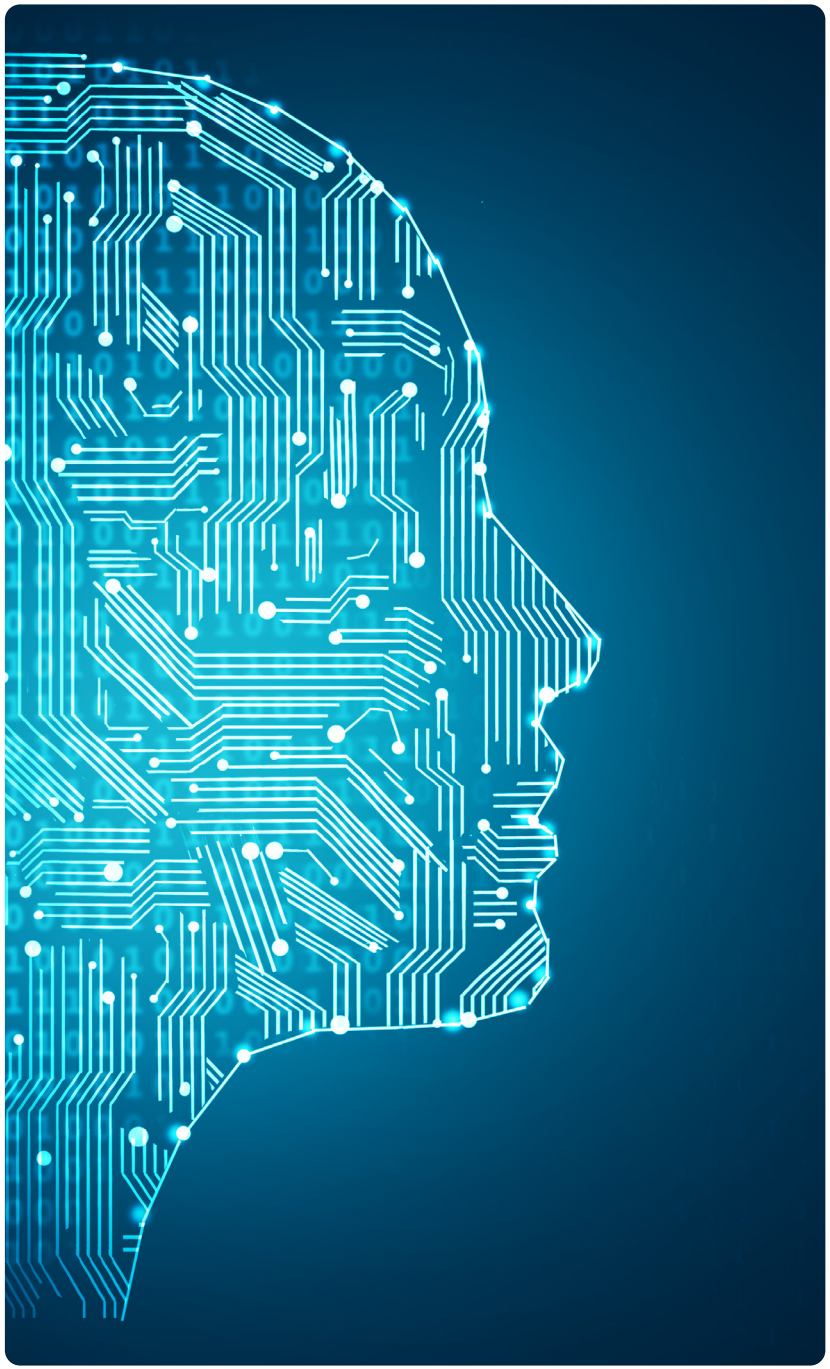

Photo by Peshkova on Shutterstock

LEXOLOGY
Getting the Deal Through

Market Intelligence

ARTIFICIAL INTELLIGENCE 2022

Global interview panel led by Lisa Peets, Sam Jungyun Choi and Jiayen Ong of Covington & Burling LLP

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Covington & Burling LLP, this Artificial Intelligence volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Government strategies
Ethics & human rights
Data protection & privacy
Industry sector application

START READING

About the editors



Lisa Peets, Sam Jungyun Choi and Jiayen Ong
Covington & Burling LLP

Lisa Peets leads the technology regulatory practice in Covington & Burling's London office and is a member of the firm's Management Committee. Ms Peets divides her time between London and Brussels, and her practice embraces regulatory counsel and legislative advocacy. In this context, she has worked closely with leading multinationals in a number of sectors, including some of the world's best-known technology companies.

Sam Jungyun Choi is an associate in the technology regulatory group in the Brussels office. Her practice focuses on European data protection law and new policies and legislation relating to innovative technologies such as artificial intelligence, online platforms, digital health products and autonomous vehicles. Ms Choi advises leading technology and life sciences companies on a wide range of matters relating to data protection and cybersecurity issues.

Jiayen Ong is an associate in the technology regulatory group in the London office. She has experience across a broad range of technology regulatory issues, with a focus on European data protection law and recent policies and legislation regarding innovative technologies.

Contents

While reading, click this icon to return to the Contents at any time

Photo by kavalenkava on Shutterstock

European Union

Lisa Peets leads the technology regulatory practice in Covington & Burling's London office and is a member of the firm's management committee. Her practice embraces regulatory counsel and legislative advocacy. In this context, she has worked closely with leading multinationals in a number of sectors, including some of the world's best-known technology companies. Ms Peets counsels clients on a range of EU law issues, including data protection and related regimes, content moderation and consumer protection, and the rapidly expanding universe of EU rules applicable to existing and emerging technologies.

Sam Jungyun Choi is an associate in the technology regulatory group in the Brussels office. Her practice focuses on European data protection law and new policies and legislation relating to innovative technologies such as artificial intelligence, online platforms, digital health products and autonomous vehicles. Ms Choi advises leading technology and life sciences companies on a wide range of matters relating to data protection and cybersecurity issues.

Madelaine Harrington is an associate in the technology regulatory group in the London office. Her practice covers a wide range of regulatory and policy matters at the cross-section of privacy, content moderation, artificial intelligence and free expression. Ms Harrington has in-depth experience with regulatory investigations. She routinely counsels clients on compliance within the EU regulatory framework.

Jiayen Ong is an associate in the technology regulatory group in the London office. She has experience across a broad range of technology regulatory issues, with a focus on European data protection law and recent policies and legislation regarding innovative technologies.

1 What is the current state of the law and regulation governing AI in your jurisdiction? How would you compare the level of regulation with that in other jurisdictions?

Currently, the European Union does not have laws or regulations that specifically regulate AI systems. However, there are a number of existing laws and regulations – both horizontal and sector-specific – that apply to AI technologies and applications. Perhaps most important is the EU's General Data Protection Regulation (GDPR), which sets out a range of prescriptive obligations that apply to the processing of personal data, including personal data processed in the context of training, testing and deploying AI applications.

The GDPR also includes transparency and other obligations relating to automated decision-makings. Other EU laws in this vein include the Better Enforcement Directive, which requires traders to inform consumers when prices of goods and services have been personalised based on automated decision-making and profiling, and the Platform-to-Business Regulation, which requires that online intermediation service providers and search engine providers be transparent about the algorithms used to rank business users and corporate websites on its services.

Other EU legal frameworks that may apply to AI applications, depending on the context, include medical devices rules, financial services regulations, cybersecurity laws, copyright and other intellectual property rules and consumer protection law.

As described below, the EU is currently considering AI-specific legislation. In that regard, the EU is fairly advanced in its consideration of the unique legal issues that can arise in the context of the development and deployment of AI systems.

"In May 2022, the EC published the proposed Regulation for the European Health Data Space. If adopted, this proposal will create a common EU data space for health data."

2 Has the government released a national strategy on AI? Are there any national efforts to create data sharing arrangements?

European strategy on AI

In 2018, the European Commission (EC) published a Coordinated Plan on Artificial Intelligence, which set out a joint commitment by the EC and the member states to work together to encourage investments in AI technologies, develop and act on AI strategies and programmes, and align AI policy to reduce fragmentation across jurisdictions.

In April 2021, the EC conducted a review of the progress on the 2018 Coordinated Plan, and adopted an updated plan with the following additional policy objectives:

- set enabling conditions for AI development and uptake in the EU;
- make the EU the place where excellence thrives from the lab to market;
- ensure that AI works for people and is a force for good in society; and
- build strategic leadership in high-impact sectors.

The EC has also proposed that the EU invests at least €1 billion per year from the Horizon Europe and Digital Europe programmes in AI.

At the national level, a 2022 review found that 24 of the 27 EU member states have adopted national strategies on AI – and that the remaining member states are working on national strategies that are expected to be published soon.

The EU has also been actively considering legislation that will regulate AI technologies. These include the following (discussed later in this chapter):

- the proposed Regulation Laying Down Harmonised Rules on AI (the AI Act Proposal); and
- the proposed Directive on Adapting Non-Contractual Civil Liability rules to Artificial Intelligence (the AI Liability Directive Proposal).

European data sharing policy

European policymakers recognise that access to data is an important requirement to enable the growth of AI technologies. In 2020, the EC published a Communication on Shaping Europe's Digital Future and a European Strategy for Data. The Communication recommended enhancing regulatory frameworks to, among other objectives, encourage and enable data sharing.

Over the past year, the EC has adopted legislation aimed at furthering the European strategy for data:

- In June 2022, the EU adopted its Regulation on European Data Governance (the Data Governance Act). The Data Governance Act includes a range of measures designed to promote the reuse of

public sector data and establishes a European Data Innovation Board, among other things.

- In September 2022, the EU adopted its Regulation on Contestable and Fair Markets in the Digital Sector (the Digital Markets Act). The Digital Markets Act introduces measures to regulate online 'gatekeepers'. One of the obligations in the Digital Markets Act requires gatekeepers to make available to business users data 'provided for or generated in the context of' the business user's use of the gatekeeper's services.

The EU institutions are currently reviewing several additional legislative proposals that are also aimed at furthering the European strategy for data. These include the following:

- In February 2022, the EC published the proposed Regulation on Harmonised Rules on Fair Access to and Use of Data (the Data Act). The Data Act includes provisions designed to give users of certain specified products and related rights to access and port data generated by their use. The Data Act also seeks to lower the barriers to users for switching between different data processing services.
- In May 2022, the EC published the proposed Regulation for the European Health Data Space. If adopted, this proposal will create a common EU data space for health data, with the ultimate aim of (1) empowering individuals to control and utilise their own health data in their home country and in other member states, and (2) furthering research, innovation, policy-making and regulatory activities within the health sector.

UK's innovation-friendly approach

Separate from the EU, the UK government in September 2021 adopted its own National AI Strategy. The UK government's strategy is focused on adopting an innovation-friendly approach to AI regulation. The UK government followed this Strategy, in July 2022, with a proposal for

Photo by Mickis-Fotowelt on Shutterstock

a new AI rulebook that sets out six AI-related principles. These 'core principles' will require developers and users of AI to:

- ensure that AI is used safely;
- ensure that AI is technically secure and functions as designed;
- make sure that AI is appropriately transparent and explainable;
- consider fairness;
- identify a legal person to be responsible for AI; and
- clarify routes to redress or contestability.

The UK government envisages that these core principles will form the basis for sector-specific guidelines to be developed by industry, academia and regulators.

QUESTIONS

"At the member state level, national strategies on AI address the ethical and human rights implications of AI. Like the EC, many member states have established independent bodies tasked with advising on ethical issues raised by AI."

3 What is the government policy and strategy for managing the ethical and human rights issues raised by the deployment of AI?

In April 2021, the EC published its proposal for an AI Act. The AI Act Proposal is the first EU legislative proposal that is designed specifically and exclusively to regulate the development, deployment and use of AI systems. The AI Act Proposal adopts a risk-based approach to regulation, imposing the most extensive obligations on providers of 'high-risk' AI systems – and prohibiting certain types of AI outright. Certain types of non-high-risk AI systems will also be subject to transparency obligations.

The AI Act Proposal has been the subject of significant scrutiny and debate during the legislative process, and while the final Act is likely to broadly track the EC Proposal, it is likely to have some meaningful differences in the obligations it imposes.

Prohibited AI systems

The AI Act Proposal would ban certain types of AI systems from being placed on the EU market, put into service or used in the EU. These include AI systems that either deploy subliminal techniques (beyond a person's consciousness) to materially distort a person's behaviour, or exploit the vulnerabilities of specific groups (such as children or persons with disabilities), in both cases where physical or psychological harm is likely to occur. The AI Act Proposal would also prohibit public authorities from placing on the market, putting into service or using AI systems in the EU for 'social scoring', where this leads to detrimental or unfavourable treatment in social contexts unrelated to the contexts in which the data was generated, or is otherwise unjustified or disproportionate. Finally, the AI Act Proposal bans law enforcement from using 'real-time' remote biometric identification systems in publicly accessible spaces, subject to limited exceptions (eg, searching for specific potential victims of crime, preventing imminent threats to life or safety or identifying specific suspects of significant criminal offences).

High-risk AI systems

The AI Act Proposal would also classify certain AI systems as high-risk, and subject those systems to more extensive regulation. Prior to placing a 'high-risk AI system' on the EU market or putting it into service, providers are required to conduct a conformity assessment procedure (either self-assessment or third-party assessment depending on the type of AI system) of their systems. To demonstrate compliance, providers must draw up an EU declaration of conformity and affix the CE marking of conformity to their systems.

The types of AI systems considered high-risk are enumerated exhaustively in Annexes II and III of the AI Act Proposal, and include AI systems that are, or are safety components of, certain regulated products (eg, medical devices, motor vehicles) and AI systems that are used in certain specific contexts or for specific purposes (eg,

biometric identification systems, systems for assessing students in educational or vocational training).

The AI Act Proposal also requires that providers of high-risk AI systems ensure that their AI systems meet certain substantive obligations. Among them, providers must design high-risk AI systems to enable record-keeping; allow for human oversight aimed at minimising risks to health, safety or fundamental rights; and achieve an appropriate level of accuracy, robustness and cybersecurity. Data used to train, validate or test such systems must meet quality criteria, including for possible biases, and be subject to specified data governance practices. Providers must prepare detailed technical documentation, provide specific information to users and adopt comprehensive risk management and quality management systems.

The AI Act Proposal also imposes obligations on importers and distributors of AI systems, to ensure that high-risk AI systems have undergone the conformity assessment procedure and bear the proper conformity marking before being placed on the market, as well as obligations on users of such systems.

Non-high-risk AI systems

The AI Act Proposal would also introduce transparency obligations on certain non-high-risk AI systems, as follows:

- Providers of AI systems intended to interact with natural persons must develop them in such a way that people know they are interacting with the system.
- Providers of 'emotion recognition' and 'biometric categorisation' AI systems must inform people who are exposed to them of their nature.
- Providers of AI systems that generate or manipulate images, audio or video content must disclose to people that the content is not authentic.

Photo by Adisa on Shutterstock

For other non-high-risk AI systems, the AI Act Proposal also encourages providers to create codes of conduct to foster voluntary adoption of the obligations that apply to high-risk AI systems.

Member state guidance on AI ethics

At the member state level, national strategies on AI address the ethical and human rights implications of AI. Like the EC, many member states have established independent bodies tasked with advising on ethical issues raised by AI. These include Germany's Data Ethics Commission and France's National Consultative Committee for Ethics. In the UK, the UK's Centre for Data Ethics and Innovation and the UK government's Office for AI publish guidance relating to AI ethics.

QUESTIONS

4 What is the government policy and strategy for managing the national security and trade implications of AI? Are there any trade restrictions that may apply to AI-based products?

On 9 September 2021, the EU's recast of the Dual-Use Regulation entered into force. While export controls under the previous EU dual use regulation applied to certain AI-based products, such as those that use encryption software, and any AI products that are specifically designed for a military end use, the updated Dual-Use Regulation broadens the scope of the controls and implements more extensive requirements for cyber-surveillance related goods, software and technology, and military-related technical assistance activities.

5 How are AI-related data protection and privacy issues being addressed? Have these issues affected data sharing arrangements in any way?

The GDPR applies to all processing of personal data, including in the context of AI systems. The GDPR imposes, among other obligations, requirements on data controllers to be transparent about their processing, identify a legal basis for the processing, comply with data subject rights, keep personal data secure and keep records to demonstrate compliance with the GDPR.

Notably, the GDPR includes specific requirements on fully automated decision-making (ADM) that has legal or similarly significant effects on individuals (article 22). This provision is likely to be particularly relevant to AI-based algorithmic decision-making processes. Under the GDPR, individuals have the right not to be subject to ADM unless the processing is based on the individual's explicit consent, is necessary for performance of a contract between the organisation and the individual or is authorised by member state or EU law. Even when these conditions are met, organisations must provide individuals with 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' (article 13(2)(f)). Organisations carrying out ADM must also implement safeguards, including, at a minimum, the right to contest the decision and obtain human review of the decision (article 22(3)).

> "Any cross-border transfers of personal data from within the EU to outside the EU will also be subject to the GDPR's rules."

The GDPR will also govern the sharing of personal data between multiple organisations where sharing of personal data is required to develop or deploy an AI application. These rules include ensuring that any joint controllers of the personal data set out their respective roles and responsibilities for compliance with the GDPR in a transparent way (article 26), and also require that controllers put in place data processing agreements with their processors (article 28). Any cross-border transfers of personal data from within the EU to outside the EU will also be subject to the GDPR's rules on international data transfers (Chapter V).

In addition, the development and deployment of AI technologies in certain contexts may also trigger the requirement to carry out a mandatory data protection impact assessment (article 35), which will require organisations to carry out an in-depth review of their data protection compliance specific to the project.

A number of member state data protection authorities (DPAs) have taken an interest in the application of the GDPR to AI. In May 2022, for example, the European Data Protection Board, which brings together all 27 member state DPAs, published guidelines on facial recognition technology in the area of law enforcement, which is awaiting adoption following a public consultation. The UK Information Commissioner's Office (ICO) has also published guidance documents regarding the application of data protection principles to AI. Other DPAs, including the French CNIL, the Norwegian Datatilsynet and the Spanish AEPD, have issued guidance on AI and data protection.

6 How are government authorities enforcing and monitoring compliance with AI legislation, regulations and practice guidance? Which entities are issuing and enforcing regulations, strategies and frameworks with respect to AI?

As there is currently no AI-specific legislation in Europe, government authorities do not yet have the power to enforce and monitor compliance with AI-specific legislation. However, once the AI Act Proposal is implemented, violations of the AI Act Proposal may be subject to fines of up to €30 million or 6 per cent of a company's worldwide annual turnover (whichever is higher).

To the extent that existing laws and regulations apply to AI applications, government authorities have been exercising their powers under these rules in relation to AI applications. As noted in question 5, some member state DPAs have issued AI-specific guidance in relation to data protection law compliance. Infringements

Photo by Songquan Deng on Shutterstock

of GDPR could result in fines of up to €20 million or 4 per cent of a company's worldwide annual turnover (whichever is higher), depending on the provisions infringed.

Further, a number of DPAs have recently taken enforcement actions focused on specific AI use cases, particularly relating to facial recognition technology (FRT) used for surveillance purposes. For example, the Swedish DPA in February 2021 fined the Swedish police for using FRT to identify individuals, and in August 2019 fined the Skellefteå municipality for using FRT to track student attendance in a state school.

In the UK, the use of FRT systems by law enforcement for policing and security purposes was also the subject of a human rights challenge before the English High Court (*R (Bridges) v Chief Constable of South Wales Police* [2019] WLR (D) 496 (UK)) and Court of Appeal (*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058), and led the UK ICO to subsequently issue an opinion on the use of live FRT by law enforcement in public places. In November 2021, the UK

"The EC announced an international outreach for human-centric AI project (InTouchAI.eu) to promote the EU's vision on sustainable and trustworthy AI."

ICO concluded an investigation into Clearview AI's facial recognition technologies, and fined Clearview AI more than £7.5 million for privacy violations (a reduction from the provisional fine of £17 million). The ICO also ordered the company to delete the data of UK residents from its systems. Subsequently, (1) the French CNIL similarly found that Clearview AI's facial recognition software breached GDPR and imposed a fine of €20 million and ordered Clearview AI to cease data collection in France, (2) the Italian DPA fined Clearview AI €20 million and ordered the deletion of data of Italian citizens, and (3) the Greek DPA fined Clearview AI €20 million and ordered the deletion of data of Greek citizens. Since many AI applications involve the processing of personal data, we expect DPAs to play an important role in monitoring AI applications.

7 Has your jurisdiction participated in any international frameworks for AI?

The EU has been a thought leader in the international discourse on ethical frameworks for AI. The AI HLEG's 2019 AI Ethics Guidelines were, at the time, one of the most comprehensive examinations on AI ethics issued worldwide, and involved a number of non-EU organisations and several government observers in its drafting. In parallel, the EU was also closely involved in developing the OECD's ethical principles for AI and the Council of Europe's Recommendation on the Human Rights Impacts of Algorithmic Systems. The EU also forms part of the Global Partnership on AI (GPAI).

At the United Nations, the EU is involved in the report of the High-Level Panel on Digital Cooperation, including its recommendation on AI. The EC recognises that AI can be a driving force to achieve the UN Sustainable Development Goals and advance the 2030 agenda.

The EC states in its 2020 AI White Paper that the EU will continue to cooperate with like-minded countries and global players on AI, based on an approach that promotes the respect of fundamental rights and European values. Also, article 39 of the EC's AI Act Proposal provides a mechanism for qualified bodies in third countries to carry out conformity assessments of AI systems under the Act.

On 1 September 2021, the EC announced an international outreach for human-centric AI project (InTouchAI.eu) to promote the EU's vision on sustainable and trustworthy AI. The aim is to engage with international partners on regulatory and ethical matters and promote responsible development of trustworthy AI at a global level. This includes facilitating dialogue and joint initiatives with partners, conducting public outreach and technology diplomacy

and conducting research, intelligence gathering and monitoring of AI developments. Also, at the first meeting of the US–EU Trade and Technology Council on 29 September 2021, the United States and EU 'affirmed their willingness and intention to develop AI systems that are innovative and trustworthy and that respect universal human rights and shared democratic values'. The participants also established 10 working groups to collaborate on projects furthering the development of trustworthy AI. This collaborative approach continued in the second meeting of the US–EU Trade and Technology Council on 15–16 May 2022, where the United States and EU agreed to develop shared methodologies for measuring AI trustworthiness and risks.

The EU member states have also been active in the Council of Europe. On 3 November 2021, the Council of Europe published a Recommendation on the Protection of Individuals with regard to Automatic Processing of Personal Data in the context of profiling, which defines 'profiling' as 'any form of automated processing of personal data, including machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an individual, particularly to analyse or predict that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. The recommendation encourages Council of Europe member states to promote and make legally binding the use of a 'privacy by design' approach in the context of profiling, and sets out additional safeguards to protect personal data, the private life of individuals, and fundamental rights and freedoms such as human dignity, privacy, freedom of expression, non-discrimination, social justice, cultural diversity and democracy.

The UK is also actively participating in the international discourse on norms and standards relating to AI. It continues to engage with the OECD, Council of Europe, United Nations and the GPAI.

Photo by ecstk22 on Shutterstock

8 What have been the most noteworthy AI-related developments over the past year in your jurisdiction?

On 28 September 2022, the EC published its proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (the AI Liability Directive Proposal). The AI Liability Directive Proposal sets out harmonised rules on (1) the disclosure or preservation of information regarding high-risk AI systems and the standard of proof required to compel the same, and (2) the burden of proof, and corresponding rebuttable presumptions, applicable to claim for damages caused by AI systems.

The AI Liability Directive Proposal gives courts the power to order providers or users of high-risk AI systems to disclose (or preserve) information about their systems to persons who seek this information to initiate (or decide whether to initiate) redress proceedings against the provider or user. A court may issue such an order upon the request of (1) a 'potential claimant', who has already

> "The use of computer vision to power FRT systems for surveillance, identity verification and border control has been a notable development."

requested this information directly from the provider or user but not received it, or (2) a claimant who has initiated proceedings. The requestor must present facts and evidence 'sufficient to support the plausibility of a claim' that the high-risk AI system caused the alleged damage.

Courts will only order a provider or user to disclose as much information as is necessary and proportionate to support a (potential) claim for damages. The court will take into account the legitimate interests of all parties, including any trade secrets. If a disclosure order covers information that is considered a trade secret which a court deems confidential pursuant to the EU Trade Secret Directive, the court may take measures necessary to preserve the confidentiality of that information during the proceedings. If the provider or user does not comply with the court's order to disclose information, the court may assert a rebuttable presumption that the provider or user breached a duty of care, including that they failed to comply with the provisions of the AI Act that the requestor alleges were violated.

In addition, the AI Liability Directive Proposal identifies a number of circumstances in which a court may presume a (causal) link between (1) the fault of the provider or user of any AI system (whether high-risk or not), and (2) the output produced by the AI system or its failure to produce such an output. For high-risk AI systems, this presumption applies if the claimant has demonstrated the provider or user's non-compliance with certain obligations under the AI Act, subject to certain exceptions and restrictions. For example, the presumption will not apply if the court finds that the claimant has sufficient evidence and expertise to prove a causal link.

9 Which industry sectors have seen the most development in AI-based products and services in your jurisdiction?

AI uptake has increased across the EU market in a range of sectors, including in the health and transport sectors and by law enforcement.

The use of computer vision to power FRT systems for surveillance, identity verification and border control has been a notable development in the EU, raising a number of data protection law-related concerns, as discussed in the response to question 6. The use of other biometric identification systems, such as voice recognition technology, has also proliferated. Biometric identification technology can be seen in many forms – from voice authentication systems for internet banking to smart speakers for home use.

The digital health sector has also seen an increase in AI-powered solutions, including apps that diagnose diseases, software tools for those with chronic ailments, platforms that facilitate communication between patients and healthcare providers, virtual or augmented reality tools that help administer healthcare and research projects

involving analysis of large data sets (eg, genomics data). The advances in autonomous vehicles would not be possible without the development of AI systems, and autonomous vehicles must implement multiple, complex interrelated AI systems to deal with the different aspects of autonomous vehicles (eg, localisation, scene understanding, planning, control and user interaction) in order to improve safety, mobility and the environment.

10 Are there any pending or proposed legislative or regulatory initiatives in relation to AI?

As discussed above, the EU is currently considering two significant AI-related legislative proposals, the AI Act and the AI Liability Directive. The AI Act was proposed in April 2021, and is far advanced in the legislative process, with adoption possible in 2023. The AI Liability Directive was proposed in September 2022, and is still in the early stages of the legislative process.

11 What best practices would you recommend to assess and manage risks arising in the deployment of AI?

Companies developing or deploying AI applications in the EU should be mindful that a number of laws and regulations may apply to their AI application – including, but not limited to, those discussed in the preceding responses. Companies would be well advised to ensure compliance with these laws and look to government authorities that are responsible for enforcement in their sector for any sector-specific guidance on how these laws apply to AI applications. Companies should also closely monitor legislative developments, and consider participating in the dialogue with policymakers on AI legislation to inform legislative efforts in this area.

Lisa Peets
lpeets@cov.com

Covington & Burling LLP
London, Brussels
www.cov.com

Sam Jungyun Choi
jchoi@cov.com

Madelaine Harrington
mjharrington@cov.com

Jiayen Ong
jong@cov.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

What skills and experiences have helped you to navigate AI issues as a lawyer?

At Covington, we have been working with leading technology and internet companies for decades, and we have a deep understanding of the sector and of technology and digital products and services. Throughout that period, we have helped clients navigate the full range evolving legal landscapes applicable to their innovations. We take a multi-disciplinary approach, and as a firm, we are also focused on collaboration across our lawyers and on bringing the best team to any given matter; this is essential when advising on AI-related projects, because those projects often raise issues under multiple legal regimes. We also work closely together across offices, which again is important given the global nature of our clients' services and solutions.

Which areas of AI development are you most excited about and which do you think will offer the greatest opportunities?

The development of AI technology is affecting virtually every industry and has tremendous potential to promote the public good. In the healthcare sector, for example, AI will continue to have an important role in helping to mitigate the effects of covid-19, along with potentially improving health outcomes while reducing costs. AI also has the potential to enable more efficient use of energy and other resources and to improve education, transportation, and the health and safety of workers. We are excited about these and many other opportunities presented by AI.

What do you see as the greatest challenges facing both developers and society as a whole in relation to the deployment of AI?

AI has tremendous promise to advance economic and public good in many ways and it will be important to have policy frameworks that allow society to capitalise on these benefits and safeguard against potential harms. As this publication explains, several jurisdictions are advancing different legal approaches with respect to AI. One of the great challenges is to develop harmonised policy approaches that achieve desired objectives. We have worked with stakeholders in the past to address these challenges with other technologies, and we are optimistic that workable approaches can be crafted for AI.