ISSUE N.1 | SEPTEMBER 2024

Diritto Intelligente

A JOURNAL ON AI-RELATED EU LAWS, CASES, AND OPINIONS BY DLA PIPER'S ITALIAN INTELLECTUAL PROPERTY AND TECHNOLOGY GROUP.

In this issue

DLA PIPER

Contents

Editorial

Welcome to the inaugural issue of *Diritto Intelligente*, the online journal by DLA Piper's Italian Intellectual Property and Technology group, focusing on AI-related laws, cases, and opinions.

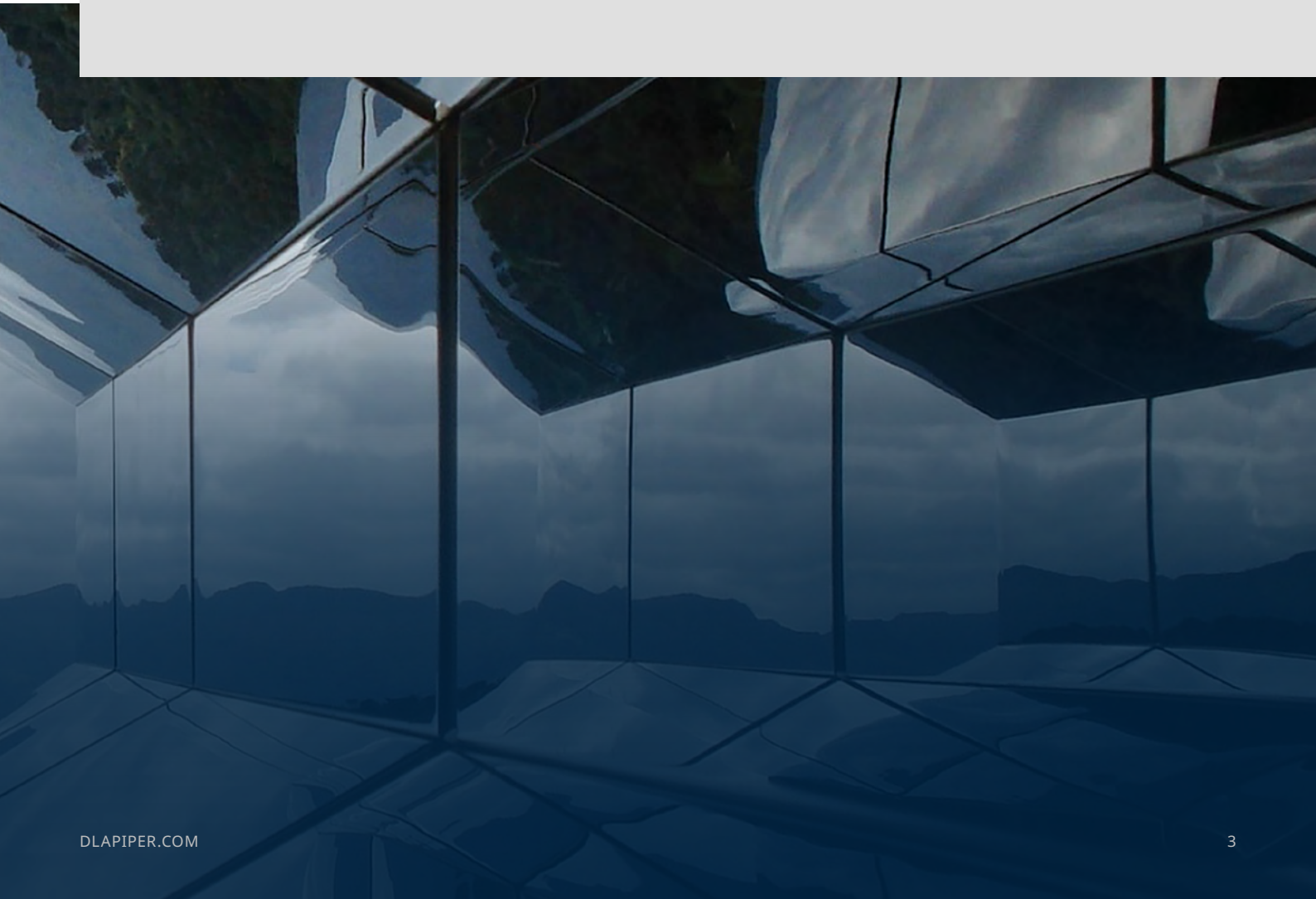
With the EU AI Act now in force and the deadline for prohibited AI systems approaching on February 2, 2025, and EU privacy authorities intensifying their scrutiny of AI data processing, this issue is exceptionally timely.

This is a pivotal moment for businesses to not only adopt AI but also ensure full compliance to avoid significant risks.

We delve into the most pressing legal challenges and opportunities in AI, offering crucial insights for businesses navigating this transformative technology.

We welcome your feedback and hope you find *Diritto Intelligente* both informative and engaging.

Giulio Coraggio
Partner
Head of Intellectual Property and Technology
Italy



AI Act and Laws

AI Act into force: Is your company ready for compliance?

Author: *Giulio Coraggio*

The AI Act was published in the Official Gazette of the European Union and has now officially come into force. Is your business ready to comply with it?

The different provisions of the AI Act will become applicable during a specific timeline that you can find in our report available here. However, with the clock running, no business can afford to adopt a technology which might have to be dismissed, renegotiated, and in any case changed in a few months.

Below is the methodology that we recommend towards becoming compliant:

Map AI systems: Identify all AI systems your business currently uses or plans to use. The risk is that your business is already using artificial intelligence solutions without it being aware and without considering the legal implications, for instance, due to local initiatives of departments or even individuals.

Create an AI governance framework: Establish internal rules for the use and approval of AI solutions. These rules should consider the obligations arising from the AI Act, data protection regulations, intellectual property laws, ISO standards for areas that are not covered, and ethical rules in line with ESG principles. These rules should not just prohibit any sort of usage of AI solutions since otherwise, there is a risk that employees will try to bypass them. They should create an approval process so that employees are aware of how business needs must be escalated.

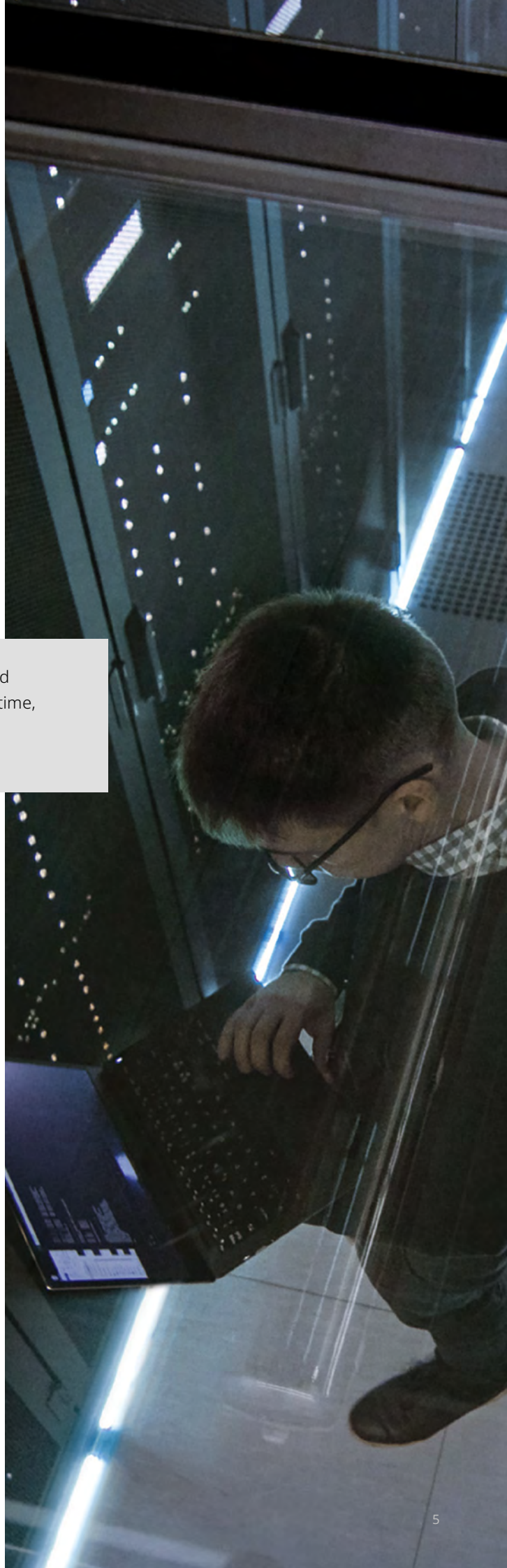
Create material to ease the understanding of the AI governance framework internally and start training your employees: The policy is usually accompanied with a leaflet that, in a short and easy-to-understand mannersummarises the most important contents of the governance framework. At the same time, organising training sessions for the different business units with a specific focus on the AI solutions impacting their activity is also a useful step. If employees and officers do not understand what can and cannot be done with AI solutions, the business will remain at risk.

Form an internal AI committee: Assign a team to evaluate AI solutions using a compliance-by-design approach. This team can include senior management, but it also needs operational members who will be involved in the assessment of the AI solution, liaise with the different business units, and monitor the AI solution even after its implementation.

Select and prioritise AI solutions: Determine which AI solutions to invest in and establish their priority levels. This activity will need a prior high-level assessment of the compliance risks and implications of the solutions identified by the business. The AI committee will then have to select solutions that fit the aforementioned requirements and obtain relevant budget approval.

Test and evaluate AI solutions: Begin evaluating selected AI technologies. This activity has technical and compliance implications. To support businesses in this potentially time-consuming task, we have developed Prisca AI Compliance, a solution that allows a convenient assessment of the compliance of artificial intelligence solutions across the AI Act, data protection laws, IP laws, and ISO standards, generating a detailed report that can be used for internal compliance as well as towards regulators and third parties challenging the conduct of the company.

Do you want to know more about the above-mentioned methodology? Reach out to us to discuss. In the meantime, you can read here some material on the most relevant legal issues of AI compliance.



AI Act: When is the survey on your employees becoming a prohibited artificial intelligence practice?

Author: *Giulio Coraggio*

The AI Act lists among the artificial intelligence prohibited practices the usage of systems inferring emotions in the workplace, but when does a survey of employees fall into this category?

The prohibited artificial intelligence practices able to infer emotions under the AI Act

The AI Act has now come into force, and the first deadline is 2 February 2025, when the provisions on prohibited AI practices (and the relevant sanctions) will become applicable. One of the prohibited AI practices that is more heavily discussed now relates to the use of AI systems to infer emotions of a natural person in the areas of workplace.

This broad provision applies to any AI system that can infer emotions. Indeed, the ability to infer emotions is also mentioned in recital 14 of the AI Act, where the Act provides that "biometric data can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons."

However, is the provision of the AI Act limited to artificial intelligence practices using biometric data?

The limits of compliance of a survey on employees with the AI Act

The issues addressed above are particularly relevant to surveys frequently run on employees to understand their level of satisfaction, morale, and potential information about their mental conditions. Especially after the pandemic, such surveys have become common and are run through software that can analyze and aggregate data.

These surveys trigger significant data protection and employment law issues across the European Union. But when do they also qualify as a prohibited AI practice?

We shall see how AI authorities address the issue. Running these surveys and allowing employees to respond to questions with open-ended answers is risky since they might communicate information beyond the purpose of the survey. However, this aspect is more of an employment and data protection law issue.

Indeed, the usage by the EU legislators of the term "inferring" seems to refer to cases when the artificial intelligence system detects some information that employees are not willing to share but can be understood through their answers. Otherwise, the legislators would have used the term "communicating," and an AI system would not be necessary to know such information.

We have seen surveys that rely on keywords to understand the mood of the interviewed individual. In such cases, the system already goes beyond what the potential employee wants to communicate. A case-by-case analysis is likely necessary. However, individuals' emotions are not inferred even in such a case since predetermined keywords are not tailored to the specific individual.

All in all, only biometric data can detect information unique to a specific individual. However, we shall see how the EU regulator interprets this provision. In any case, given the approaching deadline businesses should start scrutinising their current practices to check whether any of them qualify as AI-prohibited practices.

AI Pact's draft commitments published anticipating AI compliance

Author: *Giulio Coraggio*

The AI Act has been published, and in anticipation of its full applicability, the AI Office has launched the AI Pact, encouraging organisations to proactively adopt key provisions of the AI Act.

This initiative aims to ensure responsible AI usage and mitigate risks to health, safety, and fundamental rights.

What is the AI Pact?

The AI Pact is a voluntary commitment for organisations to start aligning with the AI Act's regulations before they become mandatory. By participating in the AI Pact, organisations can lead by example, demonstrating their dedication to ethical AI practices and preparing for the upcoming regulatory landscape. The Pact outlines several core and additional commitments that organisations can adopt based on their role in the AI ecosystem.

The AI Office has now published the draft commitments, and thanks Elinor Wahal for sharing them. Below is an analysis of their contents.

Core commitments for participating organisations

Organisations joining the AI Pact agree to implement three primary commitments:

- Adopt an AI Governance Strategy
- Map High-Risk AI Systems
- Promote AI Literacy

Additional commitments for a broader impact

While the core commitments lay the foundation, organisations are also encouraged to strive for additional goals based on their specific roles in the AI value chain. These commitments vary for AI providers and AI deployers:

For AI Providers:

- Risk Identification
- Data Quality Policies
- Traceability
- User Information
- Human Oversight
- Risk Mitigation
- Transparency in AI Interaction
- Content Marking

For AI Deployers:

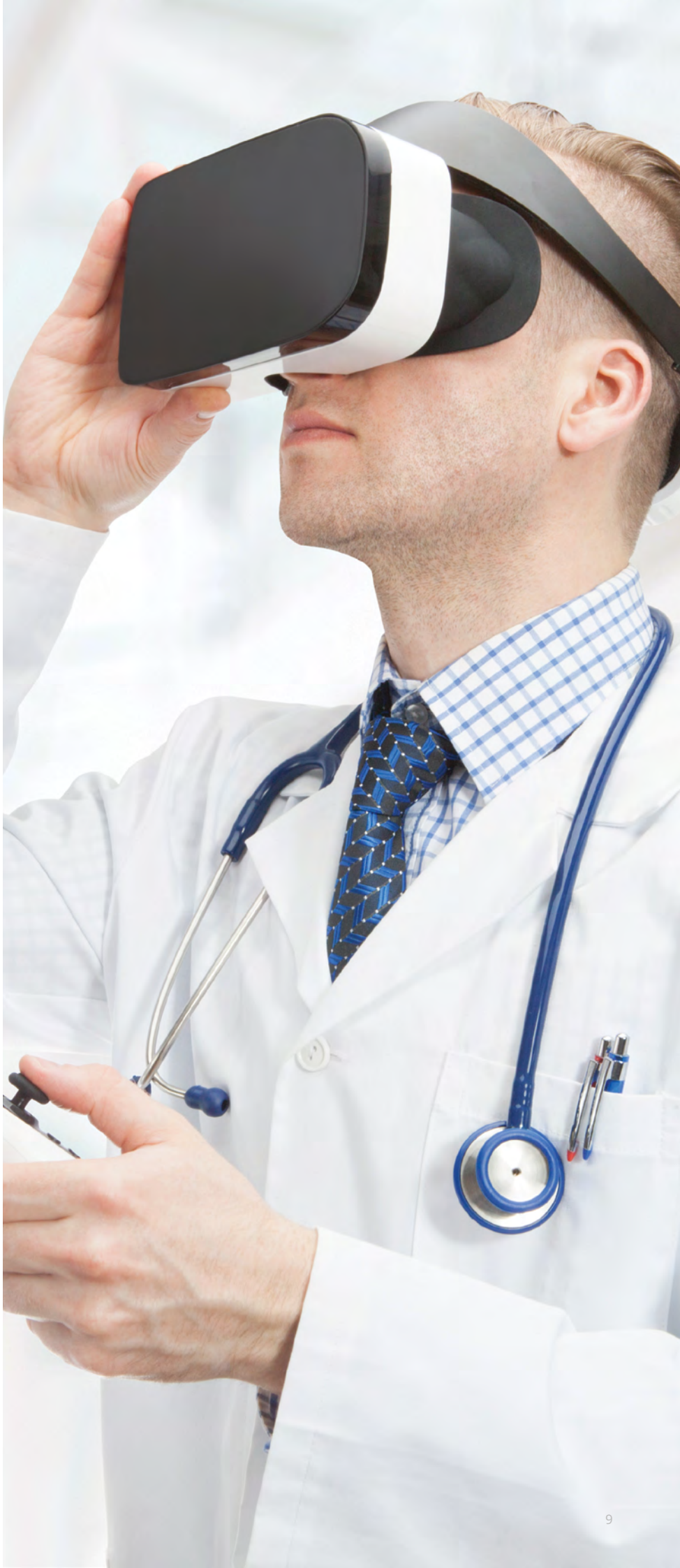
- Risk Mapping
- Human Oversight in Deployment
- Content Labelling
- User Notification
- Workplace Transparency

The path forward: Transparency and accountability

Organisations participating in the AI Pact are setting a standard for transparency and accountability in AI usage. By publicly sharing their commitments and reporting on their progress, these organisations not only demonstrate their dedication to ethical AI practices but also build trust with consumers, stakeholders, and regulators.

The AI Pact offers a unique opportunity for organisations to lead in the responsible adoption of AI. By anticipating and implementing the key provisions of the AI Act, participating organisations can mitigate risks, foster innovation, and ensure that AI's benefits are realised ethically and sustainably.

This is a crucial milestone in a process where companies want to adopt AI systems and are willing to minimise risks of potential challenges and generate trust towards their customers and employees to exploit AI at its best.



AI's intellectual property law news

Patenting AI: An important decision of the UK Court of Appeal in the Emotional Perception case

Author: *Massimiliano Tiberio*

The intersections between AI and intellectual property rights have long been the focus of numerous debates, and the rapid development of technology has often presented interpreters with scenarios not expressly contemplated by lawmakers.

This is the case, for example, regarding the possibility of patenting AI systems.

On the one hand, most jurisdictions provide that programs for computer and mathematical models can only be patented if they involve a technical contribution that's new and inventive compared to the state of the art. On the other hand, the possibility of patenting computer programs and mathematical methods as such is generally excluded (see, eg Article 52 of the European Patent Convention). But admitting the patentability of AI systems could to some extent encourage investment in innovation and the sharing of knowledge.

On 19 July 2024, the UK Court of Appeal issued an important decision on the subject *(Comptroller-General of Patents v Emotional Perception AI Ltd)*.

The dispute concerned a patent application claiming a system based on an artificial neural network (ANN) providing media file recommendations to users. For instance, in the context of music, the technology would make it possible to offer users tracks classified according to the emotions they generate, regardless of the musical genre they belong to.

The application was first rejected by the UK Intellectual Property Office (UKIPO), but the decision was later overturned by the High Court. Hence the appeal brought by the UKIPO.

To assess the applicability of the rules excluding patentability, the Court of Appeal first questioned the notion of a program for a computer. According to the judges, this is a "set of instructions for a computer to do something," a computer being any "machine that processes information."

That being clarified, the second question to be answered was: can an AI system such as the one claimed be treated in the same way as a program for computer?

The answer was affirmative: an artificial neural network, including the weights on which it is based, is still a set of instructions for a computer to do something.

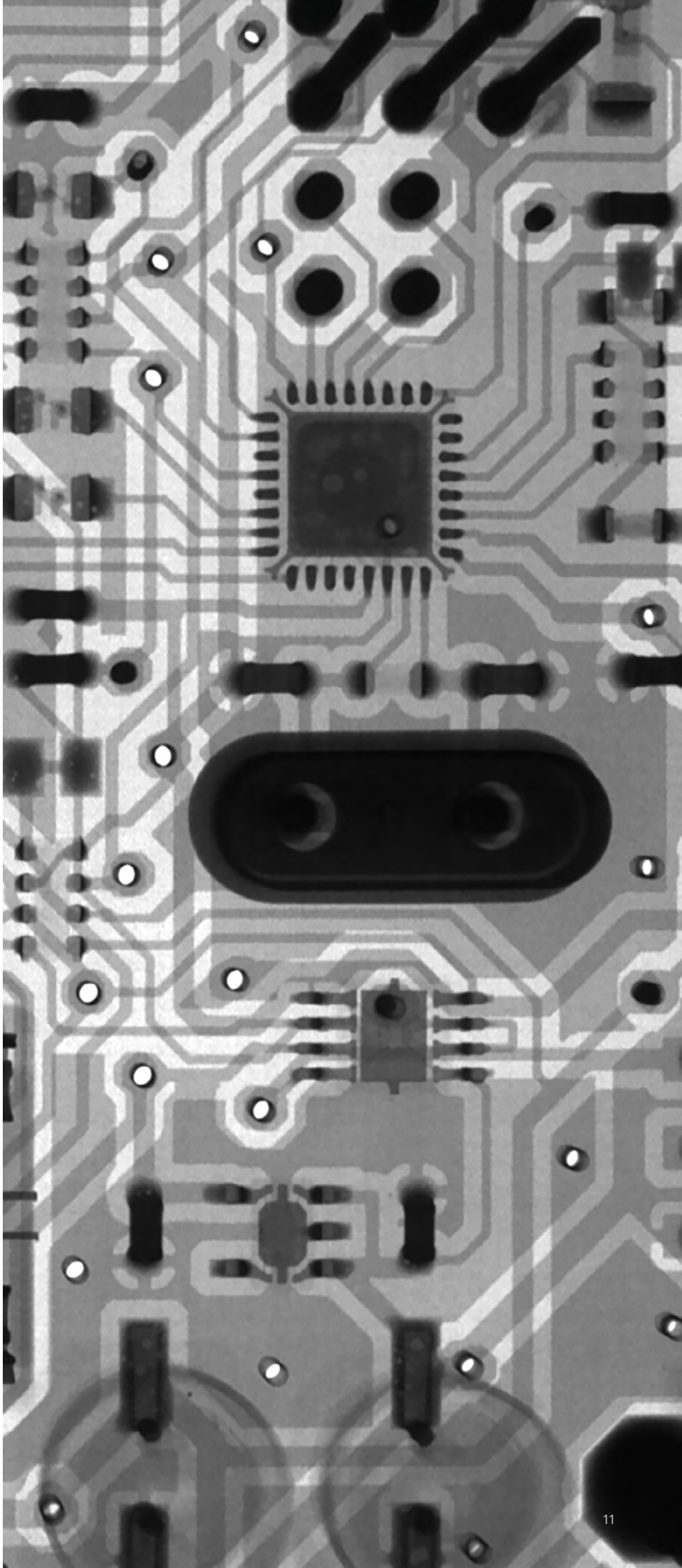
In this respect, disregarding the patentee's arguments, the court held that no relevance could be attributed to the peculiarities of an ANN system compared to more traditional computer programs. These include the lesser role of human being in defining instructions, the solution by the ANN of problems that would be difficult for a human programmer to solve, the fact that it's not a program based on "if-then" logic, or the fact that the machine learns by itself by processing a certain amount of information.

The reasoning then focused on whether or not there was a technical effect necessary for the program to qualify as a patentable invention. Considering that the system was essentially presented the user with improved file recommendations, the requirement was excluded, and the first instance decision was overturned.

Albeit very briefly, the court finally pointed out that, even if an artificial neural networks system did not qualify as a computer program, it could be qualified as a mathematical method. The assessment, therefore, would be similar.

In conclusion, what can be learned from the decision is that the patentability of an AI system based on an artificial neural network is not excluded per se, but it rather depends on whether the claimed invention involves a technical contribution. Failing that, the rules excluding the patentability of computer programs and mathematical methods as such apply.

The decision, among the first to rule on the patentability of inventions involving AI systems, is consistent with the approach taken so far by the European Patent Office. At this stage, it's not known whether the dispute will continue before the Supreme Court. What is certain is that the ruling will represent an important precedent in the jurisprudential landscape, even beyond the borders of the UK.



Elvis Act: Generative AI in copyright and advertising law

Author: *Rebecca Rossi*

On 21 March 2024, Tennessee enacted the Ensuring Likeness and Image Security (Elvis Act), a pioneering law that entered into force on 1 July 2024. The legislation aims to protect songwriters, artists, and music industry professionals from the potential dangers of unauthorized use of their voices and images by generative AI.

The Elvis Act (named after music icon Elvis Presley) represents a significant achievement in copyright protection, but its most innovative aspect lies in its extension to advertising law, including the unlawful use of artists' voices. With the increasing use of generative AI in the US and worldwide to create realistic voices and images, individual artists' reputations, images, and commercial value are often threatened. This law aims to counter these threats by regulating the use of generative AI and ensuring that artists maintain control over their own identities.

This measure aims to protect artists from potential issues, particularly economic ones, related to the computerized plagiarism of their voice or image, which is now within reach of any common application or program. With the enactment of the Elvis Act, artists will have specific legislation to seek compensation for damages resulting from the unauthorized use of their identity, including vocal clones and realistic images generated without consent.

This new law is an important step towards adapting laws to the era of new technologies, which today not only serve as creative tools but also facilitate the dissemination of so-called digital replicas. The Elvis Act comes at a time when there are numerous legal disputes against AI developers for improperly using copyrighted content.

A significant example is the case of actress Scarlett Johansson, who, in 2023, filed a lawsuit against an app that created an advertisement using her image and voice without authorisation. Similarly, the heirs of comedian George Carlin sued the creators of the podcast Dudesy for using Carlin's voice in a YouTube video, violating copyright and publicity laws. Another relevant case is Young v NeoCortext Inc, where participants of the reality show Big Brother started a class action lawsuit against a software developer for the unauthorised use of their images.

The explosion of these disputes and other dangers have necessitated the creation of specific regulations to protect the copyright and publicity rights of artists endangered in the era of generative AI. The Elvis Act, a significant response to this need, represents one of the most recent developments in this area.

With AI rapidly evolving, every jurisdiction must continue adapting to protect artists and their rights in an increasingly digital world. This is precisely what is happening lately: in Europe, the much-anticipated AI Act has also been published in the Official Journal, marking a significant step forward in this direction.

AI's data protection and cybersecurity updates

Large Language Models (LLMs) Do NOT process personal data according to the Hamburg privacy authority

Author: *Giulio Coraggio*

The Hamburg Data Protection Authority issued an insightful discussion paper addressing privacy risks and AI with a nuanced grasp of the technology.

Here are some groundbreaking insights:

- **LLM Processing and Data Storage:** Unlike traditional data systems, LLMs process tokens and vector relationships (embeddings), which the Hamburg DPC argues do not constitute "processing" or "storing" personal data under GDPR.
- **Tokenization vs. Personal Data:** Tokens and embeddings in LLMs do not have the direct, identifiable link to individuals required by CJEU jurisprudence to be considered personal data.
- **Memorisation Attacks:** While extracting training data from LLMs is possible, these attacks are often impractical and legally questionable, meaning personal data identification isn't always feasible under current legislation.
- **Legality of LLM Usage:** Even if personal data was mishandled during LLM development, it doesn't necessarily make using the resulting model illegal, offering reassurance to those deploying third-party models.

This paper reflects a sophisticated, tech-savvy approach to the intersection of AI and privacy.

Will other EU privacy authorities follow the same path? That would indeed be groundbreaking change for the industry!

AI's legal analysis

The insurability of AI risk: A broker's perspective

Authors: *Giacomo Lusardi, Karin Tayel*

There is an increasing discussion about AI risk and how companies can obtain insurance coverage to protect themselves in this sector. To investigate this issue, we spoke with a leading insurance broker. Alessandra Corsi and Rossella Bollini from Marsh provided their perspective on the nuances of AI risk coverage and the evolving role of insurance in mitigating AI-related liabilities.

1. From the broker's perspective, how is the insurance market responding to the coverage of AI risk?

The insurance market, especially since the GenAI explosion, has started to monitor the rise of new risks related to the development and use of artificial intelligence solutions, both to anticipate the demands of insureds and to start to efficiently manage exposure across existing portfolios. At the time of writing, the insurance market is still in an "observatory" stage whereby, other than for a very few cases, specific ad hoc AI solutions are not yet available. Based on Marsh global perspective, in the US and in selected European countries there is more attention around the topic: insureds do perceive the challenge that AI solutions bring along, wondering how to transfer their AI residual risk to the insurance market and pushing insurers to deliver answers and propose solutions. So far, the Italian market – both from a supply and demand angle – has not developed any meaningful initiatives; we expect this to change in the near future with carriers looking at finding value-added solutions for their clients.

2. In the described market context, how is AI risk exposure transferred? Is it possible to rely on traditional products?

Currently, there is only one ad hoc insurance product for AI risk, distributed by a leading player in the reinsurance market. Beyond this, clients looking for coverage can explore other established product lines such as Cyber, Professional Indemnity, Crime, Intellectual Property and Product Liability where typically claims and/or circumstances related to AI are not yet specifically excluded. Indeed, cover seems to be afforded on a "silent" basis: not affirmatively covered and not explicitly excluded. To give a few examples, if training data and input data can be captured by the model and leaked in the model outputs causing a data breach, the cyber policy could cover it; again, if a fraud is conducted using deepfake, the crime policy could cover it as well. Aiming to curb the level of uncertainty, AI affirmative endorsements on cyber and crime policies are very slowly being released but, at this point in time, this does not constitute the norm.

3. What risks do you think are potentially insurable with an AI policy?

Insurability is a complex topic, as it depends on the exposure, on the business conducted and on the insured's risk appetite. Depending on the situation, one could decide to cover first party damages – insuring the performance of self-built AI – or potential third-party liability profiles, either contractual or non-contractual. Depending on the business conducted by the insured, it might be relevant to cover risks from hallucination and false information, privacy infringement, intellectual property violations or unfair or biased output.

It goes without saying that a certain degree of tailoring is required to shape a product that fits the insured's needs.

4. Are traditional underwriting methods still relevant and applicable in the AI world?

They do remain relevant, but in a partial way. Let's make the comparison with cyber risk underwriting process. Although it's a complex and nuanced risk, the insurance market has settled on the use of questionnaires, sometimes combined with perimetral scanning or risk dialogues: as of now, it's a linear path. For AI risk, it may not be as straightforward. In order to quantify the risk, it will be necessary to identify the underwriting information on a case-by-case basis (deployer, user, type of AI involved) to be the evaluated together with data on model training and post-deployment controls.

The topic of quantifying damage in the event of a claim is also very complex: consider the case of an AI product provided to banks to recognise legitimate transactions from frauds. In this case, the provider would want to buy a policy to cover situations of underperformance of the product. To prevent the difficulty in quantifying the loss, it may be necessary to set a threshold eg guarantee that the tool model will catch at least 99% of all fraudulent transactions and if the AI fails to deliver as promised, the insurance company will pay.

5. Have you experienced the notification of any claims under AI policies or related to damages caused by AI? If yes, which type of claims?

As Marsh, most of the claims we've seen involving the use of GenAI are in the domain of fraud. As known, this refers to fraudulent transfer of funds obtained by creating the false belief in employees that they are complying with legitimate requests from internal parties within the company. As of now, claims that fall in this category are generally notified under crime policies. GenAI is also used to refine phishing attacks (currently, one of the main vectors of ransomware), making them more credible and increasing the success rate.

6. What are your predictions for the near future?

The path will likely be the same as experienced for cyber risk: eventually, insurers will need to quantify and monitor AI exposure within traditional insurance policies to the extent that it could represent a significant unexpected risk to their portfolios. To do so, the reinsurance markets and Lloyds of London might start imposing AI exclusions on cyber, professional indemnity, crime and other traditional products, creating a gap that will need to be filled. By that time, we expect AI-specific insurance products to be ready to perform, supported by a defined and replicable underwriting process and a consistently predictable loss quantification mechanism.

Contacts

Giulio Coraggio
Partner
Head of Intellectual Property and Technology, Italy
T +39 02 80 618 1
giulio.coraggio@dlapiper.com

Gualtiero Dragotti
Partner
Global Co-Chair, Patent Group
T +39 02 80 618 1
gualtiero.dragotti@dlapiper.com

Alessandro Ferrari
Partner
Head of Technology Sector, Italy
T +39 02 80 618 1
alessandro.ferrari@dlapiper.com

Roberto Valenti
Partner
Head of Life Sciences Sector, Italy
T +39 335 73 66 184
roberto.valenti@dlapiper.com

Elena Varese
Partner
Co-Head of Consumer Good, Food and Retail Sector, Italy
T +39 02 80 618 1
elena.varese@dlapiper.com

Ginevra Righini
Partner
T +39 02 80 61 863 4
ginevra.righini@dlapiper.com

Marco de Morpurgo
Partner
Global Co-Chair, Life Sciences
T +39 06 68 880 1
marco.demorpurgo@dlapiper.com

Alessandro Boso Caretta
Partner
T +39 06 68 880 1
alessandro.bosocaretta@dlapiper.com

dlapiper.com