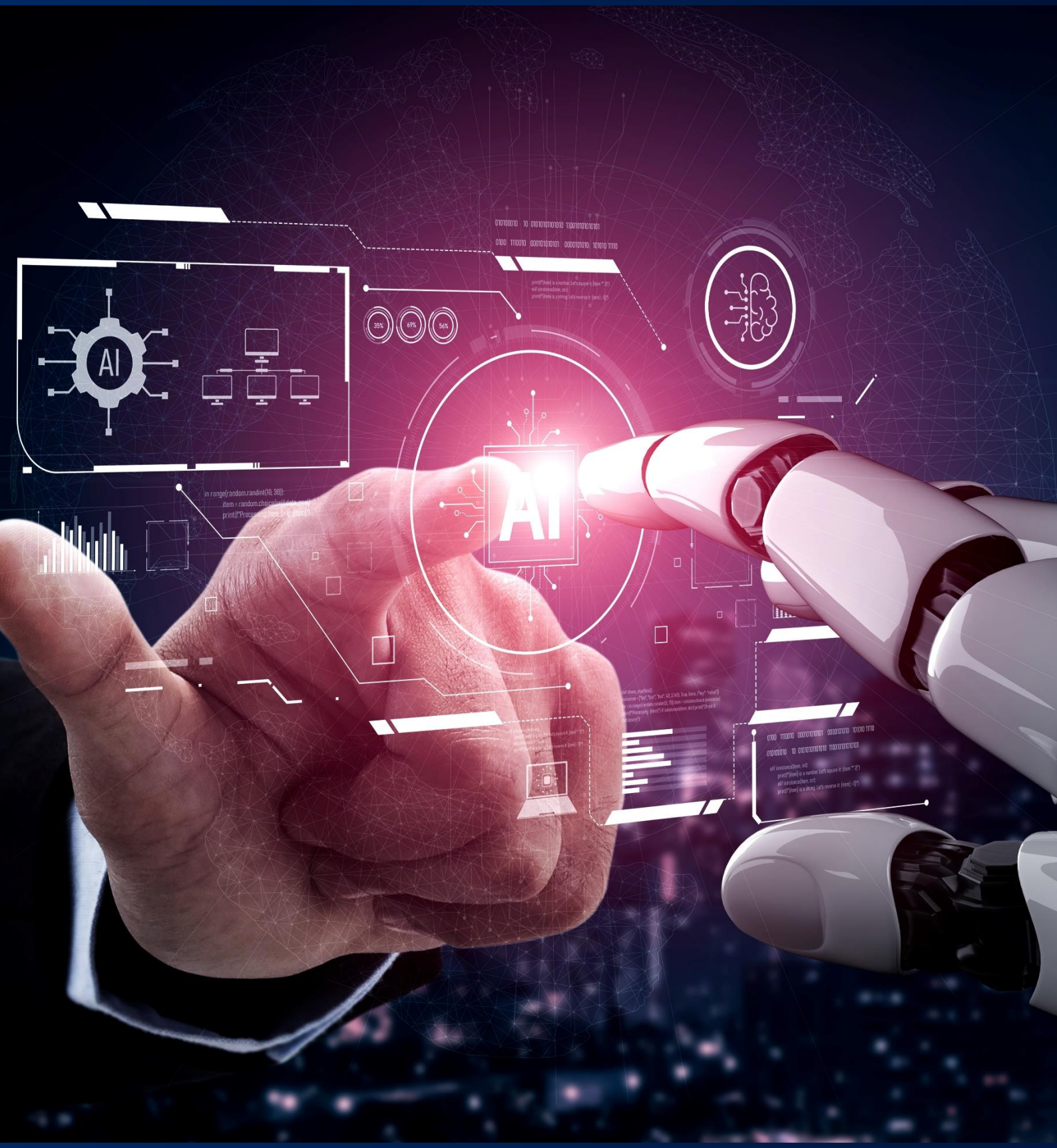
KYRIAKIDES GEORGOPOULOS
LAW FIRM



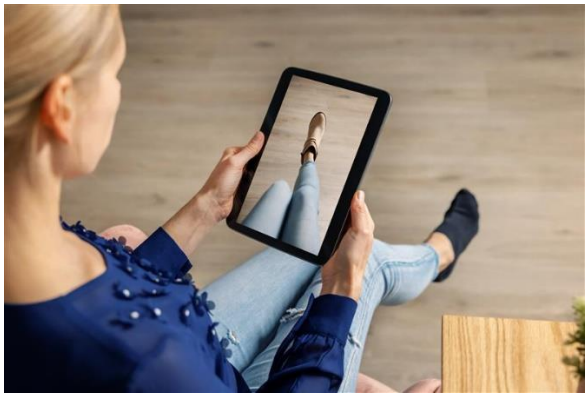
DATA PRIVACY, CYBERSECURITY & TECHNOLOGY LAW

Legal Insights on Virtual Try-On AI-Based Systems under the AI Act *(Regulation (EU) 2024/1689)*

November 26, 2025

Legal Insights on Virtual Try-On AI-Based Systems under the AI Act *(Regulation (EU) 2024/1689)*

BY VICTORIA MERTIKOPOULOU, ELECTRA RETZIKA



1. Virtual Try-On systems (VTOs)

Virtual Try-On systems (VTOs), which skyrocketed in popularity during the COVID-19 pandemic, allow consumers to virtually "try on" fashion and beauty products —namely cosmetics, jewelry, apparel, and footwear— on their own bodies, as well as to receive skin analysis and product recommendations, through the sophisticated interplay of artificial intelligence (AI), augmented reality (AR), and computer vision. In simple terms, shoppers first select the products they want to virtually try on. The system then uses a photo or a video of the shopper —either uploaded or captured in real time— to collect data such as body shape and facial features, and accurately places the selected product on the shopper's face or body.

2. Definition of AI Systems

According to Article 3(1) of the AI Act, an AI system is *"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"*.

3. The obligations and the risk-based approach of the AI Act

The obligations set out in the AI Act differ depending on whether the entity is a Provider *[Article 3(3)]* or a Deployer *[Article 3(4)]*, as well as on the risk level of the AI system in question.

With respect to **Providers**, the AI Act applies to:
- Providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether they are established or located within the Union or in a third country *[Article 2(1)(a)]*;
- Providers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union *[Article 2(1)(c)]*.

With respect to **Deployers**, the AI Act applies to:
- Deployers of AI systems that have their place of establishment or are located within the Union *[Article 2(1)(b)]*;
- Deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union *[Article 2(1)(c)]*.

The AI Act follows a risk-based approach, which so far has been found to be challenging to interpret. According to this approach, AI systems have been categorized into four risk categories:

(a) unacceptable risk (prohibited AI practices);

(b) high risk (high-risk AI systems, as listed in Article 6 and Annex III of the AI Act);
(c) limited risk (AI systems with specific transparency obligations);
(d) minimal and/or no risk (all other AI systems for which the AI Act does not introduce specific rules).

4. Biometric Data

Exacerbating the multitude of definitional frameworks on biometric data, the AI Act *[Article 3 (34)]* includes under the biometric umbrella *"personal data resulting from specific technical processing related to the physical, physiological, or behavioral characteristics of a natural person, such as facial images or dactyloscopic data".*

5. Assessment of Virtual Try-On AI-Based Systems under *"High-Risk AI Systems" and "Prohibited AI Practices"*

Data collected by Virtual Try-On AI-Based systems — such as skin characteristics (*type, tone, and conditions)* and eye tracking data *(eye color, pupil dilation, gaze patterns, blink rates, and saccadic eye movements)*, which can lead to conclusions—whether accurate or not—about a user's age, gender, race, or medical conditions (e.g. diagnosing ADHD, autism, and schizophrenia), as well as facial geometry, shapes and measurements of facial features (e.g., eye distance, nose length, jaw shape), head movement, facial muscle activity, hair color, body shape and size —can theoretically be combined to create a unique user profile.

- **Under the lens of *"High-Risk AI Systems"***

  If the body and facial images, along with the biometric data collected by such systems, were to be used for identification or categorization purposes, these systems could potentially be classified as *"high-risk"* under the AI Act. Based on current data, these systems have not, so far, been used for identification or categorization purposes and would not, at present, be classified as *"high-risk"*, while leaving open the possibility that future uses for such purposes could alter this assessment.

  It should be noted that even if a customer's biometric data collected by a Virtual Try-On AI-based system is not initially matched against a reference database —at least not one containing identifiable individuals— nothing prevents a brand from storing such biometric data in a database and subsequently comparing newly captured biometric data against data recorded at an earlier point in time. Such comparisons could, among others, reveal changes, for example in a customer's body measurements, or indicate whether the same individual is interacting with the system over time, and thereby amounting to a form of tracking. In other words, even without an external reference database, the system could potentially "identify" a returning user by comparing newly captured biometric data with previously stored data.

  This scenario also raises additional risks: **first**, the risk that such user-provided data could be shared with third parties —such as advertisers, analytics firms, or other external entities— for the purpose of targeted advertising, without appropriate safeguards; and **second**, the risk of data breaches, which, due to the sensitivity of the data, are likely to have a significant impact on data subjects. In the context of Virtual Try-On AI-Based Systems, the significance of these risks is amplified by the fact that these systems process detailed visual data containing biometric identifiers or other physical characteristics that may enable the identification of individuals. A security incident affecting such data would therefore not only constitute a loss of confidentiality but could also facilitate unlawful further processing of the data, identity misuse, profiling, or re-purposing for incompatible purposes, thereby posing a

significant risk to the rights and freedoms of data subjects.

- **Under the lens of *"Prohibited AI Practices"***

  Virtual Try-On AI-Based Systems are unlikely to fall within the scope of *"Prohibited AI Practices"* as defined in Article 5 of the AI Act. In particular, with respect to Article 5 (1)(g) of the AI Act, as follows from recital 16 of the AI Act and the relevant Guidelines published by the Commission[1], filters categorizing facial or bodily features used on online marketplaces to allow consumers to preview products on themselves, typically constitute an ancillary feature, as they are used solely in connection with the principal service, which consists of selling the products, and their use is therefore permissible under Article 5 (1)(g) of the AI Act. On the contrary, if Virtual Try-On AI-based systems were to function as biometric categorization systems capable of deducing, for example, an individual's religious orientation from their tattoos or facial features, they would fall within the scope of prohibited AI practices under Article 5 (1)(g) of the AI Act.

6. Deployers' obligations under Article 26 of the AI Act

Deployers of high-risk AI systems, in addition to transparency and accountability obligations, face an additional layer of compliance obligations, primarily under Article 26 of the AI Act. Some of the key obligations under this article include:

- Taking appropriate technical and organizational measures to ensure that AI systems are used in accordance with the instructions for use accompanying them;
- Assigning human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;
- Ensuring (to the extent the deployer exercises control over the input data) that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;
- Monitoring the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72 of the AI Act. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident.
- Keeping the logs automatically generated by the high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in applicable Union or national law, in particular in Union law on the protection of personal data.
- Cooperating with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement the AI Act.

[1] Commission has published *"Guidelines on prohibited artificial intelligence (AI) practices"*, available at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

Shifting attention to VTOs, even though robust security fortresses are built around them, should these systems be classified as "high-risk" under the criteria set out in the AI Act, their deployers would be required to comply with the aforementioned obligations. At the same time, irrespective of any high-risk classification, their deployers must at all times comply with data protection obligations, and even more so in cases where biometric data is processed. In particular, deployers should pay attention to:

- **Preventing Black Box Operations:** Taking measures to ensure that the system is not functioning as a "black box," meaning a situation in which consumers are unable to understand how the fit analysis was performed and what type of data was collected to produce the outcome,
- **Establishing and communicating a clear Policy:** Stating the purposes for which identification or categorization based on biometric data is performed, where relevant, ensuring compliance with the patchwork of privacy laws, and stipulating that obtaining explicit purpose-specific consent from the individual concerned is required, in the manner prescribed by law, to process biometric data.

7. EU's Digital Omnibus

On 19.11.2025, the European Commission officially unveiled its Digital Omnibus —a broader package of measures intended to simplify digital regulation and support innovation across the EU economy— confirming sweeping adjustments to the EU's digital rulebook.

One of the most notable changes arising from the Digital Omnibus is the postponement of rules for high-risk AI systems. The Commission proposes linking the full application of "high-risk" AI rules to the adoption of harmonized standards, common specifications or guidance. **For Annex III systems, the rules would apply six months after a Commission decision on standards, but no later than December 2027. For Annex I systems, the deadline would be 12 months after that decision, or by August 2028 at the latest.**

While the package signals a clear direction, these are not yet binding changes, until the Digital Omnibus is fully adopted and enters into force.

The Commission states that support tools — such as standards, technical specifications and guidelines — are not yet sufficiently mature, and emphasizes the need for businesses to have more time to adapt during the period in which the EU simplifies overlapping rules on data, cybersecurity and AI.

The Digital Omnibus arguably, however, represents more than a technical adjustment. It reflects a broader recalibration of priorities.

8. Conclusion

In light of the foregoing, consumers are already asking: *"Can I try something on without contributing to a training dataset? Can I preview a look without being profiled?"* These are no longer hypothetical questions. Virtual Try-On AI-Based systems have opened a legal Pandora's box, and solutions must be found promptly, before AI becomes not just a stylist, but also a gatekeeper. In this context, given that technology often moves faster than the legislative process, the principles of proportionality and legitimacy should always serve as the guiding framework in an AI-driven world, whereas responsibility to ensure that systems are used in a transparent and ethical manner on the basis of the AI Act must be taken into account.

Contact Us

Victoria Mertikopoulou
PARTNER
v.mertikopoulou@kglawfirm.gr

Follow Us

ATHENS OFFICE

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
E kg.law@kglawfirm.gr

THESSALONIKI OFFICE

31, Politechniou Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr

www.kglawfirm.gr