing society after the decrease in the birth rate. Several policy and funding programmes are being implemented by Japanese governmental authorities. Under such governmental initiatives, the collection of big data through the Internet of Things ("IoT") and the development of data analysis technology through AI are making rapid progress in Japan.

Not only are computers and smartphones connected to the Internet, but also various types of equipment and devices, such as vehicles and home appliances, and the digital data collected via such equipment and devices is utilised.

Technologies used 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 implements a general policy on 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

In 2016, the Japanese government issued its 5th Science and Technology Basic Plan (2016–2021) to further Japan's goal to lead the transition from "Industry 4.0" to "Society 5.0", a new concept to solve the challenges facing Japan and the world and to build a future society that brings prosperity by focusing on human-centric values in a new approach of integrating cyberspace and physical space. The 6th Science and Technology Basic Plan (2022–2026) states that the goal should be to make Society 5.0 a reality.

The Japanese government issued "Social Principles of Human-Centric AI" in March 2019. The "Social Principles of Human-Centric AI" are based on the following basic philosophy: 1) dignity: a society that has respect for human dignity; 2) diversity and inclusion: a society where people with diverse backgrounds can pursue their well-being; and 3) sustainability:

a sustainable society in which AI is expected to make a significant contribution to the realisation of Society 5.0 and the need for a society that is compatible with the use of AI (AI-Ready Society). In order for AI to be accepted and properly used, society (especially regional legislative and administrative bodies) should pay attention to "Social Principles of AI", and developers and operators engaged in AI R&D and social implementation should pay attention to "R&D and Utilization Principles of AI".

Based on the basic philosophy of the "Social Principles of Human-Centric AI", the Japanese government published the "AI Strategy 2022" as a follow-up to the AI Strategy 2019. In the AI Strategy 2022, the course to be taken to deal with imminent crises such as pandemics and large-scale disasters is clarified, as well as new objectives to enhance implementation in society.

Based on the above AI principles, in July 2021, the Ministry of Economy, Trade and Industry (METI) issued "Governance Guidelines for Implementing AI Principles" for AI businesses (revised in January 2022). These guidelines are not legally binding, but they present action targets to be implemented by AI companies in order to support the AI principles and facilitate use of AI. They provide hypothetical examples of implementation of AI principles corresponding to each of the action targets and practical examples for gap analysis between AI governance goals and the *status quo*. It is expected that AI companies will use it as an important reference.

1.3 Key legal issues

The 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 that 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 that 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 applicable law 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 General Data Protection Regulation ("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 that 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? 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 that 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 a 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 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 Centre ("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

The local competition authority, the Japanese Fair Trade Commission ("JFTC"), has been working to create an environment that prevents improper acquisition and use of data. 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 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 (algorithm 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. The JFTC published a report titled "Algorithms/AI and Competition Policy" in March 2021. The report states that while cartel activity using algorithms can basically be dealt with under current antitrust laws in many cases, it is necessary to continue to monitor changes in technology, trends in their use, and related cases for category (iv).

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 share 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.

In June 2021, the JFTC published a report titled "Study Group on Competition Policy Related to Data Markets". The report expresses concern over monopolisation by digital platforms that accumulate a large amount of data through network effects, as well as the exclusion of competitors and impediments to new entrants, and points out the need to take care not to intervene excessively in these matters, in order to avoid hindering innovation.

3.4 Latest trends: the JFTC's position on enforcement against digital-related vertical restraints

The JFTC publicly announced in December 2018 that it 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 this context, the JFTC conducted a survey of the contracting practices of large digital platformers in January 2019 and the Digital Platform Transparency Act adopted in 2020 became effective as of February 1, 2021. This Act regulates large-scale online malls and app stores, by requiring certain disclosures and measures to ensure fairness in operation in Japan (to be caught by the Act, the domestic sales thresholds are 300 billion yen and 200 billion yen for online malls and app stores, respectively).

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. Bilateral adequacy referrals on cross-border data transfer restrictions between the EU and Japan came into effect in January 2019. AI and big data-related issues from a data protection perspective in Japan can be explained 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 was amended in 2020 and the amendments came into force as of April 1, 2022, introducing (*inter alia*) the

concept of pseudonymised personal data, which will boost AI activity otherwise stifled by privacy restrictions.

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 other than the sufficient disclosure of purpose of use.

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 would 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 Level 4 automated driving on express highways for private cars by around 2025. In November 2020, the Ministry of Land, Infrastructure, Transport and Tourism certified a car using Level 3 autonomous driving technology developed by Honda Motor Co. Ltd. ("Legend") and intended for production lines for the first time in the world. The Road Transport Vehicle Act ("RTVA") and the Road Traffic Act ("RTA") were amended in 2019 (effective in 2020) to achieve the government's goal. The following is an outline of these amendments.

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 permitted.
(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 the modification of programs used for automated driving systems.

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, 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.

In addition, the RTA was amended in April 2022 (effective April 2023) to lift the ban on Level 4 and enable unmanned automated mobility services, with only remote monitoring, in certain geographical areas.

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 would be imposed. Another amendment was implemented in 2020 to introduce its extra-territorial application. Also, as explained in section 3.4 above, the Platform Transparency Act adopted in 2020 became effective as of February 1, 2021.

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 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 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 must be able to foresee the occurrence of specific results and to avoid such results arising from the actions of the AI. However, the actions of AI are almost unforeseeable for AI users given that its judgment process is not known to them at all. From this standpoint, it is unlikely that 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 actions of AI. At least at the early stage of AI introduction, it is not appropriate to rely fully on the actions of AI and AI users are likely to be required to comply with a certain degree of duty of care by monitoring the actions 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 the 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 the 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 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 also advises many Japanese and foreign clients on data security issues, in terms of Japanese laws, Singapore PDPA and the GDPR, including structuring of global compliance systems. He is a graduate of 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 Defence). He is a graduate of University of Tokyo (LL.B., J.D.) and Columbia Law School (LL.M.).

Taiki Matsuda
Tel: +81 3 3214 3215 / Email: taiki.matsuda@iwatagodo.com
Taiki Matsuda is an associate at Iwata Godo. He is an attorney-at-law (admitted in Japan). His practice focuses on general corporate matters and a wide variety of domestic dispute resolution. His practice also includes corporate governance, shareholders' meetings and M&A. He graduated from Hitotsubashi University (LL.B., 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

Malta

Ron Galea Cavallazzi, Sharon Xuereb & Alexia Valenzia
Camilleri Preziosi Advocates

Trends

The unparalleled global growth of, and interest in, artificial intelligence ("**AI**") has caused great tension in legal fields, particularly in the data privacy and information technology sectors. Since their inception in the 1950s, AI, big data, and machine learning have gained tremendous momentum, especially in recent years, possibly owing to their mainstream implementation. Legal norms will persistently be strained as AI becomes increasingly complex and adept at completing "life-like" tasks when utilising machine learning.

In 2019, Malta set up an AI taskforce that was entrusted with:

i. finding ways to create a sustainable local engine for growth;
ii. looking into the unknown risks of AI without hindering innovation and economic development; and
iii. creating a new sector for investment on the Maltese islands.[1]

On 3 October 2019, Malta launched its national AI strategy, called "Malta the Ultimate AI Launchpad: A Strategy and Vision for Artificial Intelligence in Malta 2030" (the "**Strategy**").[2] The Strategy is aimed at mapping the path for Malta to gain a strategic competitive advantage in the global economy as a leader in the AI field.

In addition to the Strategy, Malta created a new authority in 2018 called the Malta Digital Innovation Authority (the "**MDIA**").[3] The purpose of the MDIA is to seek the development of the innovative technology sector in Malta through proper recognition and regulation of relevant innovative technology arrangements and related services. The Innovative Technology Arrangements and Services Act (the "**ITAS Act**") was enacted along with the establishment of the MDIA.[4] The ITAS Act allows for the certification of innovative technology arrangements by the MDIA, which include: distributed ledger technologies; decentralised ledger technologies; and smart contracts.[5] The ITAS Act also allows other innovative technology arrangements to be accommodated within the scope of the Act, and it is expected that AI systems will be included as well.

On 1 June 2022, the MDIA launched the '*Technology Assurance Sandbox v2.0*', which is a regulatory sandbox specifically devised for start-ups and small companies to test their innovations in a controlled environment.[6] Applicants are permitted to participate in the sandbox for a maximum period of four years.

As part of the Strategy, in January 2022, the (then) Ministry for the Economy and Industry, in collaboration with the MDIA, launched a €125,000 fund for AI research projects called the MDIA AI Applied Research Grant (MAARG).[7] Applicants willing to contribute their research are able to receive up to a maximum of €25,000 toward their project. The first deadline for submission of proposals was 31 March 2022, and the last deadline was 31 December 2022. No further information on this initiative has been released to date.

One of the sectors in which the implementation of AI systems on the Maltese islands has been explored is the transport sector. This is possibly because AI may play an important part in offering a solution to Malta's daily road congestion. Researchers at the University of Malta have conducted a study into the feasibility of introducing "driverless" vehicles in Malta using AI systems, under Malta's Introduction of Shared Autonomous Mobility ("**MISAM**") project.[8] Part of the MISAM project sets out to explore the current legislative framework and propose initial solutions in respect of any gaps currently found within Maltese law, such as liability for any collisions or accidents that autonomous vehicles may cause. These are issues that will undoubtedly strain current concepts and the application of civil liability and will introduce moral dilemmas that may not be entirely addressed through traditional legal means.

Separately to the MISAM project, the Ministry for Transport, Infrastructure and Capital Projects and the Ministry for Education, in collaboration with the University of Malta and Malta Public Transport, launched an innovative research project on autonomous buses in May 2021.[9] The project will use four pre-planned routes to test self-driving public transport vehicles that will be integrated into the current public transport network. In June 2022, it was announced that this project is awaiting European funding in order for it to start.[10]

Legal issues surrounding the use of AI

The key legal issues that arise with AI systems include algorithmic transparency, cybersecurity and privacy vulnerabilities, bias and discrimination, intellectual property ("**IP**") and legal personhood issues, liability and lack of accountability. Regarding algorithmic transparency, it is understood that developers are often not keen to disclose their work. Given the proper satisfaction of certain requirements at law, such works could be considered as trade secrets in terms of the local Trade Secrets Act.[11] However, bar any confidential information, the operation and underlying operations of AI systems should be transparent and accessible to any users of such systems. That is not to say that the code underlying such systems should be rendered publicly accessible; rather, there should be a pre-determined set of information regarding AI systems that must be made publicly available. This information would include, for example, the high-level criteria that the system has used to set its parameters and the legal effects that such a system may have on its end-users.

The prevalent cybersecurity issues are obvious when one considers that the relationship between security, ease of access and efficiency of use are inversely proportional. The primary goal of security is to safeguard a particular dataset, which naturally increases the time to access or perform other processing operations on such dataset. Conversely, ease of access procedures aim to make the aforesaid more productive and time efficient, but typically at the cost of security.

Under 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 (the General Data Protection Regulation or "**GDPR**"), information society services must disable any cookies that are not "strictly necessary" by default, and providers must allow the end-user to opt in to use supplementary cookies. This minor example is exacerbated with complex AI systems, which are, by design, created to perform complex tasks efficiently with no human intervention. Therefore, any AI framework must carefully consider other pieces of

legislation, such as the GDPR and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) before they are introduced.

Industries/sectors leading the development and adoption of AI

With regard to industries and sectors benefitting from the introduction of AI systems, the private, transport, health, and education sectors stand to gain the most from prevalent use of such systems, at least in the short term.

In the private sector, AI is especially useful in conducting client due diligence assessments. AI's main strength lies in its ability to effectively recognise patterns and deduce outcomes to an effective degree of certainty. Additionally, such systems can process vast amounts of data in minimal time when compared to manual due diligence – this accuracy and efficiency could save companies ample time and resources, which can instead be allocated to other work.

Within the health sector, certain local companies have partnered with entities outside Malta to enhance the electronic patient record system and provide patients in the UK with the accessibility to set hospital appointments, reschedule or cancel them in real time. Given that the Government of Malta is currently undergoing a digital overhaul of its services, the implementation of such a system within the health sector could be well received if implemented with the appropriate safeguards. Since health data falls within the special categories of personal data under article 9 of the GDPR, an extra degree of caution (and additional safeguards) must be taken in any processing operations.[12]

Within the education sector, the University of Malta and the (then) Ministry for the Economy and Industry partnered up with the MDIA to run three projects using AI.[13] The intention behind all three projects is for them to lead to the Maltese language being written, understood and processed by modern day technology. One of the three projects, "Edu AI", targets children aged from eight to 10 years of age and uses AI-powered puppets during shared reading sessions. The AI system includes language and literacy tasks and games involving speech and text recognition.

In addition, the Centre for Literacy within the University of Malta initiated the "EduRoboKids" project to develop and promote the use of AI in the education sector.[14] The "EduRoboKids" programme targets children with learning difficulties who may benefit from communicating with social robots. The aim of the project is for such children to engage in constructive learning with an autonomous or semi-autonomous AI-driven robot, which would replicate traditional learning contexts.

During 2022, the MDIA also offered a scholarship called the *Pathfinder Digital Scholarship*, which intended to support postgraduate education in the field of Artificial Intelligence and Information Security, ensure that the Maltese labour market is supplied with the right individuals and guarantee that it is in a better position to compete at an international level.[15]

Ownership/protection

Malta's current legislative framework does not provide for *sui generis* IP rights relating to AI systems, nor does it cater for the nuances brought about by works or inventions created by AI systems. Furthermore, the Maltese Industrial Property Registrations Directorate ("**IPRD**") has not issued any guidelines or recommendations that would help tackle certain issues, such as the patentability of AI systems or AI-generated solutions.

In terms of Maltese patent law, ownership over such IP is bestowed upon the applicant, who must be a legal person in order to fulfil the criteria of the patent regulations.[16] While this is understandable when an AI system is developed using one's own intellectual endeavours, matters become increasingly complex when that system generates its own "content" or solution without the intervention of a legal person. If the AI system generates any invention without any human intervention, current patent law would not consider such invention as patentable. It is therefore necessary to update current legislation to provide for ownership of IP generated entirely by automated systems or to bestow such ownership rights to agents and consider creating an agency status for autonomous AI systems.

Code is predominantly based on arithmetic expression. Hence, AI (being code for the most part) is protected through the Maltese Copyright Act (Chapter 415 of the Laws of Malta) as a literary work, provided that the work satisfies the definition of a "computer program" found therein.[17] Computer programs must have an original character, be written down and reduced to material form by a specific author for copyright protection to arise (which protection arises automatically upon publication). Issues will arise for any work generated by the AI system, because Maltese copyright law defines an "author" as a natural person who created the work, thus excluding the possibly of automated systems being considered "authors". The main argument is whether the AI system was developed specifically to generate the work in question and, if so, whether the system was merely a "tool" utilised by the author; in this case, the system would not be deemed an author itself. Hence, while the developer of the AI system would be the owner of that system in terms of the Maltese Copyright Act, any subsequent works generated by this system fall within a lacuna that is not currently catered for by Maltese national legislation.

With regard to data privacy, the main concern is the automated processing of personal data and the scale at which this processing is done, particularly if the data subject (as defined within the GDPR) has not consented to the collection of personal data. A practical example is data crawling conducted by a law enforcement agency ("**LEA**") for the purposes of crime detection or investigation. While LEAs could arguably have a legitimate interest in scouring publicly available data as a preventative measure, one must also take note of the intrusive nature of such systems. Finding the right balance between data subjects' rights on the one hand, and the public interest in LEAs carrying out their duties on the other, is no easy task and such considerations would need to be carefully set out within the applicable legal framework.

Antitrust/competition laws

Big data in combination with AI has not changed the basic tenets of competition law. However, under certain circumstances, they also feature as a contributing factor to competition concerns, including: (i) increasing market power and facilitating exploitative or exclusionary practices by dominant firms; (ii) facilitating collusion; and (iii) merger control issues. Determining any alleged illegality depends on the factual context of each case and the legislative framework in the particular jurisdiction. Maltese (and EU) courts are yet to decide on such matters.

One relevant issue faced in the competition sector, for example, is that of algorithmic pricing, wherein an AI system utilises "big datasets" and machine learning techniques to automatically re-calibrate prices based on internal or external factors. These include supply and demand variables, competitors' prices, or external market data (which is typically purchased by the respective undertaking).

Algorithmic pricing is not deemed illegal *per se* where the information is obtained legitimately, and if the AI system was developed independently. Should the system be a result of collusion or collaboration between competing undertakings to set prices, however, then – regardless of whether the price setting was conducted orally, through correspondence or through algorithms – the basic tenets of Maltese/EU competition law remain true in an online environment as well, including the unlawful setting of prices among competitors.

Board of directors/governance

The use of AI systems in the decision-making process among a board of directors does not seem to be a novel concept in foreign jurisdictions. In Malta, the legal landscape does not specifically cater for, *inter alia*, liability regarding breaches of directors' duties or obligations, should these be decided upon by an AI system. The authors are of the view that the use of such systems in decision-making processes would not alter the directors' ultimate liability should a breach in duty be found. However, while an AI system could develop into a system that is arguably more capable of recognising complex patterns and predicting corporate outcomes when compared to a natural person, such systems lack the commercial insight, experience and "human touch" that is often required when taking decisions at board level.

Additionally, developing an AI system that can apply context to an inputted scenario is not easy, and until these hurdles are overcome, the authors do not foresee that AI will be given the lead role in the decision-making process. That said, the authors believe that a reasonable compromise could be to allow the AI system to function on a pre-determined basis and retain an advisory role with no legal authority. This may prove insightful to directors who, by default, are prone to human error, which an AI system is not.

Regulations/government intervention

The EU has drafted a proposal for a regulation to harmonise rules on AI throughout the EU (the "**Regulation**").[18] As an EU Member State, Malta will be bound by the Regulation, which will be directly enforceable without requiring national implementation. Through the Regulation, the EU seeks to define AI systems using a risk-based approach, ranging from low-risk to prohibited systems. The latter is a clear attempt to prohibit AI systems that evaluate persons based on their "trustworthiness" or social behaviour. Interestingly, the EU differentiates between "real-time" biometric scanners depending on their use-case. This is particularly important insofar as LEAs are concerned, as the only legislation that covers the processing of personal data by LEAs is Directive 2016/680 (the "**LED**"), which differs slightly from the GDPR, predominantly insofar as "consent" is used as a legal basis for processing.[19] That said, we are yet to see the interplay between the Regulation, the GDPR and the LED, and the possible limitations that the latter two may impose on such systems despite the possibility of the AI system being developed and used in compliance with the Regulation. Furthermore, the promulgation of large language models, such as ChatGPT, has called into question the relevance and practical application of the Regulation given its variety of uses. The Malta IT Law Association ("**MITLA**") held a webinar on this topic in January 2023 and published a whitepaper exploring the good, the bad and the ugly of such technologies. Within the whitepaper, the association issued recommendations to address legal and ethical concerns.[20]

AI and the workplace

MITLA's whitepaper argues that even though innovative technologies and systems invariably raise concerns *vis-à-vis* potential job losses, the fostering of these technologies

could also lead to new jobs that perhaps are not around today. In particular, the association highlighted that a model like ChatGPT could make up for certain skills shortages, and help people and organisations work more efficiently. Malta is attempting to pre-empt mass job displacement by encouraging the community to become interested in learning about this technology and the MDIA has grants and schemes in place to create interest in AI. These sentiments reflect the position put forward in the Strategy, where a plan for the impact of technology and automation on the Maltese labour market was set out.

Civil liability

Maltese legislation does not currently provide for non-contractual liability for damages caused by AI or other alternative digital technologies. *In lieu* of this, one must fall back on the provisions of the Civil Code (Chapter 16 of the Laws of Malta) to determine liability from a traditional tort-based perspective.

Therein, article 1031 establishes the principle that every person is liable for damages caused by their own fault. The standard of proof in determining such fault is that of the *bonus paterfamilias* ("reasonable man"). This standard is evident within article 1032 of the Civil Code, which provides that a person is deemed to be at fault where they fail to exercise the attention, diligence and prudence of a reasonable man. The extent of such reasonableness is only determined by the courts, which must exercise discretion in their determination. Moreover, article 1033 of the Civil Code further provides that any person who, with or without intention to injure, voluntarily or through negligence, imprudence, or want of attention, is guilty of an act or omission that breaches the duty of care as imposed by law, will be liable for any damage resulting from their negligence.

This prompts the question as to whether, if an AI system acts of "its own" volition and through no prior instructions of the developer, the owner would be indirectly liable for creating a system that gives rise to the damage.

Turning to the Product Liability Directive and its local implementation, it is evident that current liability rules do not fit "black-box" systems such as AI, which results in a number of legal complexities, particularly when it comes to proving any defects and the causal link between such defects and the damage incurred.[21]

The European Commission acknowledges the lacuna that has emerged in this respect and has already conducted an initial impact assessment roadmap on adapting civil liability rules to the digital age.[22] This assessment ultimately contributed to the EU's proposed regulation on AI.

For the purpose of civil liability, it would appear that the developer of an AI system would be deemed to be the legal person against whom claims for damages may be brought. This thinking would currently apply to damages arising both as a result of the use of the AI system itself, as well as the reliance on any of the outcomes of that system, even if such outcomes arose from the system's own processes. This is because, ultimately, it is the developer who implemented the system's "cognition". When coupled with the concept of the *bonus paterfamilias*, this entails that the developer should be liable for not implementing appropriate "fail-safes" or be found liable for producing a defective product. This would also suffice for the sake of practicality. A natural person would not be able to seek legal redress against an AI system unless a separate legal personality, or some form of agency status as a minimum, is attributed to it.

Discrimination and bias

A core concern with AI systems is the innate human bias of their developers that is embedded within the system *per se.* If one views code as an expression of the developer's self, it is not difficult to understand how such bias arises within AI systems. This has been identified as a major challenge related to the use of algorithms and automated decision-making. The principle of non-discrimination, as enshrined in article 21 of the Charter of Fundamental Human Rights of the European Union, is not to be taken lightly and must be at the forefront of any system. Potential examples of discrimination include candidates for job interviews, scores in creditworthiness or during trials, amongst others.

Therefore, it is imperative that any national AI ethical framework is drafted cautiously and implemented meticulously. In August 2019, Malta published a draft Ethical AI Framework called "Towards Trustworthy AI", which aims to establish a set of guiding principles and trustworthy AI governance and control practices. The intention is for the Malta Ethical AI Framework to support AI practitioners in identifying and managing the potential risks of AI, while also serving to identify opportunities to encode a higher ethical standard into AI. The draft document was released for public consultation in August 2019 and the final version was expected in October 2019, shortly after the release of the Strategy.[23] As of the time of writing, no further updates are publicly available. The intention is also for a National Technology Ethics Committee to be set up under the MDIA to oversee the Ethical AI Framework and its intersection across various policy initiatives, including investments in tools and continuous monitoring mechanisms, skills and capabilities, an innovation ecosystem and regulatory mechanisms.

There is also the IEEE P7003 standard for algorithmic bias considerations, which provides a development framework to avoid unintended, unjustified, and inappropriately differing outcomes for users. Therefore, it is vital that technical partners liaise heavily with legal practitioners to minimise the risk of such bias occurring and limit the detrimental effects it may cause.

While technical solutions are welcome, this should not come at the cost of a comprehensive regulatory framework and a policy focus that prioritises fairness, especially considering marginalised groups. Currently, the only such local framework is the above-mentioned Ethical AI Framework. Furthermore, Maltese legislation does not cater for nuances such as digital rights or informational self-determination, which, if not remedied, could prove cumbersome for AI systems in practice.

Conclusion

Society is currently undergoing a technological revolution, whereby technology is moulding and paving the way for the legislative landscape. AI and other advanced digital technologies will become increasingly complex and will challenge even the most long-standing legal concepts. Therefore, it is up to legislators to lead by example and use their knowledge and legal expertise to interpret (or reshape) the law in a manner that appropriately caters for such advancements. That said, it is imperative to exercise great caution with any legislative change, and to do so through interdisciplinary teams to avoid knee-jerk reactions that accommodate current short-term trends.

It is a fact that, in practice, laws are generally required to catch up with technological advancements (as with AI). If countries attempt to draft overarching policies that introduce unnecessary bureaucracy, technological developments will significantly slow down, or worse,

the industry will be forced to disregard overkill policies that hinder progress. Legislators should engage in more thorough discussions with stakeholders (both on a national and international level) to determine technical needs prior to drafting the relevant legislation.

* * *

Endnotes

1. Malta.AI Taskforce – Our Vision: https://malta.ai/malta-ai/our-vision/.
2. Malta The Ultimate AI Launchpad: A Strategy and Vision for Artificial Intelligence in Malta 2030. Available at: https://malta.ai/wp-content/uploads/2019/11/Malta_The_Ultimate_AI_Launchpad_vFinal.pdf.
3. The Malta Digital Innovation Authority Act (Chapter 591 of the Laws of Malta).
4. Chapter 592 of the Laws of Malta.
5. As defined within the Malta Digital Innovation Authority Act (Chapter 591 of the Laws of Malta).
6. Further information is available here: https://www.mdia.gov.mt/wp-content/uploads/2022/11/MDIA-Technology-Assurance-Sandbox-TAS-Programme-Guidelines.pdf.
7. Press release available at: https://economy.gov.mt/en/press-release/Pages/PRESS-RELEASE-BY-THE-MINISTRY-FOR-THE-ECONOMY-AND-INDUSTRY-%E2%82%AC125,000-fund-for-artificial-intelligence-research-projects.aspx & https://www.mdia.gov.mt/schemes/ai-applied-research-grant/.
8. Project MISAM (REP-2020-017) is financed by the Malta Council for Science and Technology, for and on behalf of the Foundation for Science and Technology, through the FUSION: R&I Research Excellence Programme. An initiative led by the Department of Spatial Planning and Infrastructure within the Faculty for the Built Environment at the University of Malta, with the support of Debono Group and Infrastructure Malta.
9. Press release available at: https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2021/May/14/pr210908en.aspx.
10. News article: https://www.independent.com.mt/articles/2022-06-08/local-news/Pilot-project-for-driverless-buses-awaiting-European-funding-to-begin-6736243549.
11. The Trade Secrets Act (Chapter 589 of the Laws of Malta).
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
13. Press release available at: https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2021/April/22/pr210764en.aspx.
14. Further information available at: https://www.um.edu.mt/literacy/edurobokids.
15. Further information can be found here: https://www.mdia.gov.mt/schemes/pathfinder/.
16. Patent Regulations (Subsidiary Legislation 417.01 of the Laws of Malta).
17. Article 2 of the Copyright Act: "computer program" includes computer programs whatever may be the mode or form of their expression, including those which are incorporated in hardware, interfaces which provide for the physical interconnection and interaction or the interoperability between elements of software and hardware and preparatory design material leading to the development of a computer program, provided that the nature of the preparatory design material is such that a computer program can result therefrom at a later stage.

18. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
19. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
20. The whitepaper is available here: https://www.mitla.org.mt/publications/chatgpt-the-good-the-bad-and-the-ugly/.
21. 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 and the Consumer Affairs Act (Chapter 378 of the Laws of Malta) and its subsidiary legislation.
22. Further information is available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en.
23. Information available at: https://malta.ai/wp-content/uploads/2019/08/Malta_Towards_Ethical_and_Trustworthy_AI.pdf.

Ron Galea Cavallazzi
Tel: +356 2123 8989 / Email: ron.galeacavallazzi@camilleripreziosi.com
Ron is a Partner at Camilleri Preziosi whose practice mainly involves Competition, Energy, Aviation, Employment and Information Technology.
Ron advises various businesses in different industries as well as State-owned entities on competition-related matters, including State aid and public procurement. Ron has gained ample experience regarding State aid, having advised the Government of Malta and other State-owned entities on a number of projects and proposed initiatives, mainly in the Energy and Information Technology sectors.

Sharon Xuereb
Tel: +356 2123 8989 / Email: sharon.xuereb@camilleripreziosi.com
Sharon's main practice areas are Media and Communications Law, Intellectual Property, Information Technology and Privacy Law. She also forms part of the firm's litigation team. Sharon retains interests in cyberspace law, computer law, electronic commerce, and online gaming and betting regulation, and concentrated on these areas in her postgraduate studies at Queen Mary University of London. In partial fulfilment of her LL.M. there, Sharon submitted a thesis on the regulation of online gaming and betting entitled "Legal Protection of State Monopolies over Online Gaming: A critical appraisal of the implications of recent ECJ decisions on EU Remote Gaming". Sharon graduated as a Doctor of Laws from the University of Malta in December 2009 after submitting her thesis entitled "Evolving Legal Frameworks: Defamation in Cyberspace".

Alexia Valenzia
Tel: +356 2123 8989 / Email: alexia.valenzia@camilleripreziosi.com
Alexia is an Associate within Camilleri Preziosi whose main areas of practice are Intellectual Property, Pharmaceutical and Healthcare, Technology and Privacy Law. Alexia obtained a Master of Laws (LL.M.) degree in Corporate and Commercial Law from the University of London via distance learning in 2020. Prior to this, she graduated from The City Law School in London after having completed the Graduate Diploma in Law course, and having obtained a first-class honours degree in Pharmacology from the University of Portsmouth in 2015. Alexia currently acts as the Secretary of the Malta IT Law Association.

Camilleri Preziosi Advocates

Level 3, Valletta Buildings, South Street, Valletta, VLT 1103, Malta
Tel: + 356 2123 8989 / URL: www.camilleripreziosi.com

Portugal

Sofia Barata, Nuno Carrolo dos Santos & Iakovina Kindylidi
Vieira de Almeida

Trends

Introduction

For the purposes of clarity, it should be noted that there is not a uniform definition of Artificial Intelligence ("**AI**") in Portugal or in the EU (with the exception of the definition of AI set forth in the Proposal for a Regulation laying down harmonised rules on AI – the Artificial Intelligence Act ("**AIA**") – and its pertinent criticism). As such, any reference to AI should be understood as referring only to machine learning, including deep-learning AI, while the terms 'AI' or 'algorithm' or 'AI system' are used interchangeably.

When identifying the main AI trends in Portugal, it is useful to distinguish between AI providers – entities that design, develop and provide AI solutions – and AI users – entities using AI solutions either internally in their organisations or to provide products and services to their end users.

AI providers market

The AI providers market is soaring in Portugal, with startups and SMEs offering a wide variety of AI-based solutions ranging from virtual assistants and translation tools to biometrics and anti-fraud solutions.

The year 2022 saw the conclusion of negotiations for the funding of various consortiums in the context of the national Recovery and Resilience Mechanism, created by the Portuguese Government as part of the Next Generation EU package of the European Council. The Recovery and Resilience Mechanism is organised on three structural dimensions: (i) Resilience; (ii) Climate Transition; and (iii) Digital Transition.

Among the consortiums selected is the Responsible AI Consortium, with the participation of 25 Portuguese entities, including two unicorns and 10 startups specialising in AI (Unbabel, Feedzai, Sword Health, Automaise, Emotai, NeuralShift, Priberam, Visor.ai, YData and YooniK), eight research centres from Lisbon, Porto and Coimbra (Champalimaud Foundation, Centre for Informatics and Systems of the University of Coimbra, Faculty of Engineering – University of Porto, Fraunhofer Portugal AICOS, The *Instituto de Engenharia de Sistemas e Computadores - Investigação e Desenvolvimento*, *Instituto Superior Técnico* ("**IST**"), IST-ID/ Institute for Systems and Robotics and IT), one law firm (Vieira de Almeida – VdA), and five industry leaders from the life sciences, tourism and retail sectors (BIAL, *Centro Hospitalar de São João*, Luz Saúde, Grupo Pestana and SONAE). The Consortium's goal is to position Portugal as a global leader in Responsible AI technologies, principles and regulation by creating 21 new AI products, standards and recommendations for regulation and best practices in Responsible AI and 132 postgraduate academic degrees, among other initiatives.

AI users market

Over the past two years, an increasing number of entities from different sectors are acquiring either off-the-shelf or tailor-made AI solutions. The following sectors have been the most active in adopting AI systems: (i) life sciences; (ii) banking and finance; (iii) insurance; (iv) public sector; (v) retail; and (vi) telecommunications. Regardless of the sector and the varying levels of complexity of the AI systems acquired, there has been a marked increase in the use of the following solutions: (i) recruitment and HR management; (ii) digital marketing; (iii) biometric data; (iv) virtual assistants; and (v) natural language models and machine translation.

Main legal challenges

The main legal challenges for AI providers or AI users can be grouped in the following categories:

- **Data:** Definition of a robust data strategy by clearly identifying the personal and non-personal data used in the various stages of the AI lifecycle, ensuring its quality for data-mining purposes, its sources and processing purposes, as well as the data protection relationships with different stakeholders.
- **Fundamental rights:** Identification and mitigation of the risks related to fundamental rights of individuals, as well as any risks related to bias and errors in datasets, and concomitantly to discriminatory outputs of AI systems.
- **Safety and (cyber)security:** Identification, implementation, monitoring and updating of organisational and technical security measures to ensure the robustness, safety and security of the AI system throughout its lifecycle, while ensuring compliance with any sector-specific cybersecurity and safety rules or international standards.
- **Intellectual property:** Clear management of the intellectual property rights relating to the results generated by AI, as well as matters related to trade secrets and other proprietary information used to train the system, while ensuring compliance with transparency obligations.
- **Transparency:** Provision of clear information to stakeholders in conformity with the consumer protection and data protection frameworks and with best business practices, including based on the reporting obligations of the AIA Proposal, to ensure future-proof governance. It should be noted in this regard that compliance with the transparency obligation does not require disclosure of the AI algorithm or of any proprietary information of the AI provider or user.
- **Accountability:** Ensuring there are technical, organisational and contractual mechanisms in place to promote the auditability of AI outputs and that the responsibility of the various stakeholders for any damages caused due to errors and biases of the AI system is clearly identified contractually, including the obligation to provide evidence and relevant information to support or refute claims.
- **Compliance:** Ensuring future-proof compliance by proactively fulfilling the AIA obligations, depending on the role of the entity, as well as specific obligations related to the intended application of AI or the sector in which the AI provider or user operates.

Government initiatives

In 2019, the Portuguese Government published its AI Portugal 2030 Strategy (available in English at: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3D BAAAAB%2BLCAAAAAAABACzMDQxAQC3h%2ByrBAAAAA%3D%3D) with the

aims of boosting innovation and investment in the AI ecosystem, attracting and retaining talent and promoting the adoption of AI across the country's various industries. These objectives translate into an Action Plan consisting of seven lines of action: (i) inclusion and education: disseminating generalist knowledge on AI; (ii) qualification and specialisation; (iii) thematic areas for research and innovation in European and international networks; (iv) public administration and its modernisation; (v) specific areas of specialisation in Portugal with international impact; (vi) new developments and supporting areas in European and international networks; and (vii) facing societal challenges brought by AI: ethics and safety. These objectives reflect to a large extent the EU Declaration of Cooperation on Artificial Intelligence of 2018, which Portugal has signed, as well as the OECD AI principles.

Furthermore, with a view to boosting innovation in emerging technologies, and as part of the Portuguese Government's Action Plan for Digital Transition (available in English at: https://portugaldigital.gov.pt/wp-content/uploads/2022/01/Portugal_Action_Plan_for_Digital_Transition.pdf), the Portuguese Government published Resolution 29/2020 of the Council of Ministers, establishing the general principles for the preparation of the legislative framework for Technological Free Zones (*Zonas Livres Tecnológicas* – ZLTs), and Decree-Law 67/2021, setting forth the legal framework for establishing ZLTs. ZLTs are real-life geographical areas set up as regulatory sandboxes aimed at promoting and facilitating research, development and testing activities related to innovative technologies, products and services, including AI, across all industries.

More recently, in 2022, the Agency for Administrative Modernisation (AMA – *Agência para a Modernização Administrativa*) published its Guide to ethical, transparent and responsible Artificial Intelligence in the Public Administration (available only in Portuguese at: https://bussola.gov.pt/Guias Prticos/Guia para a Intelig%C3%AAncia Artificial na Administra%C3%A7%C3%A3o P%C3%BAblica.pdf). This Guide provides an overview of the main characteristics of AI, the AI market and the Portuguese ecosystem, presenting a series of principles that must be followed in the use of AI systems by Public Administration.

Notwithstanding the above, since the AIA is still under negotiation, there have been no developments regarding its implementation in Portugal, particularly as to which national authority will be tasked with monitoring compliance with the AIA obligations or whether possible regulatory sandboxes, identified in the AIA Proposal as a means to promote innovation, will operate as part of the ZLT initiatives. Nonetheless, developments are expected during 2023 (please refer to the Regulations/government intervention section below).

Ownership/protection

In Portugal, there are no intellectual property provisions specifically referring to AI.

As such, the Portuguese Code of Copyright and Related Rights ("**CDADC**") and the Industrial Property Code ("**IPC**"), transposing the EU intellectual property framework into national law, are applicable.

More specifically, the AI algorithm can be protected by copyright. The rightsholder is usually the AI provider and registration is not necessary. The copyright protection of AI code expires 70 years after the AI provider's death and, since in most cases the AI provider is an entity, the copyright protection also expires 70 years after the first time the code was lawfully made available to the public.

When it comes to patents, in line with the EU Patent Law, it is difficult to patent AI systems that are not embedded in a physical device, since the patent claim usually fails to meet the

applicable inventiveness or novelty requirements. This may be because the AI system has been *trained* based on existing data, simply combining already established ideas in a new way. Demonstration of a technical implementation or application, besides from purely abstract AI methods, may be required for the acknowledgment of a technical effect and, therefore, inventive step.

In addition, depending on the specific application of the AI system, there is discussion regarding the ownership of its outputs, especially when data, trade secrets or other proprietary information of the AI user is used to train the AI system. Considering the lack of clarity in this regard, these aspects are usually resolved contractually by assigning or irrevocably licensing the modifications or improvements made to the algorithm to the AI provider.

In relation to the ownership of the data used to train and deploy the AI system, although the prevailing opinion is that there is no property right to data, in Portugal databases may be protected, as a whole or substantially as a whole, under Decree-Law 122/2000, which transposed the EU Database Directive into national law. Provided that the qualitative and quantitative requirements of the law are met, in line with the case law of the Court of Justice of the European Union ("**CJEU**"), the entity that created the database may be protected for 15 years, from the first of January of the year following the date of the creation or of the date on which it was made available to the public. In addition, the data providers enter into data sharing or database licensing agreements with AI providers and AI users.

In Portugal, there is also some theoretical discussion around the possibility of recognising some sort of intellectual property right to AI outputs. However, under the current wording of the national and EU intellectual property framework, it is not possible for an AI output to be protected by copyright or patent since human authorship/inventorship is necessary for this protection.

Antitrust/competition laws

Competition in Portugal is mainly regulated by the Portuguese Competition Act (Law No. 19/2012). However, as an EU Member State, the EU competition law framework and CJEU case law are also directly applicable in Portugal.

As in almost every field of law, competition law is not immune to the challenges posed by the digital economy. Aware of these challenges, the Portuguese Competition Authority ("**PCA**") has been strengthening its investigative toolbox to better detect indicators of potential breaches of competition rules by or with recourse to AI-driven tools or similar technologies (as per the PCA's Competition Policy Priorities for 2023).

Following the adoption, in 2019, of the *Digital Ecosystems, Big Data and Algorithms Issues Paper* (addressing the challenges that the digital transition entails for competition policy) ("**2019 Issues Paper**"), in 2020 the PCA set up a task force for the digital sector which has been investigating complaints and actively engaged in proactive investigation. In 2019, the PCA had also conducted a survey on the use of monitoring and pricing algorithms.

In December 2022, the PCA published its *Defence of Competition in the Digital Sector in Portugal* policy brief ("**2022 Policy Brief**"). This document provides an update of the PCA's policy for digital markets and a summary of its investigative and enforcement initiatives (which range from surveys sent to online retailers, open calls for information and sector-specific analysis to automated web scraping-based investigations to substantiate ongoing cases and dawn raid warrants).

What happens when machines collude?

The ever-increasing number of commercial (namely pricing) decisions that are delegated to algorithms raises serious concerns from a competition law perspective. As a result from the 2022 Policy Brief, the PCA is well aware that "*algorithms may be used to implement price fixing and alignment strategies between competitors, thus harming consumers. Monitoring algorithms may be instrumental in price collusion agreements by making it easier to detect price deviations. More sophisticated algorithms may be able to reach collusive equilibria without direct human intervention*".

Automated price surveillance and definition is particularly worrisome if pricing algorithms are coupled with the capabilities of reinforcement learning algorithms, as this creates a high likelihood of algorithmic collusion. Indeed, as EU Commissioner Margrethe Vestager stressed, "*it is a hypothesis that not all algorithms will have been to law school. So maybe there is a few out there who may get the idea that they should collude with another algorithm who haven't been to law school either*". Ranking, search, recommendation and nudging algorithms also seem to be on the PCA's radar.

In the 2019 Issues Paper, the PCA warned that companies are responsible for the algorithms they use, and that the use of these tools to coordinate market strategies is not compatible with competition law. Additionally, in the 2022 Policy Brief, the PCA hinted that it will be paying attention to situations where competitors use common algorithms to coordinate prices or where there is some conscious and deliberate consensus between competitors on price strategies. It is worth highlighting that, according to a survey carried out by the PCA on the online retail of electronic products and household appliances sector, in 2019 21% of market operators acknowledged using price monitoring algorithms and 12% confirmed using price definition algorithms for some of their products. These percentages are likely to have increased in recent years.

However, there is an ongoing debate on whether Articles 101(1) TFEU and 9(1) of the Portuguese Competition Act, as currently interpreted by the CJEU and the Portuguese Courts, are suited to tackle algorithm activity without revamping, *inter alia*, the notion of contact/communication between competitors.

What antitrust concerns arise from big data?

Similar questions may arise with the increasingly widespread use of Big Data. In its *Competition Policy Priorities for 2023*, the PCA highlighted the creation of its digital team, who will continue to investigate evidence of abuse and collusion in digital markets in close cooperation with other European authorities (in particular to ensure the interplay between competition enforcement and the Digital Markets Act).

Indeed, in May 2022, the PCA opened proceedings against Google for possible abuse of dominance in online advertising, in the form of an alleged self-preferencing practice. Following this investigation, the European Commission relieved the PCA of its competence in July 2022 and decided to investigate Google's conduct on its own initiative.

All in all, certain aspects of the current antitrust framework may need to be modernised to better address the challenges posed by the digital economy. Significant efforts have already been developed at the EU-level with the adoption of the Digital Markets Act, which aims at establishing an *ex ante* regulatory system ensuring contestability and fairness in the digital economy; yet further guidance is needed on how competition law should be applied in these scenarios.

Board of directors/governance

Directors are required to comply with any laws applicable to their company and its articles of association, but Article 64 of the Portuguese Companies Code further tasks them with the duty to act diligently and always in accordance with the company and shareholders' best interests, as well as those of relevant stakeholders (e.g. employees, clients and creditors).

Directors must be available, technically qualified and knowledgeable of the company's business if they are to perform their duties properly. In addition, they are bound by a duty of care and a duty of loyalty.

Consequently, if AI can be used as a tool to help directors make complex decisions, the intuitive reasoning would be: if you have technology that can assist you, you should use it. However, to do so legally may prove more complicated. If directors are to act diligently and make well-informed decisions, they should be able to avail themselves of any information and tools, including any AI algorithm, at their disposal. As such, it is only logical that the duty of care will sooner or later have directors relying on AI as part of their decision-making process.

We already saw that directors have fundamental duties, such as the duties of care and of loyalty. According to the "business judgment rule", directors' liability is excluded if they can prove that they were duly informed, had no personal interest in the matter and that the decisions taken were based on a solid business rationale.

This begs two questions: if there were an AI algorithm or a robot that could assist directors in their decision-making, would they be required to use it or not? And could directors be held liable for a decision made by an AI algorithm or robot?

The outright answer to the first question is no, directors are not required to use AI in their decision-making. They are completely free to use such tools, as they can help them immensely in their tasks, but it would be farfetched to say that if directors choose not to use them, they are not reasonably informed and have failed to comply with any procedural rule.

Other than in exceptional situations related to certain types of activity and obligations undertaken by corporate bodies, it would go against the business judgment rule if courts could discretionarily determine what it means to be reasonably informed in every specific case. Until AI programs are consolidated and become common tools in making a good decision, directors will not be required to use them in their decision-making process.

When answering the second question, we need to bear in mind that directors are bound by duties of care and are expected to act diligently and in accordance with the corporate interest, which means they must select, feed instructions to and monitor any AI systems used. Directors will therefore answer for system decisions as if they were their own. In other words, directors' liability is not excluded but rather increased: they will answer for both their own decisions and conduct *vis-à-vis* the company, as well as any decisions made by the autonomous governance system. Moreover, if directors were to allow the algorithms to decide alone, they would be further accountable for not having taken the necessary precautions, even if they only ratified an algorithmic decision. Nonetheless, it is important to keep in mind that AI is going to become increasingly autonomous and is already starting to be considered indispensable for good governance, which means that companies will slowly have to evolve from *ex-post* to *ex-ante* control.

These are still complex issues, but it is likely that the duties of care and diligence will require directors to rely on AI in their decision-making in the near future.

This means that, when making decisions, it is crucially important to obtain quality information at the appropriate time. Not all information is equal, since directors only need whatever

information is relevant for their decision-making. Quality of information has been at the top of the agenda during the last decade, as shown by EU Commission Recommendation 2014/208/EC on the quality of corporate governance information ("comply or explain"). This framework brought to reality some of the questions that lawyers have asked about AI and its implications for corporate law and governance.

For instance, is corporate law ready to deal with the implications that AI may have on a company's decision-making process? Can AI replace a director? The answer to that question is clearly no.

Portuguese law does not allow AI, algorithms or robots to be appointed as directors, since they lack the legal personality or capacity required by law.

We are aware that the possibility of granting legal personality to certain categories of robots and programs is being widely discussed, including in EU institutions, but right now that is not the case.

As such, because AI still lacks the legal personality and capacity which only natural or legal persons (represented by natural persons, in the case of corporate acts) have, it cannot have any right or obligation within companies. In terms of decision-making, AI can only support the directors, not perform their duties for them, which means that delegation to AI and robots is also out of the question.

Although many AI technologies can reach a decision based on their interpretation of data, keeping a record of how they reached that decision can be more problematic.

Mere administrative tasks, such as assessing a call for a general meeting or analysing reports and annual accounts, are undoubtedly faster and more efficiently performed by robots than human beings. In fact, robots will be able to manage more information and produce more reliable results in far less time, freeing directors to focus on other activities. AI systems can also arguably assist with a large part of directors' resolutions, namely where prognosis and judgment are needed.

Relying on AI to enhance the board's decision-making and data analysis capabilities may thus soon be more commonplace. And who knows, we may yet see the appointment of AI as directors in our lifetime; but right now, we should look to AI as a tool to make better decisions, while keeping an eye towards a future where we can start to think about AI in the role of autonomous director, because sooner or later we will have to address this issue and consider how it is going to affect corporate law as we know it.

To tackle the legal challenges identified (please refer to the Trends section above), both AI providers and AI users are gradually starting to develop their AI Governance as an incremental piece of their AI Strategy. Companies are starting by carrying out AI Legal Impact Assessments ("**AILIAs**"). Although the criteria assessed should be adapted to the specific AI application and the user's sector, most AILIAs assess compliance and possible risks of the AI system in relation to the following aspects:

- AI system classification and application/sector.
- Technical robustness, safety and security of the system.
- Data governance, including personal and non-personal data.
- Transparency.
- Fundamental rights, including due to biases and non-discrimination.
- Accountability.
- System sustainability.

This legal assessment helps companies identify the possible risks related to a specific AI system and application, as well as potential technical, organisational and contractual ways of

mitigating these risks. It is important to note that this is not a one-off exercise. Considering the upcoming regulatory initiatives that will have a direct impact on AI (please refer to the Regulations/government intervention section below), companies should periodically monitor and update their data governance and AI governance to ensure that their AI systems remain future-proof.

Regulations/government intervention

Without prejudice to the various initiatives mentioned herein, there are currently no AI-specific laws in Portugal.

However, any EU-wide regulatory or policy initiative would have an impact on the national AI market, starting with the AIA which, once finalised, will be directly applicable in Portugal, although its current wording provides for possible carve-outs in its implementation in Member States (e.g. regulatory sandboxes, designated national authorities for notification and supervision, authorisation for certain uses of high-risk AI systems, etc.). Therefore, following the entry into force of the AIA, it is expected that an implementing act will be adopted in Portugal.

Moreover, once the Directive on Liability for Defective Products and the AI Liability Directive are finalised, the Portuguese legislator will have a maximum of two years after their entry into force to transpose them into national law.

In addition, the following EU regulatory initiatives are expected to have a direct impact on the Portuguese AI market:

- Data Governance Act, which will be applicable in September 2023;
- Proposal for a Data Act;
- Common European Data Spaces initiative, with the proposal for a European Health Data Space already having been published and the proposal for European Financial Data Spaces expected during 2023.

These initiatives, which make up the three pillars of the EU Data Strategy, aim, amongst others, to ensure that there is high-quality data available to foster innovation and training, and the validation and verification of AI systems in the EU.

Moreover, in relation to cybersecurity, and more specifically the use of AI in essential sectors, we highlight the importance of the NIS 2 Directive, which should be transposed into national law by 17 October 2024.

Notwithstanding the above, the current panoply of European and national consumer protection legislation, the privacy and data protection framework, particularly the GDPR provisions pertaining to automated-decision-making, the intellectual property (please refer to the Ownership/protection section above) and cybersecurity laws, as well as sector-specific laws depending on the AI application and the sector of the AI user, will all apply to AI systems operating in Portugal.

* * *

Acknowledgment

The authors would like to thank João Carlos Assunção for his valuable contribution to the preparation of this chapter.

Sofia Barata
Tel: +351 213 113 534 / Email: sb@vda.pt

Sofia Barata joined VdA in 2005 and is Of Counsel in the Corporate Services Area. With a vast track record in M&A, she has worked in numerous domestic and international transactions over the years, notably M&A, joint ventures, acquisition and corporate finance deals.

Her combination of years of experience in the day-to-day support of clients across industries and a perfect command of the new technological tools of AI and process-automation procedures give Sofia the skill sets required to develop and optimise new cross-practice products and services within VdA, resorting to the consistent adoption of technological procedures.

Nuno Carrolo dos Santos
Tel: +351 213 113 347 / Email: ncs@vda.pt

Nuno Carrolo dos Santos joined VdA in 2015. He is a Managing Associate of the Competition & EU practice area where he has worked in several cases and transactions, particularly in the pharmaceutical and media sectors, with a focus on restrictive practices and merger control.

Iakovina Kindylidi
Tel: + 351 213 113 560 / Email: imk@vda.pt

Iakovina Kindylidi joined VdA in 2019 and provides advice, in Portugal and abroad, on matters relating to privacy, data protection and cybersecurity as well as on technologies, intellectual property, trade secrets and consumer protection. She has assisted in various national and international projects, including projects funded by H2020, and has participated in the preparation of reports for international institutions. Iakovina has expertise on matters related to emerging technologies, namely AI, robotics, Distributed Ledger Technology/Blockchain, smart contracts, NFTs, Metaverse and IoT, and has been involved in various operations involving the design and development of ICT products and services and offering advice on matters of privacy and security as well as on licensing and outsourcing. Iakovina has a background in banking and business law, allowing her to provide strategic advice to entities coming from the financial services sector, including FinTech and InsurTech, while she regularly advises clients coming from various sectors, especially IT, healthcare, media and entertainment, and energy.

Vieira de Almeida

Rua Dom Luís I, 28, 1200-151, Portugal
Tel: +351 213 113 400 / URL: www.vda.pt

Singapore

Lim Chong Kin, Anastasia Su-Anne Chen & Cheryl Seah
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 factors, have contributed to the availability of large volumes of data, which are increasingly being analysed by machine-learning algorithms to make predictions or decisions.

AI has been identified by the Government as one of the four frontier technologies that are essential to growing Singapore's digital economy, alongside cybersecurity, immersive media and the Internet of Things.[1] In 2019, the Government launched a National Artificial Intelligence Strategy, aiming to establish Singapore as a leader in developing and deploying scalable, impactful AI solutions, in sectors that are highly valuable and pertinent to both citizens and businesses by 2030.[2] There will be an initial tranche of five "National AI Projects" in the high socio-economic impact sectors of border security, logistics, healthcare, education management and estate management.

Recent key initiatives to build Singapore's AI capabilities include:

(a) the 2017 launch of AI Singapore, a National AI programme which aims to enhance Singapore's AI capabilities, nurture local talent and build an ecosystem of AI start-ups and companies developing AI products. Its activities include seeding and providing support for AI research, accelerating the adoption of AI by Singapore-based organisations, and developing talent in the field;

(b) 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 and local technological companies, corporate users of AI and advocates of social and consumer interests;

(c) 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; and

(d) the creation of the AI Apprenticeship Programme to enlarge the pool of AI engineers. As of October 2022, over 200 apprentices have been trained, and the Government is providing an additional US$50 million to double the number of AI apprenticeships in the next five years.[3]

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") Model Artificial Intelligence 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 for the purpose of addressing key ethical and governance issues that may arise from their deployment of 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) The "Principles to Promote Fairness, Ethics, Accountability and Transparency ("FEAT") in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", issued by MAS, provide a set of generally accepted principles for the use of AI and data analytics in decision-making related to providing financial products and services; and
(d) MAS's Veritas Initiative, which will enable financial institutions to evaluate their AIDA solutions against the FEAT principles (for example, through white papers detailing assessment methodologies and the open-source toolkit released by the Veritas Consortium).

Internationally, Singapore has also entered into agreements with other nations[4] to strengthen and develop AI research and collaboration efforts. Most recently, in February 2023, Singapore and the EU signed a Digital Partnership, which includes enhancing AI research and promoting cooperation with respect to regulating AI systems.[5]

The Singapore courts have also had the opportunity to address issues raised by AI in the context of cryptocurrency. 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 determine the appropriate application of legal principles to a cryptocurrency exchange where trading was conducted via an algorithmic system as opposed to direct human action.

The algorithmic program in *B2C2 v Quoine* was found by the SICC to be "deterministic" in nature, with "no mind of [its] own", but "[a] mere machine […] carrying out actions which in another age would have been carried out by a suitably trained human". However, the SICC (per Simon Thorley IJ) opined that the ascertainment of knowledge in cases where computers have replaced human action 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]). This was affirmed by the majority of the Court of Appeal on appeal, in *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02.

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 in bringing their AI products to market faster.

On 4 May 2020, IPOS launched the SG Patent Fast Track Pilot Programme, which was subsequently renamed as the "SG IP FAST" programme upon its expansion to include trademark and registered design applications. The programme will be in operation until 30 April 2024. As an example of its accelerated timelines, patent applications under this programme in all fields of technology can be granted in as fast as six months, compared to the typical period of at least two years.

Notably, when submitting the SG IP FAST application, applicants must state the reason(s) for requesting such acceleration and the field of technology to which their invention relates.[6] One possible justification is that the patent application is for an emerging technology with a short product lifecycle (e.g., FinTech, Industry 4.0 and AI).

Under section 13 of the Patents Act 1994, for an invention to be patentable, it must satisfy three conditions:

(a) the invention must be new;
(b) involve an inventive step; and
(c) be 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, IPOS stated in its IP and Artificial Intelligence Information Note that not all inventions are eligible for patent protection (even if they meet the three key criteria above). For instance, mathematical methods, i.e., algorithms *per se*, are not considered inventions, and solving a generic problem such as using the method in controlling a system is unlikely to cross the threshold.

That said, IPOS also stated in its IP and Artificial Intelligence Information Note that where the patent application relates to the application of a machine learning method to solve a specific problem in a manner that goes beyond the underlying mathematical method, the application could be regarded as an invention (for example, using the method in controlling the navigation of an autonomous vehicle).

Apart from the protection of AI solutions under patent law, the source code of a computer program may also be protected by copyright. Section 13(1)(*b*) of the Copyright Act 2021 expressly provides that "literary work" includes a "computer program" for the purposes of the Copyright Act 2021.

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 that derive their value from the underlying datasets.

In general, data *per se* is not protected under copyright law. Under the Copyright Act 2021, 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.[7] 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.[8] 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 receive copyright protection.

Singapore copyright law does not provide for a *sui generis* database right, such as the one recognised in the European Union.[9]

As an alternative, data may be subject to protection under the common law of confidence.

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 refers 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 law, as the initial phase of the work typically involves incidentally extracting or copying data from large quantities of material that may be protected by copyright.

In this light, section 244 of the Copyright Act 2021 allows the copying of copyrighted materials for the purpose of computational data analysis, provided that certain conditions are satisfied. One such condition involves the user having lawful access to the materials that are copied. Notably, the exception in question 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, natural language processing models, such as ChatGPT, are rising in popularity and are frequently used by students and organisations to generate content.[10]

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.[11] 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",[12] where authorship is defined in terms of the exercise of independent, original or creative intellectual efforts.[13]

Antitrust/competition laws

The Competition Act 2004 ("Competition Act") establishes a general competition law in Singapore. The Competition Act generally prohibits:

(a) anti-competitive agreements (the section 34 prohibition);[14]
(b) the abuse of a dominant position (the section 47 prohibition);[15] and
(c) mergers and acquisitions that substantially, or may be expected to substantially, lessen competition within any market in Singapore (the section 54 prohibition).[16]

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[17] by the CCCS.

Anti-competitive agreements and concerted practices facilitated by algorithms

Amongst the topics discussed in one of the CCCS's papers[18] is anti-competitive agreements and concerted practices facilitated by algorithms.

In the 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 in market conditions.[19]

In terms of applying competition enforcement to algorithms, the CCCS has observed that, where the use of algorithms furthers, supports or facilitates any pre-existing or intended anti-competitive agreements or concerted practices, 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 an activity may be caught by the section 34 prohibition.[20]

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 (i.e., collusive agreements being reached without any explicit communication between competitors) that 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.

Board of directors/governance

On 21 January 2020, the PDPC published the second edition of its Model AI Framework.[21] The Model AI Framework is the result of the efforts of 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 that has 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, as well as risk management and internal control strategies.
(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 determine 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) Stakeholder interaction and communication: organisations should take steps to build trust and maintain open relationships with individuals regarding the use of AI, including steps such as general disclosure, increased transparency, policy explanations, and careful design of human-AI interfaces.

Complementing the Model AI Framework is the Implementation and Self-Assessment Guide for Organisations ("ISAGO"), a companion guide that aims to help organisations assess the alignment of their AI governance practices with the Model AI Framework, as well as the Compendium of Use Cases, which features organisations that have implemented accountable AI practices.

In order to assure the public that AI systems are fair, explainable and safe, Singapore is further strengthening its ability to "test" AI, with the launch of AI Verify in May 2022, a self-assessment AI governance testing framework and toolkit for organisations containing both software for technical tests and a series of questions for process checks. AI Verify does not use pass-fail standards, but enables organisations to be more transparent about the performance of their AI systems.[22]

Regulations/government intervention

At present, Singapore does not have legislation governing the use of AI in general (unlike the proposed EU Artificial Intelligence Act), but has voluntary guidelines for individuals and businesses, such as the Model AI Framework.

Protection of personal data

The use of datasets in conjunction with AI applications has the potential to raise data protection ("DP") issues, especially where such datasets contain 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, such as those issued by MAS for the financial sector.

Under the PDPA's general DP framework, there are presently 10 main obligations, with one more obligation (i.e., the Data Portability Obligation) to come into force in the future. Since the enactment of the PDPA, the general DP framework has largely operated as 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 personal data, unless an exception applies.[23]

Importantly, the recent amendments to the PDPA under the Personal Data Protection (Amendment) Act 2020 introduced numerous revisions to the consent framework, including

recognising the presence of deemed consent under certain circumstances, as well as expanding the scope of the exceptions to consent under the PDPA, so as to empower business to use data for innovation with safeguards in place to continue to protect personal data.[24]

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. According to the PDPC's *Advisory Guidelines on the PDPA for Selected Topics*, anonymised data is not personal data. However, data would not be considered anonymised if there is a serious possibility that an individual could be re-identified, taking into consideration both:

(a) the data itself, or the data combined with other information to which the organisation has or is likely to have access; and
(b) the measures and safeguards (or lack thereof) implemented by the organisation to mitigate the risk of re-identification.

Technological advancements may increase the risk that a dataset that was previously anonymised may be de-anonymised, and thereby be considered personal data.[25] 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 that is assumed to be anonymised to constitute personal data. Companies that intend to engage in such operations should therefore exercise diligence in order to avoid inadvertently collecting, using and/or disclosing personal data without fulfilling the requisite requirements, thereby infringing the obligations under the PDPA.

Cybersecurity Act 2018

The Cybersecurity Act 2018 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 2018 operates alongside the Computer Misuse Act 1993 ("CMA"), which criminalises certain cyber activities such as hacking, denial-of-service attacks, infection of computer systems with malware, and other sector-specific regulatory frameworks. On 11 April 2022, the licensing framework for cybersecurity service providers came into effect,[26] along with the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. The licensing framework, which covers cybersecurity service providers offering penetration testing services and managed security operations centre monitoring services, aims to improve the standard of cybersecurity service providers, and address the information asymmetry between such providers and consumers.

Protection from Online Falsehoods and Manipulation Act 2019

Singapore 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 ("POFMA"), which came into effect on 2 October 2019, seeks to, amongst others, prevent the electronic communication of false statements of fact in Singapore. 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 it to communicate false statements 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 1961 was amended to include specific definitions relating to autonomous vehicles.[27]

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*".

Furthermore, the Road Traffic (Autonomous Motor Vehicles) Rules 2017 ("Autonomous Vehicles Rules") were introduced to regulate the trials of autonomous vehicles. Most significantly, there is a general prohibition on the trial or use of an autonomous motor vehicle on any road unless the person has specific authorisation.[28]

The framework established under the Autonomous Vehicles Rules sets out that parties interested in trialling 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 these 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 full control of the autonomous vehicle when required, and state the geographical area in which the trial may be conducted.[29]

In 2018, in response to queries raised in Parliament with respect to the safety measures that are currently in place for conducting 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, which will alert the safety driver of any faults and allow the control of the autonomous vehicle to be immediately transferred to the safety driver.[30]

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, with the latest update made in 2021.

AI in the workplace

With a small and ageing population, the use of AI and automation is necessary for Singapore to preserve its competitive edge over other economies. At present, automation of jobs is being used to combat the shrinking workforce in areas that rely heavily on manual labour, such as sanitation.[31] The Singapore Government has also introduced measures to encourage the adoption of AI automation, such as through the Enterprise Development Grant.[32] The IMDA also developed and published A Guide to Job Redesign in the Age of AI to help companies manage AI's impact on employees and prepare for the future of work.[33]

Implementation of AI/big data/machine learning into businesses

The COVID-19 pandemic has sped up the adoption of digital technologies by businesses. This, in turn, has led to the increased proliferation of AI adoption by companies, with a recent survey (the Global AI Adoption Index 2022 commissioned by IBM) finding that 57 per cent of around 500 technology decision-makers in small to large firms in Singapore had indicated that their companies had accelerated the roll-out of AI tools.[34]

As part of facilitating the adoption of AI by businesses, Singapore is also focused on rolling out new initiatives to enhance skillsets in AI amongst the country's workforce. One of the Singapore Government's initiatives, "AI for Everyone", is freely available to the public and seeks to introduce students and working adults to the potential of AI technologies. Furthermore, Singaporeans can make use of the TechSkills Accelerator programme, a SkillsFuture initiative driven by IMDA to develop their competencies in the ICT sector, which includes fields such as AI, software development, data analytics and cybersecurity.

Civil liability

The civil liability regime for AI is in its nascent stages in Singapore. To date, there have been cases where the courts have applied the existing legal frameworks (e.g., contractual, tortious, equitable and property law principles) to risk and liability issues concerning AI.

For example, in the landmark case of *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02, which involved smart contracts and the autonomous algorithmic trading of digital tokens, the existence of a contractual relationship between buyers and sellers when executing a trade on the digital token exchange was recognised by the Court of Appeal. Accordingly, the Court of Appeal applied traditional contractual principles of unilateral mistake and breach of contract to a contractual relationship represented by a smart contract.

In the meantime, studies on the applicability of Singapore law to AI systems are underway, with the Singapore Academy of Law's Law Reform Committee ("LRC") establishing a Subcommittee on Robotics and AI in 2020 to consider and make recommendations on the above. With respect to civil liability, the LRC published the "Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars", proposing and discussing possible frameworks for determining liability on the basis of negligence, strict liability and no-fault liability in the context of self-driving vehicles.

Criminal issues

The CMA

Although not specific to AI, the CMA is the main legislation in Singapore that prescribes a list of criminal offences relating to computer material or services (which may be relevant to AI systems). Under the CMA, a "computer" refers to an electronic, magnetic, optical, electrochemical or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of interconnected or related devices.[35]

The list of offences includes, amongst others:

(a) unauthorised access (e.g., hacking) (section 3(1) of the CMA);
(b) unauthorised modification of computer material (e.g., infection of IT systems with malware) (section 5 of the CMA);
(c) unauthorised obstruction of the use of computers (e.g., denial-of-service attacks) (section 7(1) of the CMA);
(d) possession or use of hardware, software or other tools used to commit cybercrime (section 10(1)(*a*) of the CMA); and
(e) distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime (section 10(1)(*b*) of the CMA).

Discrimination and bias

The Model AI Framework sets out principles for the ethical use of AI in the private sector, including addressing problems relating to bias within AI systems by means of:

(a) training staff dealing with AI systems to interpret AI model output and decisions to detect and manage bias in data; and

(b) using reasonable effort to assess and manage the risks of inherent bias and inaccuracy of datasets used for AI model training through ensuring data quality, using different datasets for training, testing and validation, and the periodic reviewing and updating of datasets.

For more information on the Model AI Framework, please refer to the "Board of directors/governance" section.

National security and military

The Ministry of Defence ("MINDEF") and the Singapore Armed Forces ("SAF") have been harnessing AI and data analytics and conducting research into novel technologies to improve existing frameworks and solutions designed to enhance servicemen's safety during training sessions and field operations.[36] The SAF is also conducting trials on the use of autonomous vehicles in military camps and bases for the unmanned transportation of logistics and personnel, in order to reduce manpower requirements for transport operators and improve the efficiency of ground supplies and personnel transportation.[37]

Conclusion

Singapore continues to support the use of artificial intelligence with funding, training and guidance from regulators. With growing international interest in this area as more countries release guidelines, hold public consultations and even introduce legislation regulating the use of AI, Singapore continues to monitor developments around the world to harness the most effective uses of the technology, in a way that maximises its benefits and minimises the risk of harm to any person.

* * *

Endnotes

1. The IMDA, *Tech Pillars* (updated 26 October 2022), https://www.imda.gov.sg/about-imda/research-and-statistics/sgdigital/tech-pillars.
2. The SNDGO, *National Artificial Intelligence Strategy* (19 November 2019), https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf.
3. The Prime Minister's Office, *DPM Heng Swee Keat at the Opening of the Singapore Week of Innovation and Technology 2022* (25 October 2022), https://www.pmo.gov.sg/Newsroom/DPM-Heng-Swee-Keat-at-the-Opening-of-the-Singapore-Week-of-Innovation-and-Technology-2022.
4. For instance, Singapore has signed Memoranda of Understanding with the Republic of Korea and Australia to cooperate on AI research.
5. The European Commission, *EU and Singapore launch Digital Partnership* (1 February 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_467.
6. The IPOS, *Circular No. 3/2022* (22 April 2022).
7. Section 14 of the Copyright Act 2021.
8. *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [24].

9. *Ibid.* at [34] and [35].
10. Channel News Asia, *As ChatGPT Takes the World by Storm, Professionals Call for Regulations and Defences against Cybercrime* (16 February 2023), https://www.channelnewsasia.com/singapore/chatgpt-ai-chatbot-risks-regulations-cybercrime-phishing-3282896.
11. *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 at [41], [72].
12. *Ibid.* at [81].
13. *Ibid.* at [75].
14. Section 34 of the Competition Act.
15. Section 47 of the Competition Act.
16. Section 54 of the Competition Act.
17. The CCCS (in collaboration with the IPOS and the PDPC), *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (2 December 2020); The PDPC (in collaboration with the CCCS), *Discussion Paper on Data Portability* (25 February 2019).
18. The CCCS, *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (2 December 2020).
19. *Ibid.* at pages 66 to 68.
20 *Ibid.* at pages 69 and 70.
21. The Model AI Framework was recognised by a top award in the "Ethical Dimensions of the Information Society" category by the World Summit on the Information Society Prizes.
22. The IMDA, *Invitation to Pilot: AI Verify – AI Governance Testing Framework & Toolkit* (25 May 2022), https://file.go.gov.sg/aiverify.pdf.
23. Section 13 of the PDPA.
24. The PDPC, *The Enhanced PDPA: Using Data for Innovation* (November 2020).
25. The PDPC, *Advisory Guidelines on the PDPA for Selected Topics* (revised 17 May 2022), at [3.35].
26. Part 5 of the Cybersecurity Act 2018.
27. Section 2(1) of the Road Traffic Act 1961.
28. Rule 4 of the Autonomous Vehicles Rules.
29. Rule 9 of the Autonomous Vehicles Rules.
30. Singapore Parliamentary Debates, *Oral Answers to Questions on Self-driving Vehicles Being Tested on Public Roads* (11 July 2018).
31. See for instance The Straits Times, *NEA exploring table-cleaning robot at hawker centres to support manual labour* (28 November 2022), https://www.straitstimes.com/singapore/environment/nea-exploring-table-cleaning-robot-at-hawker-centres-to-support-manual-labour, and Channel News Asia, *Local cleaning robotics firms see demand at least double amid tech advances* (19 April 2022), https://www.channelnewsasia.com/watch/local-cleaning-robotics-firms-see-demand-least-double-amid-tech-advances-video-2634181.
32. Enterprise Singapore, *Enterprise Development Grant* (updated 14 February 2023), https://www.enterprisesg.gov.sg/financial-assistance/grants/for-local-companies/enterprise-development-grant/innovation-and-productivity/automation.
33. The IMDA, *A Guide to Job Redesign in the Age of AI* (4 December 2020).
34. IBM, *IBM Global AI Adoption Index 2022* (9 May 2022), at page 5.

35. Section 2(1) of the CMA.
36. The MINDEF, *Fact Sheet: Leveraging Digital Technology and Research to Enhance Safety of National Servicemen* (3 March 2022), https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/03mar22_fs2.
37. The MINDEF, *Fact Sheet: Autonomous Vehicles in the SAF* (3 May 2021), https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/May/03may21_fs.

Lim Chong Kin
Tel: +65 6531 4110 / Email: chongkin.lim@drewnapier.com

Chong Kin is the Managing Director of Drew & Napier's Corporate & Finance Department. He heads the Telecommunications, Media & Technology ("TMT") Practice, and co-heads the Competition Law & Regulatory Practice and Data Protection, Privacy & Cybersecurity Practice. Under Chong Kin's leadership, these Practice Groups have consistently been ranked as leading practices in Singapore.

With his strong background in competition, data protection and technology laws, Chong Kin is often depended upon by his clients to deliver commercially savvy advice, particularly in the cutting-edge industries of FinTech, AI, big data and machine learning.

In particular, Chong Kin has in-depth expertise and experience in competition law matters, having advised 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, prior to advising on the general Competition Act.

Anastasia Su-Anne Chen
Tel: +65 6531 4123 / Email: anastasia.chen@drewnapier.com

Anastasia is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT, data protection, privacy and cybersecurity. She was formerly the Deputy Chief Counsel of the Personal Data Protection Commission ("PDPC") and Info-communications Media Development Authority ("IMDA") for over nine years, where she was the lead counsel for PDPC's matters, IMDA's procurement and IP portfolios, as well as the legal advisor to IMDA's Data Administration Group. A significant national project that she has advised on is the amendments to the PDPA in 2021, which include revisions to empower businesses to use data for innovation. Anastasia has extensive experience advising companies on their data protection compliance programmes, including their data transfer agreements, privacy notices and other documentation. She also advises on related TMT matters, such as regulatory compliance issues in respect of data centres and the use of AI.

Cheryl Seah
Tel: +65 6531 4167 / Email: cheryl.seah@drewnapier.com

Cheryl is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT and administrative and public law. In addition to advising on payment services and other regulatory matters, Cheryl advises clients on legal issues arising from the use of AI, from compliance with Singapore's data protection laws when using AI to process personal data, to IP and liability issues arising from the implementation of a ChatGPT-like system in the workplace to answer questions and generate documents and code. Before joining the firm, Cheryl was a State Counsel/ Legislative Drafter in the Legislation Division of the Attorney-General's Chambers (Singapore's national law drafting office).

Drew & Napier LLC

10 Collyer Quay, 10th Floor Ocean Financial Centre, Singapore 049315
Tel: +65 6531 4110 / URL: www.drewnapier.com

South Africa

Simone Dickson
Independent Consultant

Trends

Artificial intelligence (AI) remains largely unregulated in South Africa.

The AI Institute of South Africa was launched by the Department of Communication and Digital Technologies on 30 November 2022 and is stated to have been founded upon the vision set out by the Presidential Commission on the Fourth Industrial Revolution (PC4IR). The Institute aims to generate knowledge and applications that will position South Africa as a competitive player in the global AI space.

It is anticipated that regulatory development regarding AI will follow, although there are socio-economic factors at play in South Africa including inequality and unemployment, with job losses as a result of the adoption of AI being a real concern, which cannot be discounted and may impact on the prioritisation of regulation in this area. Existing laws will need to be adapted and/or new laws promulgated, with careful cognisance taken of the South African landscape, to ensure that effective governance around AI is introduced while allowing for continued innovation. This does however require an understanding of AI by policymakers.

South Africa does have legislation addressing the processing of personal information, including the automatic processing of data, but applies to responsible parties who are defined as "*public or private bodies or any other person*" and the extended application to AI would need to be tested and changes made to the legislation so as to ensure holistic protection for data subjects.

Ownership/protection

The ownership of the output of AI is a complex question which is likely to be the continued subject of debate.

Until AI-specific regulation comes into play in South Africa, traditional laws applicable to intellectual property ownership will need to be applied to each case, where practical. For instance, regarding copyright, in South Africa, it is not necessary to register copyright in order for it to come into existence. A copyright exists on creation of a work which meets the requirements for copyright protection under the South African Copyright Act. From an AI perspective, although the Act does provide for a class of computer-generated works, it would need to be established who the author of the work is and whether the work itself was original. AI creations do not have human authors and this and the other requirements for copyright protection would need to be assessed in the context of the specific arrangement.

South Africa did award a patent to an AI-generated invention and was believed to be the first country in the world to do so at the time of publication in the South African Companies and

Intellectual Property Commission journal in July 2021. However, as the AI was not a legal entity, the creator of the AI/invention was identified as the owner of the patent.

Antitrust/competition laws

Although there has been some focus around digital mergers and digital platforms from a competition perspective, there is no specific AI regulation in the competition sector.

Board of directors/governance

As AI is being adopted and developed, it and its associated risks must be included in corporate governance agendas and strategies.

Regulations/government intervention

South Africa has no laws specifically regulating AI, with existing legal principles having to be adapted, or new principles developed to ensure ethical risks are mitigated and users protected while not stifling innovation. This does, however, require that policymakers have an understanding of AI as well as socio-economic factors at play in the South African environment, with input from both the private and public sector as well as AI developers and experts being essential.

Simone Dickson
Email: simone@simonedickson.com

Simone is an independent consultant, having formerly been a director of a large South African business law firm. She has 15 years of specialisation in commercial information technology and communications law, with extensive and diverse experience across the field of IT, covering issues related to data privacy, digital platforms and licensing, among others. She has been the lead advisor to a variety of clients on their transactional requirements, including many high-profile deals, a number of which involved major international ICT companies. She is ranked by *Chambers and Partners* in Band 4 for 2023.

Simone Dickson, Independent Consultant

Sweden

Elisabeth Vestin, Caroline Sundberg & Anna Ribenfors
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"). The Swedish Government commissioned the Public Employment Services, the Swedish Companies Registration Office, the Agency for Digital Government, and the Swedish Tax Agency to promote the use of AI in public administration in 2021. The authorities' report on the assignment, which was published in January 2023, shows that a great demand to provide comprehensive and concrete support in developing and providing guidance for AI solutions has emerged in Sweden, not only in the business sector but also in public administration.[1]

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.[2] 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.[3]

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 in order to prevent 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 that 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 and AI, as well as IT security. These are factors that, 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. In Sweden, research on AI 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 the industry, 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.

The Government further emphasises the importance of a strong IT framework and infrastructure to enable the development and use of emerging technology. The Government's broadband strategy from 2016, to provide high-speed internet to 95 per cent of households with at least 100 Mpbs broadband in 2020, was already met by the end of 2019. By 2025, the goal is to increase the percentage to 100, including rural areas.[4] In a report published on 31 March 2022, the Swedish Post and Telecom Authority concluded that satellite technology is the only realistic alternative to fully reach this goal.[5]

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. In accordance with the latest report from the European Patent Office ("EPO"), Sweden is ranked 10th 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 leading Swedish companies, such as Ericsson, which has further strengthened its position, especially within the field of digital communication, with an increase in 2021 of 15 per cent compared to the previous year.[6]

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 its report.[7] Ericsson, with the largest research and development ("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 Car Corporation, Polestar 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).

The EU's Artificial Intelligence Act

On 21 April 2021, the EU Commission presented its proposal for a regulation on harmonised rules for AI, and in December 2022, the Council adopted its common position on an amended version of the act. The purpose of the proposed regulation is to harmonise rules for AI within the EU, strengthen the competitiveness and functioning as well as avoid fragmentation of the EU internal market, protect health, safety and fundamental rights, promote the positive aspects of AI and ensure the free movement of AI systems within the EU.

The proposal uses a risk-based approach, where AI systems are divided into four categories (unacceptable risk, high risk, limited risk and minimal risk) and a different set of obligations are attached to each category, with the obligations getting stricter as the level of risk increases. A system for market surveillance and regulatory compliance via public bodies is proposed to be introduced at both a national and an EU level. To be allowed to use a high-risk AI system, a CE certification is required, which can be obtained after an examination by a competent public body.

The Swedish Government has stated that it welcomes the Commission's work to create a uniform regulation for AI within the EU and highlights that Sweden must be a leader in taking advantage of the opportunities that the use of AI can provide. The Swedish Government also supports the fact that the proposal is based on human rights, including the right to privacy, freedom of expression, non-discrimination and equality, but also personal integrity, protection of individuals regarding the processing of personal data and information and cybersecurity.[8] Swedish authorities have also recognised the importance to prepare public administration in Sweden for the upcoming EU regulation, since a lack of clear governance and coordination in relation to the regulation could entail that Swedish public administration as a whole will be severely limited in its ability to use AI.[9]

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 solely on copyright is likely, to date, 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 that 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 that: (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 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. Except for computer programs, the right to works created by an employee will not automatically transfer to the employer. It is therefore important for the employer that the assignment of intellectual property rights is regulated in the employment contract. With respect to computer programs, Section 40(a) of the Swedish Copyright Act stipulates that, unless otherwise agreed, the copyright automatically passes to the employer, provided it has been created in the scope of duties in an employment relation. Thus, if the AI is considered a computer program, the employer would, in this situation, often 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 to 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 ownership of the invention.

In accordance with the Swedish Trade Secrets Act, during the term of employment, an employee may neither utilise the employer's trade secrets unlawfully, nor disclose or appropriate them 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 also provides a *sui generis* right for databases that applies to those of which obtaining, verification, or presentation has required significant investments. It should be noted, however, that database protection protects the work behind the database – not the data as such. 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 as such cannot be owned under Swedish law. The definition of ownership applies poorly to data, since data is not an interchangeable object and often refers to mere facts that may be known to several parties. Moreover, transferring data from one party to another usually does not remove it completely from the party transferring it, and it does not prevent the receiving party from using it (unless carefully regulated in a contract and followed up in an audit). Data can, however, belong to and be managed by various stakeholders, such as the party who owns the device or the service where the data is located. Thus, the ownership of the device or service is typically the default setting to establish management rights when no agreements have been made. Nevertheless, under Swedish law, it is usually more appropriate to conclude whether data can be protected as a trade secret under the Swedish Trade Secrets Act and if there are any restrictions on the intended use of the data, rather than trying to determine who owns it. For example, the GDPR has clear rules for data processing responsibility and limitations on how data may be processed.

Antitrust/competition laws

Competition law in Sweden is regulated by the Swedish Competition Act (2008:579), which, through Sweden's membership in the EU, is harmonised with the 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 that 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*[10]

in 2017, and the research report on *Collusion in Algorithmic Pricing*[11] in 2021. Both reports discuss 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. The matter has also been discussed in an interview with the head of the unit for abuse of dominance and the head of the unit for cartels and concentrations.[12] 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 such 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 must be some form of conscious underlying consensus between the competitors on price tactics in order for the practice to be deemed unlawful.

The use of such pricing practices appears to be uncommon in Sweden. In their report *Competition and Growth in E-commerce*[13] published in 2021, the SCA noted that survey results within the e-commerce market indicate that e-merchants mainly use manual pricing and that pricing tools such as algorithms and AI seem to be rare.

In January 2020, the SCA published its new strategy for AI.[14] 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.[15]

Antitrust concerns related to big data

Towards the end of 2019, 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.[16] 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 they 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, Swedish companies whose shares are listed on a regulated market in Sweden are obligated to apply the Swedish Corporate Governance Code and the regulated market's own rules and regulations. In addition to these, the Swedish Accounting Act (1999:1078), the Swedish Annual Accounts Act (1995:1554), the Swedish Securities Market Act (2007:528), and the Swedish Financial Instruments Trading Act (1991:980) are important regulations in the field of corporate governance. As the legislation is technology-neutral, there are opportunities and flexibility for the use of specific technical solutions in this field. For example, many corporate documents (e.g., a company's share register, board minutes and annual accounts) may be prepared and maintained in a digital format, and corporate documents may, as a general rule, be signed by way of advanced electronic signature in accordance with EU rules and regulations. The Swedish Companies Act contains basic provisions regarding a limited liability company's organisation and 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 of all shareholders and observe duties of loyalty and care in the exercise of their responsibilities. It is not possible to transfer these fiduciary duties to digital solutions. However, digital solutions may be appropriate to support the members of the board or management in fulfilling their duties, for example, in situations where manual processing and review would not be possible or very extensive because the data volumes are large and/or complex. Furthermore, digital solutions may support the board of directors in its responsibility under the Swedish Companies Act to ensure that the company's organisation is structured in such a manner that the company's finances are monitored satisfactorily, as well as in establishing and maintaining reporting channels to the board of directors in general. It is important that the effects and risks of using AI, machine learning, big data, and other similar solutions are duly 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. However, Swedish legislation is generally technology-neutral, and thus 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 a specific 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 will sometimes mention specific technologies.

Legislation regarding areas such as consumer protection, privacy and product safety is therefore, on some occasions, applicable to AI systems even if they are not expressly mentioned in the legislative texts. This may, however, lead to inappropriate outcomes, as the legislation is not necessarily intended 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, in practice, be deprived of its right to compensation.

The EU Commission has emphasised the need for harmonised AI legislation and has, as mentioned above, proposed a regulation for harmonised rules on AI. Such legislation would have an impact on Swedish legislation in the same way the harmonised legislation had on consumer protection, privacy and product safety. In line with EU initiatives, Sweden 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. 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, as important. Such balance must also be struck globally and at EU level, and Sweden is active in developing such rules.

Civil liability

The fact that AI technologies present new safety risks when embedded in products and services has been mentioned by legislators on several occasions.[17] 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.[18] 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, but will also mention some legislative movements at EU level.

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 conclude 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

As a general principle under the Swedish Product Safety Act (2004:451), products made available on the market shall be safe. Further, under the Swedish Product Liability Act (1992:18) (the "PLA"), a manufacturer is liable for personal injuries and damage on consumer property caused by a defective product. The PLA, which implements the EU Product Liability Directive (85/374/EEC),[19] also imposes responsibility on distributors. It is unclear whether an AI system classifies as a product under the PLA and the problem can be illustrated with a comparison to personal computers. Computer software can be considered part of the hardware, and hence a product, if highly integrated with the hardware and difficult for the user to access. Operating systems are examples of such integrated software. Where the operating system causes damages, the manufacturer of the personal computer may be held liable under the PLA regardless of whether the damage was caused by a logical software error or malfunctioning hardware. Nonetheless, in respect to more standalone software, it is clear from the preparatory works to the PLA that the software programmer will be held liable under the PLA as he/she does not create a product as defined in 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 manufacturers 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. These topics have been discussed at EU level[20] and are subject to upcoming EU legislation through the new Product Liability Directive and the AI Liability Directive. The Swedish legislator has not specifically addressed these topics nor have such issues been tried by Swedish courts. Nonetheless, the Swedish Government does welcome the ambition to make it easier for people who have suffered damage caused by AI to be able to receive compensation, considering the specific challenges associated with AI.[21]

Tort law

Tort liability outside the PLA or other speciality laws regarding liability is, as a main rule, based on negligence or intent. 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 or intent in regard to an AI system requires negligence or intent 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 R&D.[22]

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. On 11 March 2022, the Equality Ombudsman, the government agency combatting discrimination, released a report summarising answers from 34 Swedish governmental agencies from questionnaires with queries on how they used AI, automated decision-making systems and what knowledge they have of factors that might lead to discriminatory results. The report found that a vast majority of the governmental agencies' awareness of the risk of discrimination was inadequate. When AI is used, for example, for recruitment, the individual is protected by the Discrimination Act. The Ombudsman has previously stated, however, 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. The newly issued report further supports this view and highlights the importance of sufficient training for individuals in both private and public organisations involved in automated decision-making systems.

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.

Conclusion

Sweden has built a solid foundation for the continued advancement and integration of AI and digital solutions in Swedish 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 that 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. The Public Employment Services, The Swedish Companies Registration Office, The Agency for Digital Government, and The Swedish Tax Agency, Mission to promote public administration's ability to use artificial intelligence, 20 January 2023, available here (in Swedish): https://www.digg.se/analys-och-uppfoljning/publikationer/publikationer/2023-01-23-slutrapport-uppdrag-att-framja-offentlig-forvaltnings-formaga-att-anvanda-artificiell-intelligens.
2. Sweden's Innovation Agency, *Artificial Intelligence in Swedish Business and Society*, May 2018.
3. Government Offices of Sweden, *National Approach to Artificial Intelligence*, February 2019.
4. 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.
5. The Swedish Post and Telecom Authority's report, *Satellite: an opportunity for fast broadband 2025*, 31 March 2022, available here (in Swedish): https://www.pts.se/sv/dokument/rapporter/internet/2022/satellit-en-mojlighet-till-snabbt-bredband-2025---pts-er-2022-18/.
6. European Patent Office, Patent Index 2021, available here: https://www.epo.org/about-us/annual-reports-statistics/statistics/2021/statistics/patent-applications.html#tab2.
7. See endnote 2.
8. The Swedish Government's statement is available here: https://www.regeringen.se/faktapromemoria/2021/05/202021fpm-109/.
9. See endnote 1.
10. Swedish Competition Authority, *Competition and Growth on Digital Markets*, Report series 2017:2, March 2017.
11. T. Löfström, H. Ralsmark and U. Johansson, by request of the Swedish Competition Authority, *Collusion in Algorithmic Pricing,* Research report 2021:3, November 2021.
12. 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.

13. Swedish Competition Authority, *Competition and Growth in E-commerce*, Report series 2021:3, September 2021.
14. Swedish Competition Authority, *Artificial intelligence (AI) Strategy or the Swedish Competition Authority*, Dnr. 82/2020, January 2020.
15. Swedish Competition Authority, *Business Plan 2020–2022*, Dnr. 110/2020, February 2020.
16. Swedish Competition Authority, *The Swedish Consumer Agency and Swedish Data Protection Authority, Regarding 2020 Research Policy Bill*, Dnr. 2019/915, October 2019.
17. E.g., Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNIONLEGISLATIVE ACTS.
18. European Union, Expert Group on Liability and New Technologies – *New Technologies Formation, Liability for Artificial Intelligence and other emerging technologies*, November 2019.
19. 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.
20. 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.
21. The Swedish Government's statement is available here: https://regeringen.se/faktapromemoria/2022/11/202223fpm8/.
22. See endnote 20.

Elisabeth Vestin
Tel: +46 760 000 009 / Email: elisabeth.vestin@hannessnellman.com

Elisabeth Vestin 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 and media, as well as general commercial law.

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

Recommended in *The Legal 500*, 2019–2023 (IT and telecoms) as a Leading Individual: "Elisabeth Vestin is outstanding. One cannot think of a better lawyer. She is very focused, always business-driven and dedicated, renders pragmatic advice and is at the same time very pleasant to deal with." The team is ranked in *Chambers and Partners* Europe 2023 Sweden in Data Protection and Information Technology.

Elisabeth is ranked as one of the world's leading franchise lawyers in *Who's Who Legal*, 2016–2022.

Caroline Sundberg
Tel: +46 760 000 004 / Email: caroline.sundberg@hannessnellman.com

Caroline Sundberg specialises in the law related to the IT and technology sector, with a particular focus on IT agreements and data and 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, AI, Internet of Things and e-commerce.

Caroline is ranked in *Chambers and Partners* Europe 2023 Sweden, Data Protection and Information Technology and *The Legal 500*, 2019–2023 as a Future Partner 2021–2023 (IT and telecoms).

Anna Ribenfors
Tel: +46 760 000 002 / Email: anna.ribenfors@hannessnellman.com

Anna Ribenfors specialises in the law related to the technology sector, with a particular focus on complex IT and services agreements for financial institutions. She regularly advises her clients on a wide variety of arrangements, including tech sourcing, outsourcing and cloud services. She also advises on M&A in the IP & Tech field and has vast experience in the public procurement of tech.

Recommended in *The Legal 500*, 2019–2023 as a Rising Star 2020–2023 (IT and telecoms): "Anna Ribenfors is excellent counsel with a deep knowledge and experience in outsourcing matters."

Hannes Snellman Attorneys Ltd

P.O. Box 7801, SE-10396 Stockholm, Sweden
Tel: +46 760 000 000 / URL: www.hannessnellman.com

Switzerland

Jürg Schneider, David Vasella & Anne-Sophie Morand
Walder Wyss Ltd.

Trends

According to various rankings, Switzerland has been considered the most innovative country worldwide over the past few years. In the European Innovation Scoreboard 2022 report, in which Switzerland is described as an "innovation leader" and the "overall best performing country in Europe, outperforming all EU Member States", the European Commission noted that the country's strengths lie in attractive research systems, human resources and the linkages (e.g., innovative SMEs collaborating with others). The top five indicators include international scientific co-publications, foreign doctoral students, doctorate graduates, public–private co-publications and lifelong learning. The annual report identifies the relative strengths and weaknesses of innovation systems in EU member countries, European countries outside the EU and their regional neighbours. This is done based on four main indicators:

- Framework conditions (dimensions of human resources, attractive research systems and an innovation-friendly environment).
- Investment (financing, support and business investment).
- Innovation activities (innovators, linkages and intellectual property).
- Impact (impact on employment and impact on turnover).

With regard to the topic of artificial intelligence (AI), Switzerland has the highest number of AI patents in relation to its population worldwide, and the highest number of AI companies per citizen in Europe. This makes Switzerland one of the leading centres for AI development. Additionally, the country has a large number of leading AI research institutes, such as the two Federal Institutes of Technology ETH Zurich and EPFL Lausanne. ETH Zurich, in particular, opened a new research centre for AI, the ETH AI Center, in 2020. This centre aims to intensify the interdisciplinary dialogue between business, politics and society on the innovative and trust-promoting development of AI systems. This proximity to research and innovation is a decisive reason for global technology companies, such as Google, IBM and HPE, to use Switzerland as a research location. Due to its traditional strengths in life sciences, Switzerland is also driving AI development in the healthcare and pharmaceutical sectors. With a stable political and economic environment and globally operating companies, Switzerland offers a secure location for the storage, processing and validation of data. Furthermore, with International Geneva, Switzerland has a location that fulfils many of the requirements for becoming a centre for the global governance of AI. Geneva attracts many international organisations and standards organisations that are also centres of normative power or may be considered as such. For instance, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) are Geneva-based organisations. The

ICO and IEC are even associations established under Swiss law. This potentially enables Switzerland, on an informal basis, to provide early input into standards-setting in relation to AI. Hence, in principle, Switzerland is well positioned for the application and challenges of AI; however, the political environment has highlighted an additional need for action in various areas. To ensure that Switzerland remains one of the leading countries in the development and application of digital technologies, the Federal Council made AI a core theme of the Digital Switzerland Strategy in 2018. Moreover, it set up an interdepartmental working group under the guidance of the State Secretariat for Education, Research and Innovation (see also the section "Regulations/government intervention").

In addition, Switzerland is monitoring regulatory developments in the EU. On 21 April 2021, the European Commission published a proposal for an "Artificial Intelligence Act" – a draft bill on the regulation of AI – in order to develop human-centric AI and eliminate mistakes and biases to ensure AI is safe and trustworthy. The draft bill follows the European Commission's "White Paper on Artificial Intelligence" that was published on 19 February 2021 and represents the starting point for the regulation of AI in the EU. The draft bill extends far beyond the borders of the EU, however. The AI Act shall apply to all AI systems that are placed on the market in the EU or that affect people in the EU. Especially in the software sector, where new products are costly to develop but very cheap to reproduce, such rules can quickly have an impact in other countries, including Switzerland. Most AI providers will not develop their own products for Switzerland, hence new European standards will have an impact in Switzerland as well, as did the introduction of the European General Data Protection Regulation (GDPR) in 2018 (see also the section "Regulations/government intervention").

On 13 April 2022, the Federal Department of Foreign Affairs (FDFA) published the "Artificial Intelligence and International Rules" report. In submitting this report, the FDFA had fulfilled a task assigned to it by the Federal Council. The report sets out various measures to allow Switzerland to play an active role in shaping and contributing to an appropriate global set of AI rules that address the challenges and exploits of the opportunities presented by AI. The measures proposed to the Federal Council shall boost Switzerland's legal and technical expertise, ensure that its positions on AI are coherently represented in international bodies and, by working with the Geneva-based international standards organisations, make an active contribution to shaping global AI rules and standards. According to the report, the proposed measures will also reinforce Geneva's profile as an international hub for digital issues in general.

Ownership/protection

AI systems, which are partly trained with data that are themselves subject to legal provisions – as stipulated under Swiss intellectual property law – must be protected adequately. Furthermore, in certain circumstances, AI systems are also capable of creating "novelty", so that questions may arise concerning whether inventions created with AI technology may be protected by copyright or patents and, if so, who is entitled to the rights thereto.

Patents

In Switzerland, the prevailing opinion is that only natural persons may be inventors in the sense of the Swiss Patents Act (PatA), which excludes the possibility of recognising AI systems as inventors due to their lack of legal capacity and legal personality. However, it is irrelevant how inventions are created and a subjective achievement of the inventor is not required. Pursuant to Article 1 paras 1 and 2 PatA, patents are granted for new inventions

applicable in the industry, whereas anything that is deemed obvious based on the current state of knowledge cannot be eligible for patent protection.

According to prevailing opinion in Switzerland, Swiss patent law recognises only natural persons as inventors in the legal sense. However, inventions created through or by AI can be assigned to a natural person as an inventor and are thus, in principle, patentable. The natural person who first took note of the invention and understood it as a solution to a technical problem is usually considered the inventor of an AI-generated invention.

Copyright

According to Article 2 para. 1 Swiss Copyright Act (CopA), works that are considered an intellectual creation with individual character may be protected by copyright. Under the CopA, computer programs may also qualify as works and therefore enjoy copyright protection if they meet the legal requirements. It can be argued that AI algorithms as expressed in a certain programming language may be subsumed under the concept of a computer program and thus copyrightability of such AI may be affirmed. Although the CopA provides no legal definition for a computer program, it is commonly understood in a narrow sense so that AI may not be considered as a copyrightable work under the CopA after all. It may, however, be argued that the lack of a legal definition reflects the will of the Swiss legislator to leave room for future technological developments and new forms of potentially copyrightable computer programs that include or use AI. Furthermore – and similarly to Swiss patent law – pursuant to Article 6 CopA, only natural persons may be authors of copyrightable works. If computers are used as tools of the author, a work may be attributed to the natural person who is controlling the AI-based process. However, if a work was autonomously created by a computer without any human control involved, copyrightability may be denied as the work is not considered attributable to a natural person. Where, exactly, the line should be drawn between AI as a simple tool and AI autonomously acting as an author (or rather creator) of the work is currently the subject of controversial debate. If, however, an intellectually creative relationship between the human programmer or operator of an AI and the AI-generated work no longer exists, there is a risk copyright protection will be denied under Swiss copyright law.

Furthermore, many AI applications require substantial amounts of data for their learning and training process, such as photographs used for training image-recognition software. As some of this data will regularly be protected by copyright and the gathered data will usually be reproduced for use by the AI application, this may constitute, if used without a licence, a copyright infringement as stipulated in Article 10 para. 2 letter a CopA, since the right to produce copies exclusively pertains to the author of the work. Swiss copyright law will therefore have to address this issue in view of the rapid development of AI systems heading towards more autonomy.

Antitrust/competition laws

Antitrust

The use of AI may be relevant under antitrust law if parameters relevant to competition, such as prices, are affected. In particular, price algorithms can be specifically programmed in such a way that prices agreed between competitors for online offers are not undercut or used to implement signalling strategies. Further, price algorithms may promote behavioural coordination between competitors as market transparency is increased and the possibility of reacting more frequently and more quickly to price adjustments is thus extended. However, the Swiss Cartel Act (CartA) is worded in a technology-neutral manner and hence does not

contain any specific provisions on the use or implementation of AI, so that the general rules – in particular, the provisions on the prohibition of cartels – apply. If algorithms are used in a coordinated manner and with the intention of influencing the price as a competitive parameter, this may constitute a deliberate and intentional interaction, and thus an agreement affecting competition, in accordance with Articles 4 paras 1 and 5 CartA. Moreover, price algorithms can potentially be relevant with regard to unlawful practices by dominant undertakings or undertakings with relative market power in accordance with Article 7 CartA. According to Article 7 CartA, a relative market power or dominant market position may not be abused by undertakings in order to hinder other undertakings from starting or continuing to compete or disadvantage trading partners. If a price algorithm is used to enforce unreasonable prices or terms and conditions and provided other undertakings are hindered from starting or continuing to compete or concerned undertakings are disadvantaged and there is no justification for such behaviour, the latter may qualify as unlawful under the CartA.

Unfair competition law

If false or misleading information affects competition, the Swiss Act against Unfair Competition (UCA) applies. The purpose of the UCA is to enable providers, customers, trade associations and consumer protection organisations to take legal action against the dissemination of market-relevant disinformation. If consumers' purchase decisions are manipulated in a legally relevant matter by means of, e.g., recommendation algorithms or other AI applications, there is a risk that consumers may invoke the provisions as stipulated in the UCA. However, currently, there is hardly any pertinent case law in Switzerland regarding such manipulation so that it is unclear when courts would rule the latter to be legally relevant. For AI applications, such as, e.g., personalised prices or advertising, it is argued that a legally relevant manipulation under the UCA is likely to be denied, whereas it cannot be excluded that the situation could be viewed differently in cases where the decision-making is modelled in such a way that consumers appear to have no actual choice. Furthermore, the legal situation is unclear at present regarding situations where AI applications lead to non-market-relevant manipulations. In any case, further development of the law including upcoming relevant core practice will have to be closely monitored to discern potential future differences between user manipulation facilitated by AI applications that are deemed permissible under current laws, and those that are legally significant and therefore problematic.

Board of directors/governance

According to the Swiss Code of Obligations (CO), a Ltd.'s board of directors is responsible for either managing the business itself or assigning the responsibility of management to a third party. If assignable tasks are given to third parties, the board of directors of a Ltd. is only liable for the selection, instruction and supervision of the representatives. However, according to Article 716a CO, the board of directors has seven non-transferable and inalienable duties. These include the overall management of the company and the issuing of all necessary directives, the determination of the company's overall organisation as well as the organisation of the accounting, financial control and financial planning systems as required for general management of the company. In Switzerland, there are currently no AI-specific guidelines with which a board of directors must comply. However, when addressing the topic of corporate governance, Swiss companies often follow the "Swiss Code of Good Practice for Corporate Governance", a guide published by *EconomieSuisse*, the umbrella association of Swiss companies, and the corporate governance directives of *Six Swiss Exchange*, the Swiss stock exchange.

Under the keywords "digital board member", the use of AI in boards of directors has recently been discussed more frequently. It is highly plausible that AI will be used in activities that require a high degree of rationality and data-driven decision-making. By providing data-supported insights and improving the prediction of outcomes, AI has the potential to enhance decision-making processes, enabling decisions to be based on knowledge backed by data, and allowing for better prediction of the impact of such decisions. There is currently no obligation under Swiss law to include AI in board decisions, but it remains to be seen whether an obligation to use AI can be derived from the board's due diligence in the future (see also the section "Civil liability"). It may therefore be worthwhile for a board of directors to already analyse the benefits that AI could bring in the area of corporate governance. The use of AI can be seen as an extension of the board's competences and can generate enormous benefits. The advantages made possible by the selective use of AI, if identified early, can be a crucial competitive advantage. It is advised that the responsible board of directors follows this trend.

Regulations/government intervention

In 2018, the Federal Council made AI a core theme of the so-called "Digital Switzerland Strategy", a strategy on digital policy, which is complemented by further sectoral strategies. The strategy is relevant for the actions taken by the Federal Administration and can serve as a framework for other Digital Switzerland stakeholder groups, such as the scientific and business community, the administrative authorities and civil society. As part of the strategy, an interdepartmental working group on AI was established. In December 2019, the group published a report in which the AI challenges Switzerland may face are explained. The report stated that relevant legal principles in Switzerland would usually be worded in a technology-neutral way so that they could also be applied to AI systems. It was specifically pointed out that the existing legal framework would already permit and regulate the use of AI in principle (e.g., Federal Act on Gender Equality), and apply in particular to discrimination that may arise as a result of AI decisions (see also the section "Discrimination and bias"). Thus, in summary, for the moment, there is no need for fundamental adjustments to the legal framework. In 2020, the same interdepartmental working group then developed guidelines on the use of AI within the Federal Administration, meaning a general frame of reference for federal agencies and external partners entrusted with governmental tasks. The guidelines were adopted by the Federal Council in November 2020.

The "Digital Switzerland Strategy" sets guidelines for Switzerland's digital transformation. The Federal Administration is obliged to adhere to it, while it also serves as a guiding principle for stakeholders involved in digitalisation. Switzerland wishes to prioritise digital offerings for the benefit of all citizens (digital first). Every year, the Federal Council determines a couple of key topics as "*focus themes*" – these serve as a starting point for new measures and for Federal Council mandates. The three focus themes of 2023 are digitalisation in the healthcare sector, digitalisation-friendly legislation and digital sovereignty.

In 2021, the Federal Council indicated that the relevant developments regarding the European regulation of digitalisation and their impact on Switzerland would be closely monitored in order to be able to take measures at an early stage if necessary. It may be noted that the further development of the EU's draft AI Act will increasingly influence political processes and debates about the topic of AI regulation in Switzerland. Switzerland will inevitably have to position itself on the topic – firstly, because research and politics are increasingly calling for the adoption of framework conditions for the reasonable use of AI. Secondly, Switzerland is shaped by EU legislation, and is closely linked to the EU internal

market and therefore dependent on (EU) market access. While this does not necessarily imply that Switzerland must conform to the regulations of the EU, the need for action will undoubtedly increase once the AI Act comes into effect. A reflective and evidence-based debate on how the use of AI should be shaped in Switzerland is thus to be expected – especially because a high number of AI companies are based in Switzerland (see also the "Trends" section).

Civil liability

A crucial challenge regarding the use of AI is civil liability in the event of damage. Even though the general provisions on liability, as stipulated in the Swiss CO, also apply to AI systems, proving that the respective prerequisites for liability are met is associated with difficulties, particularly concerning the proof of fault. Certain areas of law have provisions on liability that apply to AI systems as well, such as for autonomous vehicles in the Swiss Road Traffic Act (RTA) or for autonomous drones in the Swiss Air Traffic Act. If, for instance, an autonomous vehicle causes an accident due to a faulty object detection system, questions regarding who or what is liable for the damages incurred arise. In the case of a regular vehicle, object detection and collision avoidance are the responsibility of the human driver. However, for autonomous vehicles, the AI system takes charge of these functions. In any case, under current Swiss law, the owner of the vehicle is subject to civil liability pursuant to Article 58 RTA, irrespective of the nature of the vehicle. Furthermore, it increasingly becomes apparent that in the future the focus of civil liability in Switzerland will be on the manufacturer of AI systems. In that respect and with certain adjustments to be made, the Swiss Product Liability Act (PLA) could gain importance in view of future technological developments for AI systems.

Swiss product liability law in its current state does not fit AI applications well, especially when it comes to determining the product nature of software, inaccuracy of decisions or aftermarket obligations of the manufacturer. Additionally, the role of the manufacturer is changing in light of the variety of persons influencing the design, functioning and use of AI systems.

In accordance with the prevailing doctrine in Switzerland, software may be classified as a product under the PLA, as it can create risks of damage typical of a product. As a result, liability derived from the PLA may also be applicable to AI applications. The standards for determining defectiveness of AI applications need, however, to be clarified under Swiss law, especially since many AI systems are self-learning, constantly evolving and thus potentially beyond the manufacturer's sphere of responsibility. According to Article 4 PLA, a product's defectiveness is assumed if it does not offer the safety that may be expected considering all circumstances at the time the product is first placed on the market. Pursuant to Article 5 PLA, there is no liability for defects that only arise after the product was placed on the market. This may give rise to certain issues, especially considering that some AI applications are self-learning and adapting to their environment. This means that in certain cases AI systems may develop new and independent solutions only after first being put on the market, so that liability for such later and potentially erroneous modifications would be excluded under the current legal system. In principle, the manufacturer of an AI application is supposed to minimise the potential risks emanating from the AI through careful programming and training. However, where self-training and self-learning AI applications are concerned, the control of the manufacturer is reduced substantially. On the other hand, users of the AI may be able to influence an AI system by selecting the learning

method or the duration of the learning process as well as the training data. It might hence be argued that users may be liable if their influence leads the AI to a faulty decision that causes damage, so that manufacturers may exonerate themselves due to the improper influence of third parties. Again, it might prove helpful to clarify these uncertainties in terms of liability with an amendment of the current legal framework.

Under Swiss contract law, the obligor is liable for any intentional or negligent breach of contract. Accordingly, if an AI application causes a breach of contract, the operator may be liable in case of intentional or negligent use. A point of debate is whether the use of an AI system in a particular field of service, once established, may eventually become the minimum standard for diligently provided services.

At present, various new forms of legal basis of liability for AI systems are discussed such as, e.g., applying existing liability provisions by analogy, the introduction and implementation of further sector-specific liability clauses distinguishing between the manufacturing and the use of AI applications or the introduction and implementation of provisions for liability of AI systems specifically.

Criminal issues

Swiss criminal law is technology-neutral and the Swiss Criminal Code (CrC) does not provide any specific provisions regarding criminally relevant behaviour of AI systems. According to the general principles under Swiss criminal law, the personal culpability of the offender is required. However, the possibility of AI applications acting culpably is currently denied, as they have neither legal capacity nor legal personality. Thus, criminal liability must necessarily be attributed to either the manufacturer, programmer or operator of an AI application.

If an AI system carries out an action that qualifies as a criminal act under the CrC, the question of who is responsible or what caused the AI system's criminally relevant action arises. If the cause of action lies in faulty programming, this may constitute a negligent act of the programmer or manufacturer. However, in case of negligence, the CrC must explicitly state that the negligent act is punishable for the specific offence. Further, in case of negligence, there must be a violation of duty of care that led to or caused the punishable offence, and it must have been foreseeable for the offender that the adopted behaviour would lead to the punishable offence. However, the foreseeability on the side of the offender may be hard to assume if the AI application concerned operates rather autonomously and especially if it is self-learning and adaptive. Hence, it may be questionable if the evolved behaviour of the AI system is still attributable to the manufacturer, programmer or operator. Moreover, if the concerned AI application was deliberately programmed to induce the criminal act, manufacturers, programmers or operators may be viewed as having acted intentionally (this may be relevant with regard to misuse of military equipment such as drones or in terms of cybersecurity, for instance, when it comes to hacking robots). In a case where the AI application was programmed correctly but used improperly, the operator or user may be criminally liable.

A recent trend shows that AI systems may be implemented as tools for so-called Predictive Policing and crime prevention, which rely on big data, AI algorithms and the evaluation of the same. Predictive Policing encompasses predictions about the occurred crime itself and the crime location, predictions about the victim(s), predictions about an individual's potential delinquency and predictions about the criminal profile of the offender(s). The aim of Predictive Policing is the evaluation of existing data and a gain in knowledge that ultimately allows for estimations or assessments on the crime and at best for prevention of future crimes. Nonetheless, as AI algorithms are unlikely to ever be completely neutral or

unbiased, Predictive Policing may lead to problematic or even discriminatory assumptions based on the collected and combined data. As this is a new concept, in Switzerland there is a lack of clarity on its implementation and handling. What is required in the future is therefore a comprehensive definition of the scope and specific application necessary.

Discrimination and bias

Data protection – Automated individual decision-making

In a growing number of areas of life, technological advances – especially in the field of AI or machine learning – are leading to an increase in automated decisions based on algorithms. A practical example is the automated decision in an application procedure or an automated termination of a contract. In Switzerland, automated decisions are specifically regulated under the revised Federal Data Protection Act (FADP) with its entry into force on 1 September 2023. The revised FADP contains a provision for decisions that are taken exclusively on the basis of automated processing. The provision obliges the data controller to inform data subjects of automated individual decisions that have legal effects on the data subjects or affect them significantly (unless exceptions apply). Although the substantive content is similar to that of the GDPR, the Swiss provision is based on a completely different concept: the new provision in the revised FADP is merely a duty of information and not a prohibition as in the GDPR. If the requirements of the duty of information are met, data subjects have the possibility to state their position upon request. Data subjects may also request that such decision be reviewed by a natural person, for example, because the data subjects suspect that they have been disadvantaged by an AI due to bias. However, there is no possibility for data subjects to challenge the decision, as is the case under the GDPR.

Transparency is important for the users of AI applications in order to be able to understand with which data an algorithm has been trained and how the algorithm is constructed. The draft EU AI Act specifies under the provisions on transparency requirements for high-risk AI systems what is required in the GDPR regarding the disclosure of logic in automated decision-making. Such a specification is missing under Swiss law – although the revised FADP explicitly states within the provision on access rights that data subjects must be informed about the logic on which the decision is based; however, it does not say anything about how the logic of automated decisions must be disclosed. It may be argued that a company will not be obliged to provide a detailed explanation of the algorithms used or to disclose the entire algorithm. Nevertheless, the information provided should be comprehensive enough to allow data subjects to understand the reasons behind the decision.

For this reason, companies are advised to develop simple procedures to inform the data subjects concerned about the underlying considerations and criteria of the automated individual decisions. For this purpose, it would be sensible to implement an appropriate internal process and to analyse the AI application to be used well in advance.

Bias by AI in the context of employment

There is no general anti-discrimination law in Switzerland. However, under Swiss labour law, there is a general principle of non-discrimination that is derived from the concept of protection of personality as stipulated in Article 328 CO. A discriminatory violation of personality exists if the unequal treatment of an employee is linked to personality traits that are sensitive to discrimination. Pursuant to Article 328 CO, AI applications in the employment context must not be programmed in such a way that they discriminate directly nor indirectly, i.e., have a discriminatory effect on different groups of employees (based on age, gender, race, nationality, etc.) despite neutral programming, unless such application is objectively justified and

proportionate. The general principle of non-discrimination under labour law is complemented by other principles of non-discrimination based on special legislation. These are the following:

(1) direct and indirect discrimination linked to gender is prohibited under the Swiss Gender Equality Act;
(2) the Swiss Disability Discrimination Act stipulates the principle of non-discrimination for disabled people, although it only applies to federal employment contracts and not employment under private law;
(3) the Swiss Act on Human Genetic Testing provides protection from genetic discrimination; and
(4) the Agreement of Free Movement of Persons between the EU and Switzerland prohibits discrimination of European migrant workers with regard to recruitment, employment and working conditions.

An AI application commonly used in employment consists of the so-called "People Analytics" (forming part of "Predictive Analytics"), which helps employers identify, hire, retain and reward their employees via data analysis. This is done with the help of algorithms that aim to slice and dice a large amount of data to extract specific information on employees. The so-called Big Data collected during this process and the AI systems used can then combine previously unrelated data to make accurate predictions via Predictive Analytics. Further, machine learning models are used to identify trends, patterns and relationships between the gathered data of employees. On the basis of the patterns discovered, things and activities will be classified, their value estimated, and behaviour predicted based on probabilities. The goal of Predictive Analytics is to provide a foundation for attributing certain characteristics to an individual employee that are linked to other employees who appear statistically similar. Within the same process, those employees who appear statistically different will be separated from the rest so that a (statistical) discrimination may occur. Discrimination can be related to the input data, the analysis model or the output of the applied AI application.

While AI may help employers optimise operations in their business, the AI applications used may (involuntarily) discriminate employees. However, certain legal authors argue that the currently applicable legislation that offers protection against employee discrimination does not (sufficiently) cover discrimination by AI applications, due to the difficulty of proving its existence and due to the lack of deterrent sanctions when violating the applicable law.

National security and military

Switzerland is considered a hub of sorts in terms of cybersecurity, with different notable actors promoting cooperation and interaction in this field. In 2019, the so-called "Cyber-Defence Campus" was founded, where governmental, academic and industrial actors interact and which focuses on various matters of national defence also with regard to cybersecurity. As the Swiss government detected a lack of clear policy in respect of cybersecurity, it adopted, in 2018, a national strategy for the protection of Switzerland against cyber-risks (the so-called "NCS") with the aim of implementing a broad set of measures. The NCS also led to the creation of a centralised cybersecurity body on a federal level, the National Cyber Security Centre (NCSC), which, amongst other tasks, serves as a contact point for market actors. The NCS further had an impact on federal laws, particularly in bolstering governmental powers in respect of intelligence services. However, there is currently no overarching and interdisciplinary cybersecurity act nor any political agenda of adopting such regulation.

Hence, Swiss data protection legislation often remains the starting point for any assessment of cybersecurity practices. The revised FADP as well as the revised Data Protection Ordinance call for state-of-the-art data security measures without specifying technical standards, just like its predecessors (in force until the end of August 2023). The revised FADP thus maintains a future-proof and technologically neutral design. Additionally, the revised FADP contains a duty to report, in certain circumstances, data breaches to the competent data protection authority (the Federal Data Protection and Information Commissioner) or even the data subjects directly. Moreover, the Swiss government wants to introduce a notification obligation for operators of critical infrastructures that are victims of a cyber-attack. Therefore, in December 2022, the Federal Council adopted the dispatch on amending the Information Security Act and submitted it to Parliament. The proposal creates the legal basis for the reporting obligation for the operators of critical infrastructures and defines the tasks of the NCSC which is intended to be the central reporting office for cyberattacks.

It is important to note that, under the revised FADP, individuals who intentionally fail to comply with the minimum data security requirements may face criminal fines of up to CHF 250,000. Thus, the criminal fines are not imposed on the company but on the person responsible for the data protection violation. However, under the revised FADP, companies may also be criminally fined – up to CHF 50,000 – if an investigation on determining the responsible natural person within the company or organisation would entail disproportionate efforts. The offending persons are fined by the state prosecutors of the Cantons tasked with the enforcement of the revised FADP's criminal law provisions. The criminal fines are expected to work as a strong incentive for businesses or their responsible managers to ensure state-of-the-art cybersecurity.

Lastly, it should also be noted that governmental authorities, such as Swiss criminal prosecution authorities or the Federal Intelligence Service, have considerable legal competences when it comes to telecommunications surveillance and are permitted to penetrate protected systems for national security purposes under certain circumstances.

* * *

Acknowledgment

The authors would like to thank Stefanie Röthlisberger for her valuable support in the preparation of this chapter.

Jürg Schneider
Tel: +41 58 658 55 71 / Email: juerg.schneider@walderwyss.com

Jürg Schneider is a partner and co-head of Walder Wyss's data protection team and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. Jürg's special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of the GDPR and the revised Swiss FADP for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc.) on data protection requirements.

David Vasella
Tel: +41 58 658 52 87 / Email: david.vasella@walderwyss.com

David Vasella is a partner and co-head of Walder Wyss's regulated markets, competition, tech and IP team. David advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. He deals with cross-jurisdictional data-protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. David also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. He is an editor of the Swiss journal for data law and information security and a member of the professional bodies International Association of Privacy Professionals and the German Society for Law and Information Technology.

Anne-Sophie Morand
Tel: +41 58 658 56 34 / Email: anne-sophie.morand@walderwyss.com

Anne-Sophie Morand is an associate in the Regulated Markets, Competition, Technology and IP team at Walder Wyss. She advises on all aspects of data protection, information and technology law. Prior to joining Walder Wyss, Anne-Sophie Morand worked for the Swiss Data Protection Authority and the Swiss Parliament, and as a research assistant at the University of Lucerne. She obtained a Ph.D. with a thesis in the field of personal rights and sports sponsorship. In addition to her work at Walder Wyss, she also completed an LL.M. in IT Law at the University of Edinburgh with a specialisation in "Law and Artificial Intelligence". She regularly publishes and lectures in her fields of expertise.

Walder Wyss Ltd.

Seefeldstrasse 123, P.O. Box, 8034 Zurich, Switzerland
Tel: +41 58 658 58 58 / URL: www.walderwyss.com

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 semi-conductor 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 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 accordance with a relevant news report in 2022, the next phase of the Taiwan AI Action Plan would focus on explainable and trustworthy AI, as well as the development of advanced technologies for small or medium-size enterprises such as joint learning, automated machine-learning tools, self-supervised learning and migration learning, and low-code platforms to accelerate AI development. Furthermore, the Industrial Technology Research Institute ("ITRI") is dedicated to establishing the infrastructure of AI governance, such as an AI testing and evaluation centre to measure AI risk, model performance and robustness. The ITRI will also set up an AI product-validation mechanism which aims to promote the development of the industry.

In addition to the above, the Ministry of Science and Technology under the Executive Yuan further announced the "AI Technology R&D Guidelines" in September 2019, in order to demonstrate the Taiwan government's commitment to improving Taiwan's AI R&D environment. Considering that 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. According to a relevant news report, the Taiwan government will continue to promote the 5+2 Industry Innovation Plan 2.0 in the future. The "Act for the Recruitment and Employment of Foreign Professionals", as enacted in 2017 and amended in 2021, 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. At the time of writing, while to our understanding there exists no court decision specifically addressing such issues, two laws were promulgated in 2018 to cope with these new trends. These laws are: the law for a Financial Technology Development and Innovative Experimentation Act ("FinTech Sandbox Act"); and the Unmanned Vehicle Technology Innovation and Experiment Act ("Unmanned Vehicle Sandbox 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. As of 18 November 2022, 13 applications for experiments of autonomous vehicles have been approved by the competent authority of the Unmanned Vehicle Sandbox Act, the Ministry of Economic Affairs ("MOEA").

In August 2022, the Ministry of Digital Affairs ("MDA") (which is under the Executive Yuan, the Cabinet of Taiwan) was formally established for matters in relation to facilitating Taiwan's digital development of its telecommunications, information, cyber security, internet and communications industries, coordinating national digital policies, supervising national cyber security policies, managing communications and digital resources and assisting digital transformation. According to the Organization Act of the Administration for Digital Industries, MDA, the Administration of Digital Industries is in charge of providing guidance and incentives for interdisciplinary digital innovation of AI, big data, platform economy and other digital economy-related industries. In addition to the above-mentioned legal issues, there have also been some discussions regarding the legal profession, such as how AI may impact said 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 of 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 as AI develops. 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 for humans to use. 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 intellectual property regime in Taiwan; it is really a challenge faced by and needed 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, including medical treatment and health examination information; genetic information; sexual-life information; criminal record; contact information; financial conditions; social activities; and other information that may directly or indirectly identify an individual.

Under the PDPA, unless otherwise specified under law, a company is generally required to give notice (notice requirement) to and obtain consent (consent requirement) from 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 a purpose regarding AI and/or big data, it will be subject to the obligations under the PDPA as advised above.

Furthermore, the Taiwan Constitutional Court announced a judgment in August 2022 (Ref. no.: Xian-Pan No.13), holding that relevant laws should be promulgated or amended within three years, so that there would be: (i) an independent supervision mechanism for personal data protection under the PDPA; and (ii) clear provisions regarding protection of personal data stored, processed, transmitted and used in the National Health Insurance Research Database ("NHIRD"), which contains the public's personal data collected through Taiwan's national health insurance system. Therefore, it is suggested to closely follow any amendments to the PDPA and related laws and regulations in the near future.

Antitrust/competition laws

Under Taiwan's antitrust/unfair competition 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 having a "meeting of minds" could be an issue when discussing and debating in court.

In addition, there have been some discussions on the competition issues of data-driven industries (including digital platforms) in Taiwan, and such discussions express concerns over the restriction of competition and/or abuse of market power arising from big data collected and used by data-driven industries and calls for the attention of the government as well as legal academia. Some academic discussions are of the view that amendments to competition laws to respond to digital economy developments do not seem to be necessary at this stage, but the regulators and the legislators should keep monitoring the changes. Besides, some researchers are of the view that, unlike the U.S. government's concern over GAFAM (Google, Apple, Facebook, Amazon, Microsoft), the data-driven industries in Taiwan are still under development and this factor should also be considered when examining the current competition law regime. To date, there have been no specific policies and/or law amendments to the FTA proposed by the competent authority specifically addressing the developments of AI. Nevertheless, given the rapid growth of use of big data and data-driven industries, the development of Taiwan's competition laws to address issues arising from big data are worthy of observation.

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 or she 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 cases 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 they involve any AI-related issues. The engagement of (an) 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, must 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 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 Sandbox Act in late 2018. The Act provides 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 must 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 FSC for fintech sandboxes, or the MOEA 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 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 at the time of writing, although several applications have been filed for the regulatory sandbox for unmanned vehicles and fintech, respectively, it is still not very clear which type of idea and technology would be considered "innovative" by the relevant competent authority with

respect to AI in the context of the above regulatory sandbox, as well as 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 use in 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 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 that 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 191-2 of the Civil Code: If an automobile, motorcycle or other motor vehicle that 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 or she has exercised reasonable care to prevent the damages.
(3) 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 or 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, similarly to the discussion on tort liability, with regard 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, a partner at Lee and Li, 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, and 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.

Mr. Hsiung 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 investigation. 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

Thailand

John Formichella, Naytiwut Jamallsawat & Onnicha Khongthon
Formichella & Sritawat Attorneys at Law Co., Ltd.

Trends

Over the past several years, Thailand has been researching, developing and applying artificial intelligence (AI) and machine learning (ML) in the public and private sectors through international collaborations with AI developers. Therefore, Thailand is adapting to AI to leverage its benefits in various areas, as demonstrated by its efforts to keep pace with current trends and adapt them for practical purposes.

The role of AI has become increasingly common in various sectors. For example, in the financial industry, AI has been employed to analyse customer behaviour to recommend appropriate investment and saving options for each customer. Furthermore, as Thailand is one of the global hubs for healthcare services, the health industry has applied AI to analyse and diagnose diseases. For instance, AI is utilised to aid in diagnosing lung disease by detecting abnormalities in chest x-rays and indicating the likelihood of tuberculosis (TB analysis score) during the early symptomatic phase. Additionally, IBM Watson's AI technology has been employed to analyse cancer treatment. Moreover, the public sector, such as the Revenue Department, has also begun to use AI to analyse tax submissions. After the introduction of AI and ML, big data has been extensively utilised across both large and small organisations in Thailand to facilitate a competitive edge for businesses.

Currently, financial institutions are leaders in adopting AI/ML to analyse strategic and non-strategic functions. Financial institutions utilise AI/ML within three primary work groups: customer service, whereby they offer service products that align most effectively with the customers' requirements; system improvement, wherein they verify the accuracy of documents; and risk management, whereby they evaluate the risk involved in loan provision and detect fraud through intricate forms. In practice, financial institutions will use AI from a third-party service provider. However, financial institutions that wish to use third-party services for essential strategic functions that financial institutions themselves must carry out may not comply with specific regulations. In such cases, financial institutions shall apply for approval or waiver from the Bank of Thailand (BOT) on a case-by-case basis. Nevertheless, the BOT prescribes considerations regarding the usage of AI/ML to be fair, non-discriminatory, accountable, transparent, secure and reliable.

According to the Government Artificial Intelligence Readiness Index 2020, Thailand was ranked 60th due to the need for more AI policies and action plans. Consequently, the Cabinet approved the (Draft) Thailand National AI Strategy and Action Plan (2022–2027) (AI Plan) on 26 July 2022, under the vision that "Thailand has an effective ecosystem to promote AI development and application to enhance the economy and quality of life within 2027".

Ownership/protection

The status of AI as property or non-property is currently debatable in Thailand. However, the Thai Civil and Commercial Code (CCC) defines "property" as corporeal and incorporeal objects that have value and can be appropriated. Therefore, under Thai law, AI could be classified as property (an incorporeal object) if deemed valuable, and the creator will own an AI algorithm.

AI is protected under intellectual property law. Nonetheless, the Copyright Act B.E.2537 (1994) (CRA) covers computer programs, which it defines as instructions, sets of instructions or any other things used with a computer to operate the computer or generate an output, whatever the computer language is. Therefore, the CRA only protects the source code and not an algorithm. Further, if an employee creates an AI, the employee will generally own the copyright to that AI unless there is a written agreement stating otherwise between the employee and the employer. Regarding the protection of AI inventions under the Patent Act B.E.2522 (1979) (PA), it's important to note that the PA does not protect inventions related to computer programs or scientific and mathematical theories or rules. In academic circles, an "algorithm" is often considered a component of a scientific or mathematical theory. Therefore, the innovation of an AI may not be eligible for protection under the PA.

Data is protected under Thailand's Personal Data Protection Act B.E.2562 (2020) (PDPA). The collection, processing, use and disclosure of any personal data are subject to the obligations under the PDPA. To collect, process, use or disclose personal data, the data controller must obtain consent from the data subject or have a legal basis, such as legitimate interests, public task, execution of a contract, etc.

Consent must be obtained in writing or electronically, and any fraudulent or misleading practices to obtain such consent are prohibited. The use or disclosure of personal data for purposes other than those initially consented to by the data subject are also prohibited unless permitted by law or the data controller obtains the data subject's amended consent after informing them of the new purpose. A data subject has the right to withdraw their consent at any time unless restricted by law or an agreement beneficial to the data subject. For example, suppose a personal data controller fails to comply with the provisions of the PDPA; in that case, the data subject may request the deletion, destruction, temporary suspension or conversion into an anonymous form of their personal data.

Board of directors/governance

There is no explanation for whether AI is harmful or not. However, AI could be defined as property that poses a danger under section 437 of the CCC, which prescribes that a person possessing property that poses a danger is responsible for any resulting damages. Moreover, section 85 of the Public Limited Companies Act, B.E. 2535 (1922) (PLCA) prescribes that directors have fiduciary duties and the obligation to perform their responsibilities per the law. Therefore, if any director performs any act, or omits any action, that causes loss to the company, the director will have liability.

As companies increasingly incorporate AI and big data into their operations, there are several Thailand corporate governance issues that directors need to be aware of, as follows:

(1) Data Privacy: Companies must collect data per privacy laws and regulations. The company must be transparent about using personal data and obtain user consent. Thus, a director should be fully aware, or appoint advisors that are fully aware, of how AI collects data, how the data is used and the security of personal data.

(2) Explanation: AI systems have become more complicated, so it can be challenging to understand how they make decisions. Companies must be able to explain how AI systems execute those decisions.
(3) Accountability: Companies must be accountable for the decisions made by their AI systems. They need mechanisms to address any adverse consequences or damages resulting from their use, apart from the PLCA and CCC.
(4) Cybersecurity: Companies must protect their AI and big data systems from cyber threats.

Regulations/government intervention

As of April 2023, Thailand does not have specific AI and ML laws. However, the critical issues under the AI Plan are as follows:

(1) Building a foundation for AI development includes establishing a national database, improving digital infrastructure and investing in education and research to cultivate AI talent and expertise.
(2) Promoting AI adoption in various sectors: The AI Plan identifies several sectors where AI can be applied, including healthcare, transportation, agriculture and manufacturing. The government aims to encourage the adoption of AI in these areas to improve efficiency, productivity and quality of life.
(3) Encouraging innovation and entrepreneurship: The AI Plan seeks to foster a culture of innovation and entrepreneurship in AI by providing support for startups, creating incentives for investment and promoting collaboration between the public and private sectors.
(4) Ensuring ethical and responsible use of AI: The AI Plan acknowledges the potential risks and challenges and emphasises the need for ethical and responsible development and deployment of AI technologies.

Overall, the AI Plan seeks to position the country as a leader in AI development and adoption, focusing on leveraging AI to drive economic growth and improve the quality of life for its citizens.

The approach that businesses must manage risks and potential liabilities is that they must determine which risks could significantly harm the organisation's business strategy or operations. Managing such risks involves monitoring internal and external operating and regulatory environments to identify any alterations to the underlying risk landscape and guarantee that the framework is still appropriate.

AI in the workplace

The advancement of technology leads to the various uses of AI in the workplace. AI has the potential to increase profits in many businesses. Moreover, AI can analyse customers' needs from an information base, and the company will use those databases to respond to customers' needs. Nonetheless, there are some concerns about AI replacing humans. A business can use AI-powered automation in numerous ways, such as automating repetitive tasks, analysing large amounts of data as above-mentioned and even making decisions based on that data. For example, some manufacturing industries in Thailand use robots to automate tasks such as assembly, welding and packaging. Chatbots automate customer interactions in the customer-service industry and provide quick and accurate responses to common inquiries without violating labour law. According to Section 121 of the Labor Protection Act B.E. 2541, companies must compensate employees who have terminated

an employment contract due to implementing machine automation to replace a worker. This obligation extends to machines such as chatbots or restaurant robots used for service. Companies must recognise and adhere to this legal requirement as Thailand has a Labour Relations Board that aggrieved employees may file complaints to.

To address this issue, the AI Plan urges governments, businesses and individuals to work together to develop strategies to help displaced workers. However, they must be aware that according to the guiding principle of AI set forth by the Berkman Klein Center for Internet and Society, the objective of creating AI is to support and promote human values. Therefore, AI technology must not supplant human workers.

Civil liability

There are no specific laws regarding AI civil liabilities in Thailand at the time of writing. Nonetheless, AI technology may be considered as property that poses a danger under section 437 of the CCC, whereby any individual who owns or controls a property which poses a threat is responsible for any resulting damages. As an illustration, in cases involving smart cars (i.e., advanced driver-assistance systems), the burden of proof is placed upon the owner or controller. It is important to note that this differs from general civil cases under the Civil Procedure Code, wherein the plaintiff bears the onus of providing evidence of wrongdoing on the part of the disputant. Another point that must be considered is whether the controller or owner would be liable under this provision if the damages are caused by an error in the AI system itself, such as a glitch or autonomous decision-making, without any involvement on the part of the controller or owner. Currently, there are no court decisions regarding damages caused by this type of incident as *force majeure*. Therefore, if the controller or owner can prove that the injuries were caused by *force majeure*, they will not be liable for the damages. However, the burden of proof is on the controller or owner.

According to the Product Liability Act B.E.2551 (2008) (PL), AI may be considered unsafe goods resulting by design. "Goods" are all property produced or imported for sale, including agricultural products and electricity. Therefore, if AI is a tangible asset, movable and not permanent, AI will be under this law, such as robots, drones and cars. Other elements of AI, such as algorithms and source code, are not within the scope of enforcement under the PL. A violation under the PL includes determining compensation for the injured party, which may consist of double damages for actual damages or compensation for emotional injuries that the CCC does not provide. In addition, an agreement between a business and a customer to limit or exempt liability for damages resulting from the use of AI cannot be enforced. If there is such an agreement, the agreement shall be voided and unenforceable under the PL.

Criminal issues

At the time of writing, no specific criminal laws are related to AI. In addition, there is no supreme court decision to clarify the definition of AI. However, the Criminal Code can apply to an incident where an AI robot or system commits a crime. It is necessary to examine whether the owner or controller of AI intended to commit a criminal offence or acted negligently. If it is proven that the owner or controller of an AI had the intention to commit a crime or acted negligently, they will be held liable for any offence caused by the AI. Further, suppose an AI is compelling others to commit a crime; in that case, the AI may be considered as a tool used to commit the crime, and the owner or controller of the AI may be held liable for the offence only if it is proven that they intended to commit the crime.

Discrimination and bias

At the time of writing, no specific laws in Thailand address the issue of bias in AI systems. However, some laws and regulations may apply to AI systems that produce biased results, particularly those that impact individuals' rights and freedoms, are as follows:

(1) The PDPA: The PDPA regulates the collection, use and disclosure of personal data in Thailand. If an AI system collects and uses personal data in a way that results in biased outcomes, we believe it could violate the PDPA and anti-discrimination law and policy.
(2) The Computer-Related Crime Act B.E.2550 (2007) and its amendments (CCA): Under the CCA, computer-related offences in Thailand, as well as unauthorised access to computer systems and data, have criminal consequences. If an AI system is used to intentionally cause harm, damage or discriminate against individuals, it could be considered a computer-related offence under this law.

National security and military

At the time of writing, Thailand has no specific laws and regulations regarding AI under national security laws. However, it is anticipated that the AI Plan will achieve the following objectives:

(1) Generating employment opportunities in digital technology and AI.
(2) Enhancing the Gross Domestic Product by creating additional value in the manufacturing and service industries via AI.
(3) Enabling access to public services that AI facilitates.
(4) Augmenting human capability in digital technology and AI.

In a national security sense, in preceding years, there have been contentious matters concerning the transparency of employing software applications known as Pegasus, which originates from Israel. The Thai government used this application to monitor the activities of both anti-government groups and journalists. Numerous scholars and educators have extensively deliberated on the matter, concluding that the conduct mentioned above conflicts with the fundamental tenets espoused by the PDPA, the CCA, the Cybersecurity Act, and the violation of rights and freedom under the Constitution. Thus, a pressing need for a legal framework to govern and regulate the utilisation of AI from an organic law perspective is possible.

Conclusion

The laws and regulations related to AI in Thailand are insufficient, which may pose challenges for parties in the event of an AI-related dispute that goes to court. However, it should be noted that specific sectors, such as banking and insurance, have particular guidelines that acknowledge AI use. Furthermore, lawmakers need to consider expanding the scope of AI regulation beyond these specific sectors to ensure the technology is used responsibly and ethically across all industries. By implementing clear legal frameworks and guidelines, Thailand can create an environment that fosters innovation while ensuring that AI is developed and deployed to benefit society.

John Formichella
Tel: +66 2107 1882 / Email: john@fosrlaw.com

John Formichella heads our Telecommunication, Media, Technology and Data Privacy Practice, and is past Chair of the Information and Communications Technology Committee of the American Chamber of Commerce in Bangkok. He is rated as a Leading Individual by *The Legal 500* and ranked as a Band 1 individual by *Chambers and Partners*.

Considered a leading expert in the technology, media and telecommunications sector in Thailand, John has over 25 years' sophisticated experience, covering technology transactions, telecommunications law, data privacy, cyber-security, data-centre outsourcing, cloud computing, media (OTT service providers, film and television) and e-commerce.

Naytiwut Jamallsawat
Tel: +66 2107 1882 / Email: naytiwut@fosrlaw.com

Naytiwut Jamallsawat heads our Corporate and Regulatory Practice with particular emphasis on data privacy, cyber-security, telecommunications, satellite and space law, and energy sector issues. Naytiwut advises multi-national enterprises from North America, Europe, Singapore, Hong Kong SAR and Mainland China on diverse regulatory matters. His practice includes advising on corporate structuring for foreign direct investment and regulatory compliance in cybersecurity, data protection, media and telecommunications. He graduated from the prestigious Chulalongkorn University in Bangkok and furthered his studies in England at the University of Kent (LL.M.) and the University of Dundee (LL.M.).

Onnicha Khongthon
Tel: +66 2107 1882 / Email: onnicha@fosrlaw.com

Onnicha Khongthon is a Senior Associate with over four years' experience in the technology, media, and telecoms sector (TMT), including corporate and commercial matters. Onnicha has assisted in the preparation, review and consultation of various contracts, as well as the development of professional relationships and interaction with government officers and agencies. Onnicha continues to strengthen her knowledge in wide-ranging matters from general commercial and TMT issues to assisting in more complex contract negotiations and disputes. Onnicha has also gained valuable experience while assisting foreign businesses to establish themselves in Thailand, including company registrations, BOI applications, American Treaty registrations and obtaining Foreign Business Licences and Foreign Business Certificates.

Formichella & Sritawat Attorneys at Law Co., Ltd.

399, Interchange 21 Building, 23rd FL., Unit 3, Sukhumvit Road,
Klongtoey-Nua, Wattana, Bangkok 10110 Thailand
Tel: +66 2107 1882 / URL: www.fosrlaw.com

United Kingdom

Rachel Free, Charles Kerrigan & Barbara Zapisetskaya
CMS Cameron McKenna Nabarro Olswang LLP

Introduction

The UK is a leading country in artificial intelligence (AI) technology and policy – it is regarded as a centre of expertise in research and application. The year 2022 saw the UK tech industry reach a combined market value of £1 trillion, despite a difficult and uncertain economic landscape.[1] It is only the third country to reach this milestone, after the US and China.[2] Further, during 2022, UK tech companies showed their resilience and market leading capability by continuing to raise at near-record levels (£24 billion), more than France (£11.8 billion) and Germany (£9.1 billion) combined.[3] This takes the total raised over the past five years by UK tech companies to a staggering £97 billion.[4] In 2022, Digital Minister Paul Scully announced that "UK tech has remained resilient in the face of global challenges and the UK have ended the year as one of the world's leading destinations for digital businesses".[5]

The UK now has 3 million people working in technology jobs, with UK companies increasingly hiring for entry-level tech roles, up from 6,596 in November 2021 to over 15,000 in 2022.[6] There is still much potential to be unlocked in the AI space if the UK can continue to drive investment into the sector, with global AI spending expected to grow from $387.45 billion in 2022 to $1,394.30 billion in 2029 at a compound annual growth rate of 20.1%.[7] London is now widely considered the top tech ecosystem outside the US using a combination of factors including early, breakout and late stage funding, university talent, patents and unicorns and $1 billion plus exits.[8]

AI in the UK

The UK now has a statutory definition of AI, albeit not in legislation directly regulating it. The National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021 define AI as "technology enabling the programming or training of a device or software to – (i) perceive environments through the use of data; (ii) interpret data using automated processing designed to approximate cognitive abilities; (iii) make recommendations, predictions or decisions; with a view to achieving a specific objective".[9]

UK Government support for AI

The UK Government has identified innovation as one of its three core pillars of its "Build Back Better: our plan for growth", which was unveiled at the beginning of 2021, in the wake of the COVID-19 pandemic.[10] One of the aims of the Build Back Better plan is to support and incentivise the development of creative ideas by, amongst other things, developing the regulatory system in a way that supports innovation, as well as by attracting the best and brightest people from all over the world to boost the international competitiveness of the UK's businesses.[11]

AI investment in the UK continues to surpass previous levels, as noted above. The Government has stated that it is committed to increasing the levels of AI research and development (R&D).[12] 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 in 2021 to £22 billion by 2024–2025.[13] 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 programmes to capture the value of innovation.[14]

Despite state funding for AI initiatives not being addressed at length in the 2022 and 2023 Budgets, state funding in this area has continued to grow year on year.[15] In March 2022, the Department for Business, Energy and Industrial Strategy (BEIS) confirmed a total budget for UK Research and Innovation of £25.1 billion, for the three financial years from 2022–23 to 2024–25.[16] This is a 14% increase from the 2021–22 budget.[17] This spending growth is coupled with the Government's £800 million investment in the new Advanced Research and Invention Agency (ARIA) in the spring of 2021,[18] which aimed to "complement the work of UK Research and Innovation (UKRI) while building on the Government's ambitious R&D roadmap",[19] noted above.

The effect of Brexit on the legal approach to AI

Similarly to the UK, Europe's strategy is to become the most attractive, secure and dynamic data-agile economy worldwide. Consequently, in 2020, the European Commission (the EC) proposed a new legal framework relating to the development and use of "high-risk" AI that focuses on human and ethical implications.[20] Following public consultation, the EC presented a legislative proposal on AI on 21 April 2021, and on 6 December 2022, the EU Regulation on Artificial Intelligence (AI Act) progressed one step further towards becoming law when the Council of the EU adopted its amendments to the draft Act, concluding months of internal Council negotiations.[21] Compared to the European Commission's proposal, the Council's approach includes narrowing the definition of "AI" to systems developed through machine learning approaches and logic and knowledge-based approaches, in order to distinguish AI from simple software systems.[22] These legislative changes in the EU have also been followed by a draft proposal for an AI liability directive aimed at "laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems".[23] The EU has also progressed with the proposed Data Act, which aims to open opportunities for data-driven innovation, such as machine learning technologies, and to give consumers and companies more control over what can be done with their data, clarifying who can access data and on what terms.

As further discussed below, it has become apparent that UK policymakers will not follow the EU approach and legislate AI.

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 true leading role to play, however, is in developing policy, regulation and standards that can become internationally renowned and implemented, in much the same way that English law is used in many private international transactions. The British Standards Institution (BSI), 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".[24]

Regulatory landscape

The responsibility for AI policy and driving growth across the economy is divided between the Department for Digital, Culture, Media & Sport (DCMS) and BEIS. The responsibility for uptake across Government lies with the Government Digital Service (the GDS), which reports to the Minister for Implementation in the Cabinet Office.

Organisations

Over the last few years, the Government has set up various organisations to facilitate the conversation around AI technology adoption:

1. The AI Council is a non-statutory expert committee. It comprises independent members from either industry, the public sector or academia (such as Mastercard, the University of Cambridge and The Alan Turing Institute). Members do not represent their organisations on the committee and do not in any way affiliate their business with the committee. The purpose of the AI Council is to "put the UK at the forefront of artificial intelligence and data revolution".[25]
2. The Government Office for AI is part of DCMS and BEIS. The Office for AI works with industry, academia and the non-profit sector and is responsible for overseeing the implementation of AI.[26]
3. The Centre for Data Ethics and Innovation (the CDEI) forms part of DCMS. The CDEI serves as "a connector between Government and wider society".[27] It is an advisory body that advises the Government on potential measures to develop the governance regime for data-driven technologies.
4. The ARIA is a new independent research body that will focus on projects with the potential to produce transformative technological change with a strategy of "high risk, high reward". It will focus on *how* research is funded, rather than focusing on a specific industry or technology, and will fall within BEIS.[28] The Advanced Research and Invention Agency Bill was passed on 15 February 2022 and given Royal Assent on 24 February 2022, effecting the creation of ARIA.[29]

AI and the Information Commissioner's Office (ICO)

The ICO is the UK's information rights regulator. AI is one of its stated priorities and it believes that existing privacy legislation is able to accommodate it.[30] It has also worked to help organisations manage AI risk.

In March 2021, the ICO launched a consultation on the alpha version of its AI and data protection risk mitigation and management toolkit, which is designed to reflect the ICO's internal AI auditing framework and its AI and data protection guidance.[31] A further consultation took place later in 2021, to gather feedback on the beta version.[32] Following this feedback, the ICO launched its AI and Data Protection Risk Toolkit v1.0 in May 2022, to provide practical guidance to organisations for the assessment of AI-related data protection risks. The Toolkit is a document that breaks down risk areas (ranked as 'high', 'medium', 'low' and 'non-applicable') that may be caused by a business's own AI systems and suggests practical steps for controlling and mitigating such risks. By undertaking the practical steps suggested in line with what is expected under the legislation, risks to fundamental rights and freedoms are reduced and business compliance with data protection law becomes more likely.[33]

Further, the Data Protection and Digital Information Bill was laid before the UK Parliament on 18 July 2022. This bill seeks to reduce burdens on businesses and includes measures on the responsible use of AI, while maintaining the UK's high data protection standards.[34]

The bill's passage through the legislative process was paused in September 2022, to allow for further consideration. This was due to change in the UK's governmental leadership.[35]

AI strategy

The Government published the National AI Strategy (Strategy) in September 2021, setting out how it will seek to utilise and implement AI over the next 10 years, in both the public and private sectors. The Strategy is built upon three pillars:

- the key drivers of advances in AI are hugely competitive and include access to people, data, computers and finance;
- AI will become mainstream; and
- regulatory and governance systems must adapt and keep up with the pace of change.

As part of the Strategy, the Government has identified key actions to be taken under each pillar in the short (three months from publication), medium (six months from publication) and long (12 months from publication and beyond) terms.

Under the first pillar, the Strategy focuses on upskilling workforces and attracting top talent in this area and collaborating internationally on research and innovation. The Strategy also aims to support the development of AI in the UK by recognising the important role that private financing – such as venture capital – plays in this regard, noting that, in 2020, UK firms that were adopting or creating AI-based technologies received £1.78 billion in funding, which is more than triple the amount raised by French companies.[36]

The second pillar turns to the importance of creating and protecting IP in AI and using AI for the public benefit, ensuring that AI supports the Government's ambition of bolstering a "strategic advantage" in science and technology, making the UK a "science superpower" and achieving its net-zero targets.

The third pillar focuses on AI governance, domestically and internationally, with an aim to build public trust and confidence in the increased use of AI through establishing a comprehensive governance framework that addresses the risks (and how to reduce them) and opportunities that AI brings to individuals and society. The Strategy admits that the existing technology rules and norms are not necessarily appropriate for modern AI. The Strategy notes that, having embraced a strong sector-based approach since 2018, now is the time to decide whether there is a case for greater cross-cutting AI regulation or greater consistency across regulated sectors. Inconsistent approaches or a narrow framing of AI regulation across sectors could introduce contradictory compliance requirements and uncertainty around responsibility. Consequently, the Government intended to work with the Office for AI to develop a national position on developing and regulating AI, to be set out in a White Paper that was expected in early 2022 (but is yet to be published at the time of writing).

Overall, the Strategy hopes to achieve in the UK:

- growth in the number and type of discoveries made using AI;
- economic and productivity growth due to AI; and
- the most trusted and pro-innovation system for AI governance in the world.[37]

The Strategy: current progress

The Government has made progress against their actions under each pillar. For example, all the short-term actions under pillar one have been delivered. This has included publishing a framework on the Government's role in enabling better data availability in the wider economy,[38] launching a consultation on the role and options for a National Cyber-Physical Infrastructure Framework (which closed in May 2022)[39] and work to support the development of AI, data science and digital skills through the Department for Education's Skills Bootcamps (with an

announcement made on 10 February 2022).[40] Across pillars two and three, almost all the short-term actions have also been delivered.

With the Strategy now having been published around 18 months ago (at the time of writing), the Government has made steady progress on the mid- and long-term Strategy objectives across all three pillars, with almost all mid-term objectives realised. However, some long-term objectives require further development, which is understandable and to be expected, given the ever-changing AI landscape.

Regarding the first pillar, in 2022, the Government clearly focused its investment into upskilling and encouraging people from different backgrounds, industries and jurisdictions to enter the AI workspace by providing various incentives, such as scholarships, additional funding for AI research and visa opportunities. It has also made significant headway in investing in AI capability across various sectors (such as transport, defence and health).

A key long-term goal of pillars one and two that remains to be realised is the launch of the National Research and Innovation Programme, which is intended to align funding programmes across UKRI and support the wider UK AI ecosystem.

A key action under pillar three is the introduction of an "AI Standards Hub" (the Hub). The Hub aims to place the UK at the heart of shaping and developing global AI standards. This approach begins to show the differences between the UK and EU post-Brexit, as the EU seeks to continue to take a risk-based approach.

The Hub launched in October 2022 and is led by The Alan Turing Institute, the UK's national institute for AI and data science, in partnership with the BSI and the National Physical Laboratory.[41] Since its launch, the Hub has formed a database of over 300 AI-related standards that are being developed or have been published by a range of prominent Standards Development Organisations. For example, process and management standards are being adapted for the AI context to set out repeatable guidance, for activities such as risk-management processes or transparency reporting.[42] A long-term goal under pillar three is also the "development of an AI technical standards engagement toolkit to support the AI ecosystem to engage in the global AI standardisation landscape".[43] This global standards framework has not yet been realised but will ultimately be delivered by the Hub.

A further key medium-term goal under pillar three is the production of a White Paper that is intended to set out the Government's position on possible risks and harms posed by AI technologies, and how these risks and harms can be mitigated through regulation, specifically whether there should be sector-specific regulators for the UK AI landscape. In light of this, on 18 July 2022, the UK Government published a policy paper titled "Establishing a pro-innovation approach to regulating AI" (the Paper).[44]

The Paper is intended to be an interim publication to the White Paper, setting out details on scope, the Government's regulatory approach, key principles, and next steps. Instead of giving responsibility for AI governance to a central national regulatory body, as the EU is planning to do through its draft AI Act, the Government's proposals will allow different regulators to take a tailored approach to the use of AI in a range of settings. The regulatory approach will be underpinned by a set of overarching principles, such as safe usage of AI, technical security, transparency, accountability, avenues for redress, and fairness. It is expected that the White Paper will provide further clarity and detail on the Government's approach, in particular how it will balance the need for coherent regulatory coordination, while also promoting sectoral flexibility and encouraging innovation. Ultimately, however, the Paper lacks detail on how the proposed AI framework will work in practice, and how the Government will put its approach into practice, and what specific changes will need

to be made in order for it to do so. The Paper re-emphasises the priority on growth and innovation as the two cornerstones of AI regulation in the UK. This continues to be in contrast to the draft EU AI Act, which is more risk-based.

Intellectual property and AI

Patentability of inventions created by computers

Recently, 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 that patent protection is unavailable. However, there is ongoing debate on this, including a consultation led by the World Intellectual Property Organization (WIPO) and a consultation led by the UK Intellectual Property Office (the UK IPO). In December 2019, the UK IPO found that DABUS is not a person and so cannot be considered an inventor of a patent; DABUS is an AI machine. In September 2020, the situation was confirmed by the High Court. The High Court accepted the indication that DABUS is an inventor at face value, and did not argue that AI technology is only a tool that is incapable of independently creating an invention. The High Court found that even if DABUS was 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 High Court decision is useful because it clearly sets out legal and ethical arguments concerning the nature of personhood and creative agency. The UK Court of Appeal confirmed, on 21 September 2021, that inventors must be human beings. However, Birss LJ offered a dissenting view regarding the correct way to process patent applications through the UK IPO. Birss LJ found that Dr Thaler (the applicant) had named whom he believed the inventor to be and so the UK IPO had been wrong to find the statement of inventorship invalid and, as a consequence, treat the applications as withdrawn. In contrast, Arnold LJ and Laing LJ found it correct for the DABUS applications to be deemed withdrawn, due to not listing a human on the statement of inventorship form. The UK IPO 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. An "AI Inventor" is not acceptable as the term does not identify "a person", the only type of entity to which "intentorship" can, in a legal context, be attributed. The consequence of failing to supply a correct statement of inventorship is that the application is taken to be withdrawn under section 13(2). An appeal has been filed in the Supreme Court with a hearing date of 2 March 2023. The Chartered Institute of Patent Attorneys (CIPA) has intervened in support of the applicant during the permission to appeal stage. The CIPA, in their intervention during the permission to appeal stage, submitted that all the Act requires is that an applicant states their belief as to who the inventor is and how the applicant derives their rights, in alignment with the case being considered. It was submitted that it remains open to a third party to contest the mention of an inventor with correction of the mention, and open to a third party who believes they have a right to grant of the patent to contest this matter. Additionally, the CIPA submitted that the decision to refuse the appeal would introduce a new, non-statutory ground for refusing patent applications, and is in direct conflict with the drafting intent of the Act, alongside being contrary to the policy objective of providing a stimulus for innovation. The outcome of the appeal is not yet available.

The results of a UK IPO consultation on AI and intellectual property (IP) were published in March 2021 and led to enhanced UK IPO guidelines on patent exclusion practice for AI inventions. The guidelines, released in September 2022, set out the legal framework

for examining applications for or using AI and how this will be applied. The guidelines are accompanied by a set of scenarios, each with a draft independent claim, and explain how the IPO would apply the guidance. The guidelines also contain information about how sufficiency will be assessed by the IPO for inventions involving AI, such as machine-learning technology trained using novel data sets.

The UK IPO launched a follow-up consultation, "Artificial Intelligence and IP: copyright and patents", which closed in early January 2022. The consultation proposed three options regarding whether and how to change the law in the UK regarding AI systems as inventors and sought views on the following three options:

- Option zero: make no legal change.
- Option one: expand the definition of inventor to include humans responsible for an AI system that devises inventions.
- Option two: allow patent applications to identify AI systems as inventors.

The CIPA responded that option zero is acceptable for the time being – subject to the qualification that the UK IPO actively engages with other jurisdictions to develop a harmonised approach relating to AI and patents. The consultation outcome[45] was a decision to proceed with option zero for the time being. The consultation outcome promised a new copyright and database rights exception for text and data mining. However, more recently, that proposal has been dropped after generative AI tools became widely available in 2022.

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 such a 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 website and includes the following positive comment from the UK IPO welcoming "further exploration of how additional protection for data as a right could incentivise the AI industry". On the other hand, the UK's CIPA stated 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 sufficient.

While it is the case that existing IP 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. It is also not clear how such a right would apply to synthetic data, which is often used in AI technology. Synthetic data comprises data that is independently generated but which duplicates patterns or properties of existing data needed for machine learning. It is interesting to note that the outcome of the recent UK IPO consultation on AI and IP does not appear to have any explicit mention of a new *sui generis* right for data, suggesting that the idea has not flourished. Indeed, the UK IPO follow-up consultation, which closed in January 2022, did not have an explicit mention of the idea.

Trademarks

The recent UK IPO consultation on AI and IP has a dedicated section regarding trademarks and infringement. It is pointed out that "many of the traditional concepts relating to trademark infringement are founded on human interaction with banding and human

involvement in the purchasing process". It is acknowledged that current AI technology, such as recommender systems, are able to learn the preferences of individuals and generate purchasing suggestions. Eventually, AI technology may become a purchaser of products and, as a result, there could be difficulties applying existing legal concepts – such as "average consumer" – when assessing whether there is a likelihood of confusion. The outcome of the consultation suggests that it will be left for the courts to interpret how to apply the existing law when considering who is held liable for trademark infringement (examples of entities that may be liable are listed as "the owner, the operator, the programmer, the trainer, the provider of training data, or some other party"). There is a statement suggesting that the language in section 10 of the Trademarks Act, which references "a person", will be reassessed in terms of its appropriateness.

Copyright, designs and trade secrets

There are dedicated sections in the outcome of the UK IPO consultation on each of copyright, designs and trade secrets. The explicit actions set out for these sections generally relate to further consultations, engaging with like-minded nations and multilateral organisations, holding university-led seminars and conducting research. There is an action for the UK IPO to use AI tools as part of the services it provides, such as the recently launched pre-apply service for trademarks.

The UK IPO consultation "Artificial Intelligence and IP: copyright and patents", which closed in early January 2022, sought views on copyright protection for computer-generated works without a human author. Opinions were sought as to whether these works, which are currently protected in the UK for 50 years, should be protected at all, and if so, how. Licensing or exceptions to copyright for text and data mining for machine learning are other areas where opinions were sought in the consultation.

Healthcare and AI

While the use of AI and the significant opportunities and benefits it offers patients and clinicians are largely welcomed, it has yet to transform the UK healthcare system. That said, the National Health Service (NHS) is taking a commendably realistic approach in an environment traditionally resistant to change.[46] The CDEI recently reported on how AI was prevalent not only in the healthcare system combatting the COVID-19 pandemic, but also for maintaining essential public services.[47]

Examples of AI can be found throughout the healthcare ecosystem in the UK, with its application becoming more prevalent:

- **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. The same collaboration now has a second, entirely AI created molecule in clinical trials,[48] with other companies also producing partially and wholly AI generated medicinal molecules in addition.
- **Drug repurposing** – during the COVID-19 pandemic, Remdesivir (a medication originally developed to treat Hepatitis C) was discovered to be an effective treatment for the COVID-19 virus thanks to AI screening methods. The speed at which AI can screen pre-approved medications can bring known medications to patients much faster and with less cost than that of developing new drugs.[49]
- **Efficient detection, diagnosis and decision making** – at Moorfields Eye Hospital, Google 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.[50] Addenbrooke's Hospital uses Microsoft's InnerEye system to mark up scans to assist radiology treatment for cancer patients, drastically reducing wait times by up to 90%.[51]

- **Robot-assisted surgery** – intuitive da Vinci platforms, now boosted by AI and machine learning insites, have pioneered the robotic surgery industry, featuring cameras, robotic arms and surgical tools to aide in minimally invasive procedures and act in tandem with healthcare proffesionals.[52]

AI in healthcare promises a new era of productivity in the UK where human ingenuity is enhanced by speed and precision. We understand that AI will play a crucial role in the future of the NHS,[53] and the data-rich nature of healthcare makes it an ideal candidate for its application across multiple disciplines. However, the sensitivities surrounding patient data raise crucial concerns about privacy, security and bias. These conflicts make the industry one of AI's most challenging domains of application, and for AI to truly thrive in the UK healthcare system, both the quality and scope of health data on which it is based need to be significantly improved. Public trust in data-driven interventions needs to be strengthened if they are to be sustainable post-pandemic recovery.

Financial services and AI

AI is pervasive in financial services. Since the industry relies on the production, assessment and manipulation of information, any tools that assist with these processes will be rapidly adopted.

In the UK, regulation of AI systems and software occurs at an industry level. This means that there is no directly applicable AI regulation to financial services and users are obliged to apply existing industry-specific rules to new technologies.

In determining the application of rules to AI used in financial services, the first step is to determine the location of the regulatory perimeter in relation to the relevant services. The primary regulation establishing this is contained in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001. Regulated activities, or those within the regulatory perimeter, are licensed and supervised by the Financial Conduct Authority (the FCA), the UK regulator for financial services.

The perimeter is relevant to AI service providers in multiple ways. For example, if they are simply service providers to financial services businesses, they will most likely wish to be categorised as technology businesses rather than financial services businesses themselves. This avoids them being subject to the costs of compliance with financial regulation. However, their customers are subject to this regulation and it is therefore important for these companies to be aware of and working in a context that takes account of the regulation.

The obligations relating to regulated activities fall into a number of conventional categories, comprising themes in the FCA Handbook and Prudential Regulatory Authority Handbook:

- **Responsibility** – the UK senior managers' regime requires senior employees at regulated firms to be accountable for activities in their firms, and this includes technology deployment. Therefore, is now necessary for holders of these positions to be able to evidence that, and how, they have appropriate governance control of AI systems and software.
- **Conduct** – financial regulation in the UK is principles-based. Those principles are intentionally broad and hence there is work to be done to apply those principles smartly in relation to AI, in ways that have regard to both inputs and outputs. The FCA Handbook principles include: paying regard to the interests of customers; paying regard to the information needs of clients; and taking care to ensure the suitability of

advice. At this stage, we have few cases to guide us. It is thus necessary to ensure that applications of AI are both tested and defensible against the principles in question.

- **Transparency** – the FCA, via its blogpost on AI transparency in financial services, recommends that a "transparency matrix" is produced and used by financial institutions to evidence that appropriate steps are taken in relation to AI usage within the business. This recommendation should cover, among others, the following issues: what AI is used in the business; how its use is procured; who is responsible for it at a policy level; who is responsible for it at a technical level; when and how it is used in customer-facing roles (and in consumer-facing roles); and how technical information about it is disseminated in ways that are understandable by all those with responsibility.
- **Risk management** – as with all new types of service, it is of vital importance to establish exactly what it is being contracted for. The novelty and potential lack of transparency in AI systems and software mean that the parties' potential liabilities and protections in contract and tort must be carefully addressed and managed. By definition, AI performs actions that operators do not specifically tell it to carry out. Therefore, the implications of this capacity to generate behaviours with some degree of independence must be tested. Standard software contracting forms will not be sufficient to handle all of these concerns.

  Since financial services is such a fertile area for AI, we have chosen it to illustrate our topic in Chapter 1, Practical Risk Management in AI: Auditing and Assurance by use cases in this industry.

Examples of AI can be found throughout the financial services industry in the UK:

- **Robo-advice** – this is a hard case because the financial position of consumers will be impacted by the operations of the AI. There are many providers of this service now, including Wealthsimple and Betterment. There is a regulatory distinction between providing information and giving advice, and robo-advisors are careful to understand their position.
- **Algorithmic trading** – many hedge funds say they use algorithms, including Two Sigma and Renaissance Technologies. Unlike robo-advisors, hedge funds applying algorithmic trading strategies do not have retail customers. In their case, the risks relate to the large sums at stake and questions of whether systemic risk can be introduced into markets by their operation. These questions are largely answered by reference to MiFID II and the FCA's rules on market conduct.
- **Anti-money laundering** – this is a case where financial institutions use technology to deliver services where they are their own customer. The relevant rules here are the Money Laundering Regulations that apply to all UK financial institutions. The FCA takes a "technology-neutral" approach to its regulation; in other words, regulations apply howsoever the regulated entity chooses to comply in practice. In this case, the entity must investigate its ability to evidence that AI has found and applied information that is reliable, accurate, sourced from third parties and sufficient in all circumstances.
- **Insurance products** – AI is widely used in the insurance industry, in use cases from customer service, to claims management, to pricing risk, and to identifying trigger events for policies. Relevant rules range from those relating to discrimination, to GDPR, to specific industry applications of common law rules on misrepresentation and implications of breach of conditions. In particular, insurance firms often use multiple AI systems alongside each other, thereby increasing the complexity of ensuring compliance.

Endnotes

1. UK tech sector retains #1 spot in Europe and #3 in world as sector resilience brings continued growth. Available at https://www.gov.uk/government/news/uk-tech-sector-retains-1-spot-in-europe-and-3-in-world-as-sector-resilience-brings-continued-growth.
2. *Ibid*.
3. *Ibid*.
4. *Ibid*.
5. *Ibid*.
6. *Ibid*.
7. AI Market Size to Reach USD 1394.30 Billion by 2029. Available at: https://www.globenewswire.com/en/news-release/2022/09/13/2514767/0/en/AI-Market-Size-to-Reach-USD-1394-30-Billion-by-2029.html#:~:text=13%2C%202022%20(GLOBE%20NEWSWIRE),in%20the%20next%20several%20years.
8. The next generation of tech ecosystems report. Available at: https://dealroom.co/reports/the-next-generation-of-tech-ecosystems-report.
9. https://www.legislation.gov.uk/ukdsi/2021/9780348226935/schedule/3.
10. Build Back Better: plan for growth. Available at: https://www.gov.uk/government/publications/build-back-better-our-plan-for-growth/build-back-better-our-plan-for-growth-html.
11. *Ibid*.
12. Advanced Research and Invention Agency (ARIA): policy statement. Available at: https://www.gov.uk/government/publications/advanced-research-and-invention-agency-aria-statement-of-policy-intent/advanced-research-and-invention-agency-aria-policy-statement.
13. https://www.gov.uk/government/publications/budget-2020-documents/budget-2020.
14. https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.
15. 2022/23–2024/25 budget allocation for UK Research and Innovation. Available at: https://www.ukri.org/wp-content/uploads/2022/05/UKRI-Budget-Allocations-2022-25_FINAL2.pdf.
16. *Ibid*.
17. *Ibid*.
18. https://www.gov.uk/government/publications/build-back-better-our-plan-for-growth/build-back-better-our-plan-for-growth-html.
19. ARIA: policy statement. Available at: https://www.gov.uk/government/publications/advanced-research-and-invention-agency-aria-statement-of-policy-intent/advanced-research-and-invention-agency-aria-policy-statement.
20. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
21. https://www.wsgr.com/en/insights/council-of-the-eu-proposes-amendments-to-draft-ai-act.html.
22. https://www.allenovery.com/en-gb/global/blogs/digital-hub/the-council-of-the-eu-adopts-an-approach-on-the-proposed-ai-regulation.
23. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.
24. https://www.bsigroup.com/en-GB/industries-and-sectors/artificial-intelligence/.
25. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836907/AI_Council_Terms_of_Reference.pdf.

26. https://www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/missions.
27. https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about.
28. https://www.gov.uk/government/publications/advanced-research-and-invention-agency-aria-statement-of-policy-intent/advanced-research-and-invention-agency-aria-policy-statement.
29. Advanced Research and Invention Agency Act 2022. Available at: https://bills.parliament.uk/bills/2836.
30. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.
31. https://hsfnotes.com/data/2021/11/17/ico-publishes-consultation-on-the-ai-and-data-protection-risk-toolkit/.
32. https://hsfnotes.com/data/2021/11/17/ico-publishes-consultation-on-the-ai-and-data-protection-risk-toolkit/.
33. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/.
34. UK Government sets out proposals for a new AI Rulebook. Available at: https://cms-lawnow.com/en/ealerts/2022/08/uk-government-sets-out-proposals-for-a-new-ai-rulebook#:~:text=It%20also%20comes%20as%20the,UK%27s%20high%20data%20protection%20standards.
35. The UK's Data Protection and Digital Information Bill – Further Reform on the Horizon. Available at: https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/11/the-uk-data-protection-and-digital-information-bill-further.html.
36. https://www.gov.uk/government/publications/government-response-to-the-house-of-lords-select-committee-on-artificial-intelligence/government-response-to-the-house-of-lords-select-committee-on-arti-cial-intelligence.
37. *Ibid*.
38. https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy.
39. https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation.
40. https://www.gov.uk/government/news/23-million-to-boost-skills-and-diversity-in-ai-jobs.
41. https://www.gov.uk/government/news/new-uk-initiative-to-shape-global-standards-for-artificial-intelligence.
42. https://aistandardshub.org/resource/main-training-page-example/2-different-types-of-standards/.
43. https://aistandardshub.org/the-national-ai-strategy/.
44. https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai.
45. https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/outcome/artificial-intelligence-and-intellectual-property-copyright-and-patents-government-response-to-consultation.
46. https://transform.england.nhs.uk/ai-lab/ai-lab-programmes/the-national-strategy-for-ai-in-health-and-social-care/.
47. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/968515/Local_government_use_of_data_during_the_pandemic.pdf.

48. https://investors.exscientia.ai/press-releases/press-release-details/2021/exscientia-announces-second-molecule-created-using-ai-from-sumitomo-dainippon-pharma-collaboration-to-enter-phase-1-clinical-trial/Default.aspx.
49. https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30192-8/fulltext.
50. https://www.moorfields.nhs.uk/content/latest-updates-deepmind-health.
51. https://www.cuh.nhs.uk/news/ai-speeds-cancer-treatment.
52. https://www.intuitive.com/en-us/about-us/newsroom/exploring-new-advancements-in-robotics.
53. *Ibid*, note 45.

* * *

Acknowledgment

The authors would like to thank Hannah Curtis (Partner, CMS) for her invaluable contribution to the preparation of this chapter.

Rachel Free
Tel: +44 20 7067 3286 / Email: rachel.free@cms-cmno.com
Rachel Free is a European and UK patent attorney with an M.Sc. in AI and a D.Phil. 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 an independent advisory board member of the University of Bath's Centre for Doctoral Training in Accountable, Responsible and Transparent AI.

Charles Kerrigan
Tel: +44 20 7067 3437 / Email: charles.kerrigan@cms-cmno.com
Charlie Kerrigan is a lawyer working in finance and emerging technology with specialisms in AI, crypto and DeFi. He is an Advisor to Cointelligence Fund; a Board Advisor to Holistic AI; an Advisory Board Member of the Investment Association's Engine; and an Advisory Board Member of the UK APPGs on AI and Blockchain. He is editor of *AI Law and Regulation* (Edward Elgar) and author of *The Financing of Intangible Assets*: *TMT Finance and Emerging Technologies* (Butterworths, 2019).

Barbara Zapisetskaya
Tel: +44 20 7367 2543 / Email: barbara.zapisetskaya@cms-cmno.com
Barbara Zapisetskaya is a senior associate in the Technology & Media Team. She has a particular interest in the regulation of AI and is a regular contributor on this topic. Barbara's experience lies in the areas of commercial and technology law. She has been advising clients on a variety of commercial matters, including the 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: www.cms.law

USA

Sean D. Christy & Chuck Hollis
Norton Rose Fulbright US LLP

Trends

The usage and adoption of artificial intelligence ("AI") (which we refer to broadly herein to also include the application of AI to analytics of large data sets ("Big Data") and in the context of machine learning ("ML") (which includes the subsets of ML operations and deep learning)) has increased significantly over the past few years. However, in the past 12 months, AI has gone from a topic of conversation in relevant business and academic circles to regular dinner table conversation, with AI being profiled in some form in nearly every news cycle and dominating the social media feeds of nearly everyone in the professional world.

Generative AI models like ChatGPT have been a big part of normalising AI as part of the day-to-day vernacular, with useful application and adoption in almost every knowledge-worker context and by educators and students alike. At the same time, global investment in AI fell from 2021 to 2022, but still outpaces 2020 spend by a margin consistent with prior years' growth.[1] Even so, the private industry is now far outpacing academia in the development of AI models, and it is expected that government investment in AI will continue to increase, with the US government allocating $1.7 billion (a 13% year-over-year increase) to AI research in 2022.[2]

With increased adoption and media coverage, some of the risks and downsides of AI continue to garner attention. The environmental costs of AI can be high – for example, the CO^2 emissions from training ChatGPT are estimated to be 500 times that of a single passenger flight from New York to San Francisco.[3] The societal costs can be high as well, with incidences of AI misuse and bias increasing significantly, likely due to the increased social awareness of AI in the first instance and to the biases inherent in the data sets that are used to train generative AI in the second. These and other potential adverse consequences inform our clients' approach to AI policies and procedures.

At the same time, AI can be used for environmental benefit (e.g., to optimise almost any system to reduce energy consumption), and industry experts are finding ways to combat bias with techniques like instruction tuning.[4] While biased AI data sets receive a fair amount of bad press, AI is proven to reduce the cost (and by natural extension, the societal impact) of data breaches.[5] These benefits are driving adoption of AI among our clients.

With the increase in adoption also comes additional marketplace competition. That competition benefits purchasers of AI by providing many more options for vendors with whom to partner. However, the more crowded market also puts more pressure on the vendor selection and due diligence process, especially in view of certain risks inherent in the usage and deployment of AI, as discussed in more detail below. For that reason, we have seen

a shift in the contracting process for AI technology and the M&A due diligence process for AI-related M&A from less focused, more commoditised treatment, to more strategic treatment with a heavier focus on risk mitigation in both regulated and unregulated sectors.

While as recently as last year's publication, we and other commentators were stating that technology is outpacing the law, the law is starting to catch up, with a significant increase in interest and activity at the US federal level and the passage of several US state laws and local municipal ordinances related to the use and governance of AI, as covered in more detail below.

Ownership/protection

Patent applications related to AI themes have continued to lead other areas throughout 2022 and into 2023.[6] From Q3 2018 to Q3 2022, the average annual growth rate for AI-themed patent applications was 29%, substantially outpacing other areas.[7] In its Q1 2022 report, GlobalData noted the increase in AI applications was "primarily owing to the rise in the invention of machine learning (ML) models, speech recognition, image analysis, and natural language processing systems" and that IBM led in filings in AI this quarter with a focus on ML models, natural-language-processing algorithms and neural-network fingerprint-verification technologies.[8] Interestingly, patent application filings provide insights into potential disruptions in emerging and accelerating technologies, with humanoid robots, generic algorithms and intelligent embedded systems noted as emerging technologies and remote health assessment, emotion AI and AI-assisted clinic trials as some of the accelerating technologies.[9]

The United States Patent & Trademark Office has recently recognised the importance of protecting AI inventions and launched its AI/ET Partnership with the "goal to foster and protect innovation in Artificial Intelligence (AI) and Emerging Technologies (ET) and bring those innovations to impact to enhance [the US's] economic prosperity and national security and to solve world problems".[10]

When considering intellectual property ("IP") protection and infringement risk for AI, we can break each AI solution into three primary areas – the AI itself and its application, the data that is used to train the AI, and the output from the AI – and each may be subject to one or more of patent, copyright and/or trade secret protection. In addition to these three general areas, there may be other processes specific to the AI workflow that may be patentable in and of themselves. For example, training and data cleansing/organisational processing for training purposes may be patentable. Also, the overall application of the AI solution should be considered for patentability.

For the AI itself, patent protection is one of the leading means and strategies for IP protection. Of course, to obtain patent protection for the AI or its functional application, the AI must meet the requirements and thresholds for patentability (including those focused on the patentability of computer- and software-related inventions). Because the AI is typically expressed in software or code, protection under copyright law may be available as well. Finally, if the disclosure of the AI is suitably limited, and certain other thresholds are maintained, the AI may be protected by the various state trade secret laws in the US.

In many instances, the data that is used to train the AI may be protected by copyright laws. Accordingly, the ability to use (copy) copyrighted data to train an AI without infringing the copyright of the underlying data is a relevant, fact-based question that must be considered. The use of copyrighted data may be permissible under "fair use" standards, but that theory is being challenged on many fronts. For example, a class action lawsuit filed in California

in November 2022 is challenging GitHub Copilot, which assists in writing computer code; and Getty Images filed a lawsuit in the US in early 2023, following an earlier announcement in the UK, against Stability AI and Stable Diffusion contesting the appropriate use of images used to train the AI. To counter these issues related to the use of "questionable" training data, there are groups forming that are working on responsible training of large language models for coding applications (e.g., https://www.bigcode-project.org/).

The extent to which the result or output of the AI is protectable, in many cases, will depend on the type of output provided. For example, if the AI generates a fraud score or decision on a financial transaction, the output (e.g., flagged for fraud or no fraud) may not be protectable under patent or copyright laws, but may be protectable as a trade secret and, in any event, can be made subject to contractual confidentiality protections. If, on the other hand, the output of the AI is the generation of software code, the code may be protectable under copyright law, but copyright protection for an AI-generated work requires more careful inquiry. In March 2023, the US Copyright Office issued a statement of policy to clarify its practices for examining and registering works that contain material generated by the use of AI technology.[11] In general, there must be some creative contribution from a human for the work to be copyrightable. The Copyright Office did note that a work generated by AI may be copyrightable if the work contains enough human authorship. In such cases, the copyright will only protect the human-authored aspects of the work, but not the AI-generated portions. Whether there is enough human authorship to warrant copyright protection will have to be determined on a case-by-case basis.

Similar to the issue of copyright protection for AI-generated materials, the Federal Circuit has held that an AI system may not be an inventor and is not an "individual" for purposes of patent protection.[12] However, the court left open the question of whether inventions made by humans with the assistance of AI tools could be patentable.

Ultimately, the strategy and methods for protecting an AI solution will require a review and analysis of the AI solution – in total – considering the technological advances made and the underlying data used. Further, to the extent the AI is developed or provided under contract, the contract should be clear as to how IP ownership is allocated or reserved in each of the areas discussed above and should address infringement risk.

Moving from protection to defensive measures, one of the byproducts of the increase in patent applications for AI is the need for companies to monitor and assess the patent application landscape from both a freedom to operate perspective for infringement avoidance and to ensure that the USPTO is issuing patents that are specifically focused on the particular inventions and are not overly broad. This review and "defensive" posture should be part of any AI IP protection and risk mitigation strategy.

Antitrust/competition laws

Another risk associated with AI is that the usage of AI algorithms and the amalgamation of data in certain ways or for certain purposes could run afoul of US federal and state antitrust laws. The use case that has perhaps garnered the most attention and warrants close scrutiny is the usage of AI to directly or indirectly fix pricing amongst competitors, with the combination of ML and Big Data making it possible for competitors to fix pricing without obvious collusion. The amalgamation of data sets through data sharing arrangements or through M&A activity, and the resultant usage of Big Data, may also result in usage that frustrates competition in violation of applicable antitrust law. Much like the potential (and in some cases actual) resultant discriminatory and biased results of the usage of AI described

in more detail below, these antitrust considerations are not novel in and of themselves inasmuch as they mirror behaviour that has existed in other contexts, albeit behaviour that with AI is carried out by machines and algorithms. Regardless, the same legal principles apply, as do the steps that companies can undertake to mitigate risk, from the board of directors down to operations.

The Department of Justice ("DOJ") and the Federal Trade Commission ("FTC"), the agencies charged with enforcing US federal antitrust laws, have taken notice, with Jonathan Kanter, the antitrust chief of the DOJ, noting during a recent speech at South by Southwest in March 2023, that the agency views AI as tools that warrant DOJ regulatory scrutiny and is paying close attention to their use; and Lina Kahn, the chair of the FTC, recently published a guest essay in the *New York Times* in which she indicates that the FTC will not make the same mistakes it made with what she refers to as Web 2.0 and will be more proactive in regulating AI.[13]

Board of directors/governance

As discussed elsewhere in this chapter, AI is a powerful tool that will advance our lives, the economy and our communities – when developed and implemented appropriately – but can present significant risks when not property developed, implemented and monitored. A company's board of directors has a responsibility to manage and mitigate the risks of AI, both to the company and to its shareholders.

From a corporate law perspective, directors of companies have a fiduciary duty to their shareholders (or constituents for non-profits). At a high-level, these duties primarily include the duty of care and the duty of loyalty. In exercising these duties, among other requirements and obligations, a director is required to make decisions that are in the company's interest after reasonable diligence. Satisfying this standard in essence requires directors to ask questions, gather information, make decisions and monitor systems and processes to mitigate risk to the company. Because the implementation of AI tools and solutions will inevitably introduce risk and liability to the company, directors must be active in the management and oversight of AI solutions and to do so, must understand the inherent risks presented by AI and how those risks and issues make their way into the AI solutions.

At a minimum, boards should implement an AI governance plan. The plan should be designed to monitor the full AI lifecycle in order to identify and mitigate risks attendant to the design and implementation of AI solutions. However, like any plan, it needs to be designed in a manner that manages the compliance risk to the company, but at the same time is practical relative to the type of AI solution being deployed. In today's market, where ESG issues are top of mind for both companies and their investors, the AI governance plan must also be integrated with the company's ESG plan and structured so that the governance of AI mitigates ESG risk to the company and also ensures good corporate stewardship by the company. Microsoft's responsible AI framework has gained an industry following as an exemplary framework, with underpinning principles of fairness, inclusiveness, transparency, reliability and safety, privacy and security and accountability.[14]

Key components of an AI governance plan include the governance framework itself and also a responsible C-suite level owner of the plan, defined and periodic testing and auditing throughout the AI deployment and utilisation lifecycle, documentation of relevant findings, implementing mitigating controls and remediation of adverse findings.[15]

Boards of directors must also consider AI-risk in transactions that require board review, including material AI technology licences or developments and mergers with and acquisitions of companies that have implemented and deployed AI solutions.

Regulations/government intervention

In general, and not unlike other historical technological advancements, AI technology has outpaced the legal and regulatory landscape. However, in recent years, the US federal and state law and policymakers have been making strides to close those gaps, and in the past year, those strides have noticeably increased.

Perhaps the most developed and well-known area of the law that touches on the Big Data components of AI are the various US federal and state privacy laws that govern the collection, usage and protection of personal data. This is an area of law that is undergoing rapid change in the US, with the most attention over the past year being given to the CCPA/CPRA in California and to the Colorado Privacy Act, Connecticut Data Privacy Act, Iowa Consumer Data Protection Act, and Virginia Consumer Data Protection Act, all of which in varying degrees bring to the US protections that, while not entirely consistent, provide for a right against automated decision-making. At the US federal level, in 2022 the proposed American Data Privacy and Protection Act ("ADPPA") successfully exited committee and was the closest the US has come to passing a comprehensive consumer data privacy law. While the ADPPA did not pass, it remains to be seen whether there will be a federal consumer data privacy law in 2023.

Aside from data privacy, concerns over the misuse or unintended consequences of AI, and the benefits and consequences of its use, have prompted US state legislatures to study the impact of AI on their constituents. In 2022, excluding laws related to facial recognition and autonomous vehicles, at least 30 states and territories introduced bills or regulations related to AI, with laws being enacted in four states.[16] Many of these state laws and their resultant regulations focus on the study and impact of AI, while others are directed at preventing, or at least outlawing, the use and implementation of AI with discriminatory impacts.[17]

In addition to the state level, cities and other local municipalities have been active in addressing and implementing restrictions on the use of certain AI tools in the hiring and promotion process. More specifically, Local Law 144 in New York City prohibits employers from using any automated employment-decisions tools for recruiting, hiring or promotion, unless those tools have first been audited for bias.

While the federal government has not passed any legislation governing the use of AI, it is on the radar of the White House, where action is being taken through the means available to the executive branch. In October 2022, the White House released a document titled "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People". While this Blueprint does not have the effect of law, it does provide guidance for agency rulemaking and potential legislation. Since the release of the AI Bill of Rights, the White House has taken a number of other steps through the executive branch related to the governance of AI and executing against the Blueprint ("Blueprint Actions"), including, by way of example, the Department of Labor ("DOL") efforts to protect worker rights, the Equal Employment Opportunity Commission ("EEOC") and DOJ efforts to protect workers with disabilities and to promote equal employment opportunities, FTC rulemaking related to privacy and discrimination, the Consumer Financial Protection Bureau ("CFPB") guidance regarding disclosure of algorithmic decision-making in creditworthiness determinations, the Department of Health and Human Services ("DHHS") rulemaking related to discrimination in healthcare, the establishment of the National Institute of Standards and Technology's AI Risk Management Framework and partnering with the private industry to evaluate predominant generative AI platforms against the principles set forth in the AI Bill of Rights.[18]

Companies implementing or acquiring AI solutions will have to monitor and react to the changing regulatory and legal environment, as this area of law continues to evolve to catch up with technology.

Civil liability

In the US, civil liability arising from the usage of AI would arise from the context, field and industry of usage rather than merely as a result of the usage of the AI itself. For example:

- usage of AI in consumer products might give rise to product liability claims;
- usage of AI in financial and other consumer services may give rise to liability under federal and state financial services and consumer protection laws and regulations;
- usage of Big Data may give rise to liability for fines and penalties and private rights of actions under various US federal and state privacy laws;
- usage of AI in healthcare and legal services may give rise to liability under theories of malpractice; and
- usage of AI in the employment context may give rise to liability under various federal and state civil rights and employment laws.

Discrimination and bias

Discrimination and bias of AI continues to be a topic of concern as companies and regulators continue to work to address these issues. The Harvard Law School Forum on Corporate Governance suggests that we are at a "critical moment for companies to take proactive mitigation measures to avoid harmful biases from becoming discriminatory practices that are the subject of litigation and front page stories in the Wall Street Journal".[19]

Bias can be introduced into AI at varying stages of its development (through coding and also through ingestion of biased data sets), resulting in biased and/or discriminatory outputs depending on the AI application and functionality. Companies are leveraging developments in technology and training techniques to combat those biases, using techniques such as instruction tuning and being more mindful about the data sets that are used to train AI.

The regulators, too, are continuing to leverage existing laws on the books to adapt and address discrimination and bias in AI, and the White House has catalysed those efforts with its Blueprint Actions:[20]

- The FTC stated in its Business Blog in April 2021 that it has decades of experience enforcing three specific laws against developers and users of AI: (i) Section 5 of the FTC Act, which prohibits unfair and deceptive practices; (ii) the Fair Credit Reporting Act, which may be applicable if the AI is used to deny people employment, housing, credit, insurance or other benefits; and (iii) the Equal Credit Opportunity Act, which makes it illegal to use a specific AI that results in credit discrimination on the basis of a protected class.[21] As noted above, the chair of the FTC has stated publicly that the agency intends to more proactively regulate AI, and the White House announced actions include FTC rulemaking to curb algorithmic discrimination.
- The Fair Housing Act ("FHA") prohibits housing-related discrimination on the basis of race, colour, religion, sex, disability, familial status and national origin. The Blueprint Actions include DHHS rulemaking to address algorithms used for tenant screening that may violate the FHA.
- AI is also prevalent in the workplace and is being used by companies in the hiring process to screen and evaluate candidates and in other employment decisions. This usage has created interest from the EEOC, which seeks to ensure that the AI used

in these decisions complies with US federal civil rights laws. The Blueprint Actions include technical assistance and guidance promulgated by the EEOC and the DOL related to the Americans with Disabilities Act considerations in employment algorithms and the initiation of a multi-year joint EEOC and DOL effort to rethink hiring and recruitment practices, including in automated systems.

- The CFPB is leveraging the Consumer Financial Protection Act to address algorithmic discrimination in the financial sector and, as noted above, is requiring disclosure of algorithmic decision-making in creditworthiness determinations.
- The Department of Education is making recommendations regarding the use of AI in education, including specifications for fairness in AI models used for education.
- The DHHS has proposed rules and guidance to prohibit discrimination in algorithmic clinical determinations, and to reduce algorithmic discrimination in other healthcare algorithms and has sought input through the rulemaking process regarding how Medicare policy can be used to reduce bias in algorithms and predictive modelling.

Some states and other jurisdictions have also passed laws that are directly applicable to the use of AI in employment decisions. For example, New York City, in a law that took effect on January 2, 2023, has banned the use of automated employment decision tools unless the technology has undergone a bias audit within the past year. The companies using these tools will also be required to notify the candidates that the tool was used in the employment decisions. Illinois also passed a law in 2019 that applies to AI when video interviews are used.[22]

As fairness continues to be a guiding principle for the ethical development and deployment of AI, companies developing and using AI will need to continue to monitor this everchanging regulatory landscape so that those efforts can be adapted and executed in a way that maintains compliance.

Conclusion

Where that leaves us as legal practitioners in the AI space is in an exciting time where the needs from our clients for AI advice continue to expand into new areas and increase rapidly in frequency, including as it pertains to the development of board and corporate policies regarding the responsible usage and adoption of AI; regulatory monitoring and compliance; technology transactions for the acquisition and/or development of AI; counselling on AI development strategies (including IP, ethical practices and commercialisation); advising on data privacy and security considerations attendant to the usage of AI; conducting privacy impact assessments on data processes that involve the use of Big Data; conducting training data assessments for potential bias exposure and freedom of use; advising on the potential antitrust implications of the usage of AI and particularly Big Data; and other areas. We expect that the pace of change in this area of practice and the law will only continue, as technical capabilities and adoption continue to accelerate at an ever-increasing pace.

* * *

Endnotes

1. Tekla S. Perry, *10 Graphs That Sum Up the State of AI in 2023, The AI Index tracks breakthroughs, GPT training costs, misuse, funding, and more,* IEEE Spectrum (April 4, 2023) https://spectrum.ieee.org/state-of-ai-2023.
2. Nestor Maslej, Loredana Fattorini, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Vanessa Parli,

Yoav Shoham, Russell Wald, Jack Clark, and Raymond Perrault, "The AI Index 2023 Annual Report", AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2023; Perry *supra* Note i.

3. Perry *supra* Note i.
4. Maslej *supra* Note ii.
5. IBM Security, *Cost of a Data Breach Report 2022*, July 2021 at 5, https://www.ibm.com/resources/cost-data-breach-report-2022 (follow "Get the Report" hyperlink; then insert contact information; then follow "Register for Report" hyperlink).
6. GlobalData, *Patent Statistics and Analysis Q1 2022* (Report Code GDDT-PL-M101), *Patent Statistics and Analysis Q2 2022* (Report Code GDDT-PL-M102), *Patent Statistics and Analysis Q3 2022* (Report Code GDDT-PL-M102), available via login at https://www.globaldata.com/.
7. *Id*.
8. *Id*.
9. *Id*.
10. The partnership page is available at https://www.uspto.gov/initiatives/artificial-intelligence.
11. United States Copyright Office, *Works Containing Material Generated by Artificial Intelligence*, March 16, 2023, 16190 Federal Register, VOL. 88, NO. 51.
12. *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022).
13. Ashley Gold, *DOJ has eyes on AI, antitrust chief tells SXSW crowd*, Axios (March 13, 2023) https://www.axios.com/2023/03/13/doj-kanter-ai-artificial-intelligence-antitrust; Lina Kahn, *Lina Khan: We Must Regulate A.I. Here's How*, The New York Times (May 3, 2023) https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html.
14. Microsoft's responsible AI principles are available at https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1:primaryr5.
15. Robert G. Eccles and Miriam Vogel, *Board Responsibility for Artificial Intelligence Oversight*, Harvard Law School Forum on Corporate Governance (January 5, 2022) https://corpgov.law.harvard.edu/2022/01/05/board-responsibility-for-artificial-intelligence-oversight.
16. *Legislation Related to Artificial Intelligence*, National Conference of State Legislatures (January 5, 2022) https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.
17. *Legislation Related to Artificial Intelligence*, *supra* note 8.
18. The White House, FACT SHEET: *Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public* (October 4, 2022) https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.
19. Eccles *supra* Note xv.
20. The White House *supra* Note xviii.
21. Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, Federal Trade Commission (April 19, 2021) https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.
22. Erin Mulvaney, *Artificial Intelligence Hiring Bias Spurs Scrutiny and New Regs*, Bloomberg Law Daily Labor Report (December 29, 2021, 5:30 AM) https://news.bloomberglaw.com/daily-labor-report/artificial-intelligence-hiring-bias-spurs-scrutiny-and-new-regs.

Sean D. Christy
Tel: +1 404 443 2146 / Email: sean.christy@nortonrosefulbright.com

Sean Christy counsels public and privately held companies around the world on technology, outsourcing and other strategic commercial transactions in the financial services, hospitality, healthcare, life sciences, consumer products, retail, energy and technology industries. His practice includes serving as both a business and legal adviser to his clients in the following areas: digital transformation (including as pertains to this chapter, on the development, acquisition and deployment of AI), traditional and digital outsourcing, acquisition-driven technology and operations transactions and advice, technology and commercial disputes and workouts, and fully or portfolio-outsourced commercial contract consulting and support. He provides guidance on strategic direction and negotiation strategy, analysing client operations, selecting suppliers, scope/pricing/quality, providing post-transaction support, counselling on post-transaction governance and disputes, audit defence and other key commercial issues his clients face throughout the lifecycle of their deals.

Chuck Hollis
Tel: +1 404 443 2147 / Email: chuck.hollis@nortonrosefulbright.com

Chuck Hollis is a technology, outsourcing and strategic commercial transaction lawyer handling a range of technology and commercial arrangements both in the US and globally for a range of clients including those in the financial services, hospitality, energy, healthcare and consumer products/retail industries and sectors. Chuck provides not only transactional legal advice, but also negotiation business strategy, vendor selection and consultative advice. His technology, outsourcing and commercial transactions experience includes global support for cloud services, cloud operations, digital transformation initiatives, development and implementation of ERP, SaaS, XaaS, AI/ML and other technology and software platforms and solutions. Chuck's practice also includes support for the more traditional outsourcing arrangements (ITO, BPO, ADM), and provides post-transaction governance and dispute support, including realignments and workouts related to outsourcing and technology arrangements.

Norton Rose Fulbright US LLP

7676 Forsyth Blvd, Suite 2230, St. Louis, Missouri 63105, USA
Tel: +1 314 505 8800/ URL: www.nortonrosefulbright.com

www.globallegalinsights.com

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

Banking Regulation
Blockchain & Cryptocurrency
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

GLI GLOBAL LEGAL INSIGHTS