Biometric Verification Systems in Ride-Hailing and Delivery Platforms:

A Critical Analysis of the EU AI ACT's Exclusion from the HIGH-RISK CLASSIFICATION

Maha Omar Abdelnabi Omar Elsayed

[1] PhD Candidate, Civil Law Department, Faculty of Law, Ain Shams University, Cairo, Egypt
[2] Research Visitor, Department of Innovation and Digitalisation in Law, Vienna University
mahaomar195@outlook.com

Abstract. This paper argues that the blanket exclusion of biometric verification systems from the scope of high-risk AI under point 1 (a) of Annex III of the AI Act is unjustified in the context of platform work. In ride-hailing and delivery courier services, facial recognition technologies, used solely or coupled with other algorithmic tools, affect the workers' livelihood and trigger violations of their data protection rights. This Exclusion lies on the assumption that the impact of these systems on the persons subjected to it is minimal. An assumption that this paper challenges on four grounds: the inherent sensitivity of biometric data regardless of its use in verification or identification, the precarious nature of platform work, the divergence between the provider's intended purpose and the deployer's actual use, and the contribution of these systems in algorithmic management. This paper further demonstrates the Exclusion's implication, depriving BVS of heightened regulation exclusively triggered for high-risk AI. Especially, the provider-level obligations provided for in articles 43 (1), 13, and 14 of the Act.

Keywords: Biometric Verification Systems, Facial Recognition Technologies - High-Risk AI, Algorithmic Management, Ride-hailing – Delivery Couriers – Intended Purpose – Actual Use - Biometric Data – Sensitive Data – Data Processing - Precarious Work – Platform Work – Powers Asymmetry – Managerial Prerogatives

1 Introduction and Context

Ride-hailing platforms and delivery courier platforms **("Platforms")**, as digital labour platforms, operate as data-intensive businesses whose models depend on continuous collection and processing of personal data from their users. Uber, Ola, Didi, Lyft, Glovo

and Deliveroo, among others, collect and process their drivers' and couriers' **("Workers")** data through biometric verification systems **("BVS")**, especially facial recognition technologies **("FRT")**.[1] The latter is a two-step verification process that, first, collects facial images and creates a template which it then compares with other templates to recognize a person.[2] Platforms confirm their use of the system is to confirm a Worker is who they claim to be by comparing a selfie the latter willingly submits to another they previously uploaded, or their profile photo.[3] An alleged typical authentication verification,[4] arguably used to enhance the safety of using their app by preventing account sharing between drivers and combating fraud.[5]

Nevertheless, BVS cause significant risks to the health, safety, or fundamental human rights of the workers[6], especially if the processing of biometrics, as a special category of personal data, is in the context of precarious digital platform work.[7] The deployment of BVS in platform work triggers fundamental rights protection, including human dignity, right to privacy, and personal data protection, as well as non-discrimination, provided for in articles 1, 7, 8, and 21 of the EU Charter respectively. For instance, in Bărbulescu *v.* Romania, the European Court of Human Rights interpreted the protection of privacy to include the protection of individuals at workplace, and reiterated that Any interference with workers' rights shall be prescribed by law, pursuant a legitimate aim, and necessary in a democratic society in the sense that the measure imposed was the least intrusive means workplace monitoring, even if pursuing a legitimate aim, must be strictly necessary and proportionate.[8] Fundamental rights implications of algorithmic management and biometric

---

[1] *Hießl, C. (2025). Case law on algorithmic management at the workplace: Cross-European comparative analysis and tentative conclusions. SSRN*, p. 41.

[2] European Data Protection Board. (2023). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Version 2.0, adopted 26 April 2023). EDPB, p. 9.

[3] Uber. (n.d.). *How does Uber verify my identity*? Uber Help. Last visited on the 23rd of July, 2026.

[4] EDPB, Guidelines 05/2022 (Version 2.0, 2023), p. 9.

[5] Uber. (n.d.). *How does Uber verify my identity*? Uber Help. Last visited on the 23rd of July, 2026. See also, Hießl, C. (2025), p. 58.

[6] 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), 2016 O.J. (L 119) 1, GDPR, Recital (51).

[7] Dubal, V. (2017). Wage slave or entrepreneur? Contesting the dualism of legal worker identities. *California Law Review, 105*, 103. https://doi.org/10.15779/Z38M84X., P. 103.

[8] Bărbulescu v. Romania [GC], App. No. 61496/08, 5 September 2017. In this case, the ECHR examined whether the State, in the context of its positive obligations, had struck a fair balance between the applicant's right to respect for his private life and correspondence and his employer's interests. held that there is no violation of the applicant's, a sales engineer in a private company, right to privacy (art. 8.1. – Respect for Correspondence & private life) for monitoring the applicant's use of the internet at his work place, and for using the collected data as a ground justifying his dismissal. In this regard, he court held that the employer's monitoring had been limited in scope and proportionate as, apart from the communications on yahoo messenger account, no data stored on the emloyee's computer were examined.

surveillance are extensively discussed by existing scholarship,[9] and fall outside the scope of the present article.

The FRT's reliability, efficiency, and overall issue of quality and accuracy of the source data and the results of processing, regardless of whether the system is used for biometric verification or identification purposes, are often challenged.[10] BVS, including facial recognition, raise concerns of discrimination due to false results when used at a large scale,[11] and if trained on biased data.[12] Facial recognition verification systems are reported to have a higher error rate in confirming the identity of people with darker skin tones,[13] contributing therefore to indirect discrimination against certain categories of platform workers.[14]

In Manjang v. Uber Eats,[15] Manjang, a black courier working for Uber Eats, claimed to have been subjected to indirect racial discrimination[16] after repeatedly being asked to undergo several facial recognition verifications before having his account on Uber Eats deactivated due to a continued mismatch.[17] Manjang's data collected by the platform were obtained through an access request prove that the submitted selfies were of him.[18] Civil society organizations supporting Manjang[19] in his case against the platform expressed their concern over the latter's dismissal and deprivation of income due to a false negative.[20]

AI systems intended for one purpose but used for another might have harmful effects for the person subjected to it,[21] simply by being used in the context of work.[22]

---

9 De Stefano, V. (2018). "Negotiating the algorithm": Automation, artificial intelligence and labour protection (ILO Employment Working Paper No. 246). International Labour Organization. *See also*, Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. Academy of Management Annals, 14(1), 366–410. As well as, Adams-Prassl, J., Binns, R., & Kelly-Lyth, A. (2023). Regulating algorithmic management: A blueprint. European Labour Law Journal, 14(2), 124–151. And, Cefaliello, A., & Kullmann, M. (2022). Offering false security: How the draft Artificial Intelligence Act undermines fundamental workers' rights. European Labour Law Journal, 13(4), 541–562.

10 EDPB, Guidelines 05/2022 (Version 2.0, 2023), p. 12.

11 EDPB, Guidelines 05/2022 (Version 2.0, 2023), p. 9.

12 Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

13 EDBP (2022), P 9.

14 ACRE. (2025). Driven out by AI: How Uber uses facial recognition to fire drivers. ACRE.

15 Manjang v Uber Eats, Case No. 3206212/2021, East London Employment Tribunal (settled March 2024).

16 Manjang v Uber (Case No. 3206212/2021), 9 July 2022, p. 81.

17 Manjang v Uber (Case No. 3206212/2021), 9 July 2022, p. 51.

18 BBC News. (2024, March 5). Payout for Uber Eats driver over face scan bias case. BBC News.

19 Li, W., & Toh, J. (2023). Data subject rights as a tool for platform worker resistance: Lessons from the Uber/Ola judgments. In H. Matsumi, D. Hallinan, D. Dimitrova, E. Kosta, & P. De Hert (Eds.), Data protection and privacy: In transitional times (pp. 119–156). Hart, P. 38.

20 BBC News (2024).

21 Cefaliello, A., & Kullmann, M. (2022), p. 547., referring to Lin, B. (2021, October 30). Uber patents reveal experiments with predictive algorithms to identify risky drivers. The Intercept.

22 Cristofolini, E. (2024). Navigating the impact of AI systems in the workplace: AI Act loopholes. Italian Labour Law e-Journal, 17(1), 99–118, p. 85.

In the specific context of the Platforms work, the biometric data feeding the verification system initially for authentication purposes is often used for other purposes, or the systems are coupled with another, mostly for a functionality that is a managerial prerogative, constituting or contributing, therefore, to algorithmic management.[23] Algorithmic management, including disciplinary prerogatives, like dismissals,[24] intensifies the challenges faced by platform workers, including lack of transparency, discrimination, and precarity.[25]

Foodinho, a subsidiary of Glovo, uses Jumio FRT, which resulted in the couriers' account deactivation, or the account may still be active but the courier will not be able to book any delivery slots, if failing to identify them, or if the latter refuses to comply with it.[26]

On the basis that BVS, (one-to-one), are solely used to confirm identities,[27] and the assumption that they create minor impact on fundamental rights of the persons subjected to them, compared to the biometric identification systems(one-to-many)[28],[29] the EU Artificial Intelligence Act **(herein "Act" or "Regulation")**[30] differentiates in the regulatory treatment between by classifying the latter as high-risk AI falling under the scope of art. 6 (2) read in conjunction with point 1 (a) of Annex III, but excluding the former from the scope of art. 6 and category of high-risk AI altogether **(herein the "Exclusion")**.

This distinction between both systems is not only blurred, but it is also becoming more and more outdated.[31] It further serves as a basis for covert use of AI systems in platform work whereby the deployers (in this case the Platforms) use BVS intended for verification for other purposes.[32] Systems that escape the heightened regulation of high-risk AI systems by being put on the market and in service (precarious platform work in the context of this article). Particularly, the requirements

---

[23] Adams-Prassl, J., Binns, R., & Kelly-Lyth, A. (2023), p. 126.

[24] De Stefano, V. (2018), p. 9. See also, Kellogg, K. C., Valentine, M. A., & Christin, A. (2020), p. 368.

[25] Li & Toh (2023).

[26] Garante per la Protezione dei Dati Personali. (2024). Ordinanza ingiunzione nei confronti di Foodinho S.r.l. (Glovo) (Provvedimento del 22 novembre 2024, Docweb No. 10074601).

[27] Recital 54 of the EU AI Act defines biometric verification systems as the "*AI systems intended to be used for biometric verification, including authentication, the sole purpose of which is to confirm that a specific natural person is who that person claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secure access to premises"*

[28] Dubal, V. (2025). Data laws at work. The Yale Law Journal Forum, 134, 405–450, p. 426-427.

[29] EU AI Act, Recital (17).

[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689.

[31] Sumer, B. (2024). The AI Act's exclusion of biometric verification: Minimal risk by design and default? European Data Protection Law Review, 10(2), 150–161.

[32] Cefaliello & Kullmann (2022), p. 546, citing IndustrAll Europe's Contribution to the public consultation on the Proposal for an Artificial Intelligence Act (Brussels, 3 August 2021). See also, Hießl, C. (2025), (reporting Garante, Order of 22 November 2024, Foodinho/Glovo, Docweb 10074601).

to opt for independent pre-market conformity assessment (art. 43), and to design an interpretable system allowing effective human oversight (art. 14), allowing for transparency and providing the deployer with the necessary information (art. 13), all due to the Exclusion.

Alongside the AI Act's provisions, this contribution draws on relevant CJEU case law and national data protection authorities' decisions, particularly French and Italian DPAs, to illustrate how the BVS already trigger relevant data protection and fundamental rights issues. Especially since any interpretation of the Act's provisions is still anticipatory of actual application given the fact that no complaints are yet lodged nor decisions rendered under its framework. The Digital Omnibus Regulation's postponement of high-risk obligations until 2 December 2027 further delays the actual testing of these provisions in practice.[33]

The practical implication of this Exclusion in ride-hailing and delivery courier platforms necessitates focusing on the legal issue of this article being whether EU law sufficiently regulates BVS deployed in digital labor platforms characterized by precarity, and provides adequate protection to vulnerable platform workers. In the scope of this article, the most relevant EU instruments to the matter at hand examining the regulation of sensitive data processing in the context of platform work through the means of machine learning algorithms, are the EU AI Act as the AI product safety regulation, the General Data Protection Regulation ("GDPR") as the data protection law, and the Platform Work Directive ("PWD")[34] governing the context of platform work where this automated processing occurs. This contribution acknowledges the importance of addressing the gaps identified herein in light of each of the GDPR[35] and the PWD, and critically examines, herein, whether the AI Act provides sufficient regulation for BVS deployed in the context of platform work, specifically ride-hailing and delivery courier services, and where it defers the examination of the issue in light of the two other instruments to future contributions.

In the below section (2), the article demonstrates that, by excluding the BVS, including authentication, solely purposed to confirm identities from the scope of art. 6 (2) read in conjunction point no. 1 (a) of Annex III on high-risk AI, the Act fails to provide the necessary regulation for the level of significant risk potentially created by the use of BVS in the context of platform work, and specifically ride-hailing and delivery courier service platforms. Consequently, allowing the system's introduction into the market without undergoing necessary scrutiny, and in the absence of necessary design obligations.

---

[33] European Parliament and Council of the European Union. (2026). Digital Omnibus on AI (adopted by Parliament 16 June 2026; Council 29 June 2026; entry into force July 2026, pending OJ publication).

[34] Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work [2024] OJ L 2024/2831.

[35] This contribution does not tackle the fulfilment or not of each of the requirements for a compliant biometric data processing process according to the GDPR. Rather, reference to these requirements throughout the paper is merely to draw on the regulation of data processing, and the application of EU law that provides for heightened protection for sensitive data processing which the Act then classifies as minimum or low-risk AI system.

2 The Exclusion - A Leeway from High-Risk AI Heightened Requirements

The Act is a cross-sector product safety regulation[36] addressing the providers and the users of the AI systems rather than the persons that may be subjected to them.[37] It is not specifically designed to govern the impact of AI use in the context of work and employment. Therefore, even though the Act classifies some AI systems as high-risk systems and provides heightened requirements for them, the determination of the level of risk attributed to certain systems and their classification, it does not sufficiently account for the asymmetries in power and information in the context of work. The Act, therefore, fails to provide a framework for rights and redress to empower persons potentially affected by the AI systems; in this context, the workers.[38]

In examining whether the Act sufficiently regulates AI systems used in platform work, specifically ride-hailing and delivery courier, this section argues, on three main pillars, that the Exclusion from the classification of high-risk AI provided for in Art. 6 (2) read in conjunction with point no. 1 (a) of Annex III of the Act, and its attached heightened requirement, the AI Act does not provide sufficient protection for the ride-hailing and delivery courier services, as platform workers. This is since the Act *(i)* imposes a blanket exclusion on BVS from the scope of AI systems, regardless of the sensitivity of the data processed and the precarious nature of platform work, and by (*ii)* failing to account for the misalignment of the actual purpose of use by the deployer from the intended purpose of the system set by the provider, and by *(iii)* failing to consider the practice where BVS are never solely used in work platform, rather they are often coupled with another for managerial prerogative functionalities.

Unlike with biometric identification systems, the Act explicitly excludes BVS from the classification of high-risk AI provided for in Art. 6 (2) read in conjunction with point 1 (a) of Annex III. Consequently, the heightened requirements imposed on providers and deployers of high-risk AI are not triggered by those systems.[39] Point 1 (a) of Annex III of the Act stipulates: *"High-risk AI systems pursuant to article 6 (2) are […] 1. Biometrics, […] (a) remote biometric identification systems. This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be"*.

By the Exclusion, the Act decontextualizes the use of BVS, and determines the same level of risk to systems rather used in a spectrum of contexts and functionality varying from authentication merely allowing a person to access a device or access a platform to more delicate contexts such as digital labor platform work, generally,

---

[36] Cristofolini (2024), p. 79.

[37] Li & Toh (2022), at page 37

[38] Cristofolini (2024), p. 79.

[39] The Act, Annex III, 1(a) and recital 54. Recital 54 states that: "*[…] the sole purpose to enable access to a service, unlocking a device, or having secure access to premises* […]*"*

and ride-hailing and delivery services, specifically, where BVS is incomparable to allowing access to a device. Rather, it may determine access to income, and the livelihood of platform workers depends on it. Contexts that merit different levels of protection and, consequently, must not be equally disqualified from the classification of high-risk AI systems. Furthermore, the Act completely ignores the fact that, in the context of platform work, these systems, even when BVSs are solely used for authentication and regardless of any further implications of the use of such a system might have on decision-making processes against workers, these systems still process sensitive data of vulnerable workers in a precarious work environment. Therefore, I argue that BVS used in ride-hailing and delivery services constitute high-risk AI systems, and shall consequently benefit from the heightened requirements imposed by the Act for this type of risk. I further argue that the basis on which the Regulation bases the Exclusion (Sole use of identity confirmation, and Intended Purpose) is impractical and often inapplicable in the context of platform work.

In doing so, this article demonstrates ***(1)*** biometric verification systems based on the processing of sensitive data in ***(2)*** the precarious context of platform work could create significant risk, and shall therefore be treated as high-risk AI systems, even if they are merely used for confirmation of identity in this specific context of employment. Furthermore, in the context of platform work, ***(3)*** BVS are rarely solely used for confirmation of identity, rather, it is more probable to be used by the employer coupled with another purpose of management, proving therefore that ***(4)*** the actual use of AI systems often deviates from its intended purpose.

2.1 Biometric Verification Systems Inherently Based On Sensitive Data Processing Creates Significant Risk

EU law[40] and case law,[41] in context of data protection and platform work, confirm that biometric data are sensitive data[42] only allowed to be used under strict legal and regulatory bases. In this regard, processing revealing biometric data is prohibited unless the worker's explicit consent is obtained, or there is an employment necessity, and a

[40] The AI Act application is still predictive and anticipatory, examples from the application of GDPR, as the data protection law, are relevant, where I am deriving principles to highlight the significance of biometric data use in a general manner. Furthermore, the EU AI is not a stand-alone regulation and shall be perceived in light of other EU instruments.

[41] Commission Nationale de l'Informatique et des Libertés. (2024). Employee monitoring: CNIL fined Amazon France Logistique €32 million (Deliberation No. SAN-2023-021, 27 December 2023). . See also, Garante per la Protezione dei Dati Personali. (2021). Ordinanza ingiunzione nei confronti di Foodinho S.r.l. (Glovo) (Order No. 234, 10 June 2021, Docweb No. 9675440). And, Garante, Order of 22 November 2024, Foodinho S.r.l. (Glovo) (Docweb 10074601). And,

[42] GDPR, Art. 9 and recital 51.

legal basis for the processing of biometric data,[43] including data of physical characteristics of a natural person which allows or confirms the unique identification of that natural person, such as facial images.[44] Furthermore, processing of photographs is treated, under EU law, as processing of special categories of personal data when it is made through specific technical means allowing the unique identification or authentication of a natural person.[45]

Furthermore, in all cases decided by European data protection authorities in Italy, France, and Germany, in the context of ride-hailing and delivery platforms, the authorities found that the data collection and storage for purpose of algorithmic processing is excessive and unjustifiably intrusive.[46]Therefore, as an indicator on the level of risk the processing of such data might pose. Unlike the Act's assumption that BVS are of minor impact on the affected subjects, these DPAs decisions signifies the weight the authorities give to the processing of personal data, even when the purpose is mere authentication.

In the 2024 Italian DPA Glovo decision,[47] it was decided that[48] the use of an invasive tool of facial recognition that requires storing sensitive biometric data is contrary to the principles of data minimization and proportionality provided for in Article 5 of the GDPR,[49] in the event where the company does not bring evidence that the less intrusive means are less effective of identity control for access to workplace, such as checking badges and registration.[50] The Italian DPA further stated that the facial recognition software had very low reliability rate in a way that made it possible to circumvent it, which occurred in actual cases of fraud, and led to many other incidents were the drivers were incorrectly accused of attempting to fraud

---

43 GDPR, art. 9 "Processing of special categories of personal data".

44 EU AI Act, Recital 14, whereby the Act adopts the GDPR definition of biometric data provided for in art. 4 (14) of the GDPR defines biometric data as *"personal data resulting from specific technical processing relating to the physical, physio logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic",*

45 GDPR, recital 51.

46 Hießl, C. (2025), p. 41

47 Garante, Order of 22 November 2024, Foodinho S.r.l. (Glovo) (Docweb 10074601). See also CNIL, Deliberation No. SAN-2023-021 of 27 December 2023, Amazon France Logistique. Where the DPAs confirm that biometric data processing should be proportionate, and minimalized.

48 Garante, Order of 22 November 2024, Foodinho S.r.l. (Glovo) (Docweb 10074601).

49 Similarly, in cases like Amazon France, the French DPA cautiously deciding on the duration of biometric data storage finding that it should be further reduced to 7 days, and prohibited the constant collection of data which it deemed intrusive and in light of the purpose indicated by the company. See, CNIL, Deliberation No. SAN-2023-021 of 27 December 2023, Amazon France Logistique

50 Hießl, C. (2025), p. 26-27 (reporting Garante per la Protezione dei Dati Personali. (2024). Provvedimento del 22 febbraio 2024 nei confronti di L'Igiene Urbana Evolution S.r.l. (Docweb No. 9995680). See also, Hießl, C. (2025), p. 41 (reporting Garante, Provvedimento del 22 febbraio 2024, L'Igiene Urbana Evolution (Docweb 9995680).

the system.[51] In this regard, the authority found that the unreliability of the mechanism is an additional reason of making its use even more unacceptable to use the system.[52]

This confirms that the collection and processing of biometric data is inherently intrusive and that BVS is intrinsically based on sensitive data processing, which is only conditionally allowed under the European law, and surrounded by a whole set of requirements that indicate a high-level of risk which the exclusion of the AI Act does not consider nor align with by excluding biometric data solely used for identity confirmation broadly speaking from the scope of high-risk, and regardless of the nature of the processed data as presented herein, as well as the precarity of platform work as presented hereafter.

2.2 Biometric Verification Systems in Precarious Platform Work Merits High-Risk AI Classification

The context in which BVS are used should also be considered in the determination on the level of risk it poses. In the context of platform work generally, such systems automatically deviate away from the limited and/or low levels of risk, let alone ride-hailing and delivery services as part of platform work, specifically, where the drivers' and couriers' work security and identify safety are diluted due to the precarious nature of work in digital platform.[53] In this regard, the processing of personal data in contexts that are by nature sensitive may create significant risks to fundamental human rights and freedoms and merits specific protection since their processing.[54] European courts emphasize on the fact that employment context creates structural vulnerabilities[55] of social, economic and psychological nature in the workplace.[56] Power imbalance in the context of work (broadly perceived beyond the limitation of the existence of an employment contract[57]), is a barrier to the worker's explicit expression of consent to the

---

[51] Hießl, C. (2025), p. 33 (reporting Garante, Order of 22 November 2024, Foodinho/Glovo, Docweb 10074601).

[52] Hießl, C. (2025), p. 29 (reporting Garante, Order of 22 November 2024, Foodinho/Glovo, Docweb 10074601).

[53] Dubal, V. (2017). Wage slave or entrepreneur? Contesting the dualism of legal worker identities. *California Law Review*, *105*, 103.

[54] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1, recital 51.

[55] Case C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums, ECLI:EU:C:2023:270 (CJEU, 30 March 2023).

[56] Uber BV v Aslam [2021] UKSC 5, [71], [75].

[57] Case C-34/21, Hauptpersonalrat (CJEU, 30 March 2023), para. 45 and 55 where a broader interpretation of the protection provided for by art. 88 of the GDPR is interpreted by the court. What matters is subordination rather than the existence of an employment contract. Subordination exists in platform work by virtue of algorithmic management. the protection of data subjects for processing in context of work in of traditional work is broadly perceived to protect platform workers as much as employees. Additionally, as

processing of personal data,[58] without experiencing fear and risks of detrimental effects consequential to their refusal of processing.[59]

In the context of ride-hailing and delivery courier's platforms where the latter denounce any employment relationship with the drivers on the basis that the workers willingly choose flexibility of work over work security as self-employed drivers, leaving the drivers with lack of stability and regulatory protection,[60] it is inconvenient to argue that the workers voluntarily and willingly subscribe to facial recognition systems and undergo biometric verification systems.

Garante, the Italian DPA, confirmed that Glovo's processing of the drivers' biometric data by Jumio FRT to verify the identities of the drivers is unlawful. In this regard, when deciding on the seriousness of the breach, the authority took into account the vulnerability of the platform drivers and the nature of the processing by FRT, which entailed data relating to data subjects (the drivers) in a vulnerable position. In this regard, Garante reiterated that this biometric verification system is used in a work context characterized by the significant asymmetry of the powers of the drivers and the platform.[61]

This consideration of the context of platform work and its precarious nature when assessing biometric verification systems negates the AI Act assumption that the BVS is low impact on the affected persons' fundamental rights and signifies that the processing of sensitive data of vulnerable platform workers is intrinsically high-risk, and so should not be excluded from the classification of high-risk AI systems. Not only is the exclusion of the BVS even if used for mere authentication purposes from the scope of high-risk constitutes a blanket exclusion that puts all BVS at the same level and neglects the sensitive nature of biometric data and the context of precarious work in which these systems deployment.

Therefore, firstly, the Act's Exclusion magnifies the risk that the affected persons might be encounter due to being subjected to AI systems have not undergone any heightened requirements before being put in market. Secondly, the biometric verification systems used in the context of platform work generally and ride-hailing and delivery courier specifically shall be re-classified as high-risk systems under Art. 6 (2) in conjunction with point 1 (a) of Annex III.

---

emphasized in the aim of the labor protection is to protect vulnerable workers, the aim of the labor protection is to protect vulnerable workers.

[58] Li & Toh (2022), at page 36. Furthermore, With the GDPR Consent requirement to collect or process data, is not possible in the context of employment or even worker relationship. In other words, the contract of employment is still based on the mutual and, therefore, bilateral consent of the parties at the moment of its conclusion, since workers have to freely accept to enter into the contract. Once the contract is in force, however, they are subject to the unilateral prerogatives of employers, who no longer need their consent to direct, supervise and discipline their work performance, within the limits of what is reasonable and lawful under the given contractual and legal system. See, in this regard, De Stefano (2018), p. 14.

[59] Article 29 Data Protection Working Party. (2018). Guidelines on consent under Regulation 2016/679 (WP259 rev.01, adopted 10 April 2018)..

[60] Dubal, V. (2017). Wage slave or entrepreneur? Contesting the dualism of legal worker identities. California Law Review, 105, 105..

[61] Garante, Order of 22 November 2024, Foodinho S.r.l. (Glovo) (Docweb 10074601).

Furthermore, not only that the Act wrongfully exclude BVS from the scope of high-risk as presented above, but the Act's misclassification of these systems based on its own definition of BVS is incorrect. This is because the definition itself is flawed and narrows the scope of protection from high-risk AI systems by adding components and criteria that would allow for the exclusion of many biometric verification systems where just at the face of it, it seems that they fulfil these criteria many of the systems are included. In the following part of the article, this contribution demonstrates that the "intended purpose" criterion, and the assumption that BVS could be, in any context, solely used for authentication, are two inconvenient criteria included in the definition of BVS and leading to less inclusion of BVS which the intended purpose alter in the value chain of the system, and when the systems are intended for sole use of authentication but are actually not used merely for it.

2.3 BVS in Ride-Hailing and Delivery Services: Intended v. Actual Purpose

The Act's Exclusion from the scope of high-risk AI systems based on the intended purpose of use is a narrow perspective in identifying the level of risk potentially created by a system. This is because on the one hand, only the provider's intended purpose, determined at the time of the systems development is considered in the identification of the level of risk even though the deployer's actual use in the context of platform work might differ from the intended purpose. In this regard, the "intended purpose", on one hand, is defined by Article 3 (12) of the Act as *"the use for which an AI system in intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation."*.

On the other hand, the actual use of an AI system, in the context and for the purposes of this article, means the purpose which the deployer, rather than the provider, intends to use the AI system for, either as a stand-alone AI tool or as part of a more complex system, and regardless of whether the deployer had initially planned to use the AI system for a purpose or in a context other than those defined by the deployer. This actual purpose could also refer to the change in purpose that the deployer make at some point during the deployment phase by using the system for other than it is originally intended for. In any of these scenarios, an AI system developed for a purpose and used for another might have harmful effects on the person subjected to it simply by being used in the workplaces, for instance, if used for monitoring purposes.[62]

Business practices in platform work include incident of differences between the intended purpose and the actual purpose of use of AI systems.[63] Automated systems used in workplaces collect data from workers, and feed machine learning algorithms which then make hiring calls, determines pay, influence behavior, among

[62] Cristofolini (2024), p. 85.

[63] Cefaliello & Kullmann (2022), p. 547.

other uses.[64] Microsoft Face API is intended to support societal benefits. In the specific context of Uber Real Time ID checks, Microsoft said that it is intended to increase rider and drivers security[65] The contexts mentioned in these AI systems the technical documents refer to cases such client onboarding and KYC, access control, and fraud prevention. Employment and/or work are not mentioned in the intended purposes of these systems, the purpose is still general enough to allow the use in such contexts. However, these systems are not necessarily designed with the context of employment considered, meaning that the particularities of platform work are not accounted for while developing the systems.

Platforms, such as Uber, Deliveroo, and Glove rely on biometric verification AI systems such as Microsoft Azure face, or Jumio, respectively, where their developers' intended purposes for them systems is identity verification purposes.[66] Glovo's use of Jumio FRT eventually, if failing to identify the courier or if the latter refuses to comply with it, lead to the courier's account deactivation, or the account may still be active but the courier will not be able to book any delivery slots.[67] For these reasons, I further argue that in the ride hailing and delivery courier services, the platform usually deviates from the intended purpose of the AI system.

This definition of the "intended purpose" and its attachment to the provider is narrowing down the scope of purposes of the AI systems. By considering only the provider's intended purpose at the time of the development of the systems, the Act negates the fact that the user of the system might have a distinct use for it, at the deployment stage. In this sense, the provider's intended purpose for the BVS could be the mere confirmation of identities, while the deployer's actual use may not align with it. Yet, the system won't trigger the heightened requirements imposed by the Act for high-risk AI systems since, as per its intended purpose identified by the provider at the pre-use stage, it is not a high-risk AI.[68]

Consequently, even though Art. 25 of the Act provides for the shift of the high-risk AI attached obligations from the provider to the deployer where the latter uses the system for a purpose other than intended by the former,[69] it depends on the new

---

64 Dubal, V. (2023). On algorithmic wage discrimination. Columbia Law Review, 123(7), 1907–1980, p. 2.

65 Microsoft, Letter to the App Drivers & Couriers Union and Worker Info Exchange (22 April 2021), cited in Worker Info Exchange. (2021). Managed by bots: Software automation, surveillance and management of drivers at Uber. Worker Info Exchange.

66 In jurisdictions other than in the EU, incidents of using the AI system for purpose other than that intended by the provider after putting the system on the market or in service also exist in the context of ride-hailing services. in the United States, Uber deployed in its platform an AI systems intended to predict safety incidents, and the likelihood of involvement in road accidents; the system was used to perform managerial prerogatives by sanctioning the drivers based on the results of the system initially developed for safety purposes. In this regard, please see: Cefaliello & Kullmann (2022), p. 547, citing Lin (2021).

67 Garante, Order of 22 November 2024, Foodinho S.r.l. (Glovo) (Docweb 10074601).

68 Cefaliello & Kullmann (2022), p. 547.

69 EU AI Act, Art. 25: "Responsibilities along the AI Value Chain", stipulates that *"Any […] deployer or third party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under art. 16, in any of the following circumstances […] (c) they modify the intended purpose of an AI system, including a general purpose AI system, which*

provider's own initiative not only to declare that an AI system as becoming high-risk due to their use, but also to self-declare themselves as AI system providers. This is despite the fact that, since the system is originally not a high-risk system, the deployer is under no regulatory obligation to report their use of the non-high-risk system neither to the initial provider, nor to the market surveillance authority. Even though the Act requires the initial system provider to "cooperate" with the new provider in assuming the relevant high-risk requirements by making available the necessary information among other assistance to help the latter assume the liabilities of the provider.[70] There remains a gap on how would the unintended use of the non-high risk AI system be disclosed if the deployer, who is supposed to become the new provider, does not proactively disclose it.[71] Especially with the post-market monitoring, information sharing and market surveillance obligations only dedicated to high-risk AI systems by virtue of chapter IX of the Act.[72]

Even market surveillance authorities capacity, provided for in Art. 79 of the Regulation, to carry out evaluation for an AI system, even if it is not high-risk AI, when it has sufficient reasons to consider that this system presents risk(s) to the health or safety, or to fundamental rights, of persons as defined by Art. 3 (19)[73] of the EU Regulation (EU) 2019/1020,[74] remains an insufficient safeguard against the covert

---

has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Art. 6.".

[70] EU AI Act, Article 25: *"[…] Where the circumstances referred to in paragraph 1 occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation.".*

[71] Aside from the gap in the AI Act presented in this paragraph, the deployer use of an AI system might be revealed, if not willingly disclosed, in light of contractual obligations between the deployer and the provider. However, this remains a contractual rather than a regulatory approach to filling the gap, which, should not be the only resort where the altered use of AI systems from their intended purposes might cause significant risks to the affected persons.

[72] EU AI Act, Art. 71 & 72 "Post Marker monitoring, as well as Art. 73 "Sharing information on serious incidents.

[73] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L 169/1, Art. 3 defines "Product Presenting a Risk" as: "(19) *"a product having the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements."*

[74] Regulation (EU) 2019/1020 (Market Surveillance Regulation).

alteration of intended purpose. This is because mainly it requires the existence of sufficient reasons which would initially drive the authority to consider that the system presents risks and starts investigating.[75]

It may be argued, however, that in the context of ride hailing and delivery services specifically, there might be indicators that could draw the attention of the authorities given the fact that BVS used in these platforms already pose other regulatory issues, such as privacy and data protection issues, under other EU instruments, such as the GDPR, and is already examined by European DPAs. While this might enable the enforcement of Art. 79 of the Act, it remains a collateral incident triggered by the authorities' examination or decision on other matters. Alternatively, it could be argued that the workers themselves or civil society organizations, as natural or legal persons, could bring it to the attention of the authorities by exercising the right to lodge complaints where they have grounds to consider that is an infringement of the Act, as provided for in Art. 85 of the Regulation.

Therefore, deployers of AI systems who are using a certain non-high risk AI system might continue to use it for their own intended purposes covertly to avoid assuming the provider liability and operate the system without undertaking the burden of complying with the heightened requirements that the Act imposes for high-risk AI systems. For instance, for most relevance to the context of platform work and ride-hailing services, the new providers would delay assuming provider's obligations to avoid informing the workers and their representatives before deploying a high-risk AI system in workplaces.[76]

That said, the limitations of the "intended purpose" in the identification of the BVS level of risk and the non-consideration of the deployer's intent negates the fact that actual purposes need to be extensively aligned with the intended purpose from the early development stage. The Act's regulation of the deviation of purpose by imposing the capacity of the provider on the deployer altering the purpose is also insufficient since there are no mechanisms to reveal the deviation of the actual use of the system from the intended purpose for the non-high risk AI systems.

In this regard, it can be both said that 1. The intended purpose required by the Act to be determined by the provider at the time of the development of the system, and that on the basis of which the product's risks are assessed before being put into market, is neglecting the deviation of purpose by the system deployer. 2. While the intended purpose of use has been authentication, the actual use has surpassed

[75] The Market Surveillance Authority's capacity to carry out an evaluation of an AI system where it has sufficient reasons to consider that an AI system classified by the provider as non-high risk in application of Annex III is, indeed, high-risk provided for by Article 80 (1) of the EU AI Act,[75] is not applicable to biometric verification systems since it is on the basis of art. 6 (3) whereby the Act provides for the exceptions from the classification of high-risk AI Act in defined cases. This capacity vested in the authority does not cover the case where Biometric verification systems intended for confirmation of person's identities are used otherwise. This is because the exclusion of those systems from the scope of high-risk AI is not rooted in any of the exceptions rooted in art. 6 (3) of the Act. Rather, they are explicitly excluded by virtue of Annex III of the Act. Consequently, the preconditions is not fulfilled to extend the MSA's authorities to evaluate the miscategorised AI systems to include the biometric verification systems intended to be used for confirmation of identity.

[76] EU AI Act, Deployers obligation, art. 26 (7), recital 92.

this purpose, the system is no longer solely purposed for the verification. Where in the context of work, such systems have not been properly assessed before being put in market, and it does not account for the context of work it is deployed in.

In the next section, I argue that, in the context of platform work, specifically ride-hailing and courier services, it is almost never the case that the verification is solely merely to verify the identity of the person. I, therefore, argue that in the said context, biometric identification is always accompanied with another purpose (e.g., access to work), and does not fall within the excluded biometric verification category from the high-risk AI classification. The fact that identity verification is argued by many scholars -in the context of platform work- to be part of algorithmic management rather than mere identity verification supports this claim.

2.4 BVS in Ride-Hailing and Delivery Services: Solely Purpose of Identity Confirmation or Algorithmic Management?

The Exclusion under point 1(a) of Annex III applies only where the biometric verification system's 'sole purpose' is to confirm identity. This purpose-dependent classification aligns with the CJEU's reasoning in Hauptpersonalrat (Case C-34/21), where the Court held that fingerprint data constitutes 'biometric data' under Article 9(1) GDPR only where it is processed "for the purpose of uniquely identifying a natural person" (CJEU, 30 March 2023, para. 42).[77] By analogy, where the actual use of the BVS in the context of ride-hailing and delivery courier services is almost never solely confirmation of the workers' identities, and is rather often coupled with one or more of the managerial prerogatives such as monitoring and/or discipline to perform algorithmic management, the exclusion shall not apply.

European DPAs consistently find that deployers' use of automated systems, including BVS, extends beyond their intended purpose. The Italian DPA found that Glovo's facial recognition use is not merely for identity confirmation but serves as a gateway to automated deactivation since the riders who fail or refuse to undergo the biometric check have their accounts deactivated. In 2023, the French DPA (CNIL) fined Amazon's French subsidiary € 32 million for excessive and opaque data collection and processing is disproportionate in workplaces, and puts the workers under undue pressure, leading to significantly negative repercussions of their well-being.[78]

The Exclusion from high-risk classification under point 1(a) of Annex III on the assumption that such systems serve the 'sole' purpose of identity confirmation. This assumption focuses exclusively on the provider's intended use at the development stage, without accounting for the deployers' actual use which, as demonstrated above, usually encompasses the sole purpose of verification by being coupled with managerial purposes. The exclusion therefore does not reflect the reality of how biometric verification operates in platform work.

---

[77] Case C-34/21, Hauptpersonalrat (CJEU, 30 March 2023), para. 42.

[78] Molè, M. (2024). Minimised work surveillance exists under the GDPR: Amazon France and the DPA sanction. Global Workplace Law & Policy.

The Act's gap is in this sense is structural. Unless a BVS is specifically developed for employment contexts, the provider is not expected to account for work-related risks in its design, training data, or risk assessment. This is as shown above for systems such as Microsoft's Azure Face API that is developed as general-purpose verification tools with no employer prerogative or workplace-specific features in mind. When a platform deploys such a system and couples it with automated deactivation, the risk profile changes fundamentally. Yet the system's classification of risk remains anchored to the provider's original intended purpose, not the deployer's actual use. The consequences of such is that deployers of BVS may covertly use them for purposes beyond identity confirmation, including as inputs to algorithmic decision-making processes that determine workers' access to their livelihood.

3 IMPLICATIONS OF BIOMETRIC VERIFICATION SYSTEMS EXCLUSION FROM SCOPE OF High-Risk AI UNDER POINT 1 (a) of Annex III:

The Exclusion limits the providers' and the users' obligations to the lightened requirements imposed on them for AI systems other than those high-risk,[79] and, in context of ride-hailing and delivery as work platforms, leave the drivers' as the persons affected by the AI system with a level of protection that is inequivalent to the level of risk they may incur due to the system use in the precarious platform work. In this case, the providers' obligations of non-high risk biometric verification AI systems vary from a mere option for them to voluntarily adopt a code of conduct to meet standards similar to those imposed by the Act for high risk AI[80] to their obligations to inform users when interacting with an AI system.[81] Deployers of non-high risk AI, on the other hand, are only required to inform the affected persons when deploying certain AI systems.[82] A level of protection that is inconvenient with the potential level of risk which BVS use in ride-hailing and delivery courier services, and platform work generally, as demonstrated earlier in this article.[83]

---

[79] EU AI Act, Art. 52 to 55.

[80] EU AI Act, Art. 55.

[81] EU AI Act, Art. 52.

[82] EU AI Act, Art. 52, providing for other obligations of more specific AI are provided for by the Act, such as the additional obligations in case of General purpose AI, but they are irrelevant in this context.

[83] This argument is not to say that the AI Act regulation of high-risk AI is flawless. However, this is to argue that the protection of high-risk AI systems provided under point 1 (a) of Annex III is the minimum level of protection for affected person against the use of AI systems deployed in platform work. Scholarship on where the AI Act regulation of high-risk AI might improve exist. In this regard, Veale & Borgesius (2021) argue that *"the Act also has severe weaknesses. It is stitched together from 1980s product safety regulation, fundamental rights protection, surveillance and consumer protection law. […] 1. The high-risk regime looks impressive at first glance. But scratching the surface finds arcane electrical standardisation bodies with no fundamental rights experience expected to write the real rules, which providers will quietly self-assess against. 2. The transparency provisions either add little to existing law or raise more*

The blanket Exclusion from high-risk AI scope consequently excludes them from the heightened protection that the Act prescribes for these systems. Chapter 3 of the Act whereby provides for the providers and the deployers of the high-risk AI systems are required to comply with the High-Risk AI requirements[84], and for the former to provide for the establishment, implementation, documentation, and maintenance of a risk management system for high-risk AI systems,[85] as well as to keep technical documentation,[86] and record keeping[87].

This contribution sheds the light on the implications of exclusion of BVS from the scope of high-risk AI system provided for in Point 1 (a) of Annex III of the Act in terms of three main requirements. These requirements are the providers' obligation to (1) opt for an independent third-party conformity assessment before the AI system is placed on the market, and (2) design the system in a way that they can be effectively overseen by natural persons to ensure risk mineralization to health safety and fundamental human rights and ensure aligned with the intended purpose and conditions for reasonably foreseeable misuse, and (3) design a system which output can be interpreted by the deployers and to provide the later with instruction of use including information on the systems intended purpose, level accuracy metrics, level of robustness and cybersecurity, provided for in articles (43), (14), and (13) of the Act, respectively.

Even though ride-hailing and delivery courier services fall within the category of digital labour plaform and, consequently, it could be argued that while the Act excludes BVS from point 1 (a), the AI systems used in these services may fall under the high-risk categorization of point (4) "Employment, Work management and access to self-employment". However, BVS solely used for confirmation of identity may still falls outside the scope of the latter provision because it is neither intended for recruitment or selection (point 4.a), nor for making decisions affecting terms of work, promotion, task allocation, or termination of a work relationship, nor is it intended for monitoring and evaluation of the ride-hailing (point 4.b).

Where the BVS are coupled up with another system intended for any of these managerial prerogatives, it cannot automatically be assumed that this will trigger the classification under point 4 of the Annex. This is because the Act is silent as to the consequences of combining between two AI systems where one is not high-risk (biometric verification system) while the other is high-risk (AI system intended for monitoring purposes). Even if classified as such this will likely be due to the use of the second system only as highlighted in the draft European Commission guidelines

questions than answers when their implications are considered. 2. The enforcement mechanism is a creature of product safety. 4. The regime is expected to regulate AI users too, yet affected communities are provided with (i) no mechanism for complaint or (ii) judicial redress", See Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22(4), 97–112, p. 25.

84 EU AI Act, Art. 8.

85 EU AI Act, Art. 9.

86 EU AI Act, Art. 11.

87 EU AI Act, Art. 12.

on high-risk AI systems[88] where it states:[89] *"where multiple **AI** components operate together so that their combined purpose or outputs materially influence a decision, the set-up should be assessed as a whole".*[90] However, this is still untested in practice. Even though this might be case, this article is more prone towards the claim that the inclusion of BVS under the high-risk AI systems in point 1 (a) rather than point 4 of Annex III is more appropriate, and even necessary. This is to ensure heightened regulation for the BVS used in context of platform work, and specifically ride-hailing and delivery courier services, including triggering the requirement for the provider of AI systems classified under point 1 (a) to opt for a third-party notified body conformity assessment under art. 43 (1) of the Act, whereas under point 4 (b), the provider is only required to conduct a self-assessment under art. 43 (2) which may allow the provider to escape the system by narrowly defining the intended purpose.

4 CONCLUSION

This contribution thouroughly analyzed the EU AI Act's Exclusion, including authentication, intended for the sole use for identify confirmation from the scope of high-risk AI system, and demonstrated that such an exclusion is an unjustified blanket exclusion of all BVS with a varying spectrum of significance disregarding the sensitive nature of biometric data regardless of whether it is used for verification or identification purposes, and the sensitivity of the context they are deployed in. In the specific context of ride-hailing and delivery courier services, BVS, including facial recognition, increases the struggles already faced by the drivers and the couriers due to the precarious nature of work, by subjecting them to these systems challenged for inaccuracy and high false rate, especially, for people with dark skin and of minorities representing a significant percentage of these platform workers.

---

[88] European Commission. (2026, May 19). Draft Commission guidelines on the classification of high-risk AI systems. Directorate General for Communications Networks, Content and Technology. The guidelines were open for stakeholders contributions until the 23rd of June 2026. Since then, no final version of the guidelines is issued.

[89] European Commission, Draft Guidelines on High-Risk AI Classification (19 May 2026), p. 2, para 3 and 6, respectively state: *The Commission's interpretation of certain concepts that are relevant for classification purposes and, in accordance with Article 6(5) AI Act, contain practical examples of AI systems that should or should not be classified as high risk.". The Guidelines are not binding. Any authoritative interpretation of the AI Act may ultimately only be given by the Court of Justice of the European Union ('CJEU')* and *"They aim to support providers and deployers of AI systems, as well as competent market surveillance authorities, in assessing whether an AI system should be classified as high-risk, thereby facilitating the uniform application and effective enforcement of Article 6 AI Act.".*

[90] European Commission, Draft Guidelines on High-Risk AI Classification (19 May 2026), p. 124. It is worth mentioning that these draft guidlines point is not tackled in the guidelines under the scope of Point No.4 Of Annex III specifically. Rather it is stated as part of the elaboration on AI Systems Falling Within the Use Case of Point 7(b) Of Annex III.

I have further demonstrated that, in the context of platform work, generally, and ride-hailing and deliver courier platforms more specifically, the biometric verification data may cause significant harm to the fundamental rights of the workers whose livelihood depend on the platform work. Additionally, I demonstrated that BVS is almost always used coupled up with another purpose rather than just for identity verification. Cases from European Courts and DPAs provide on the increasing reliance on Algorithmic management, whereby the platform uses BVS and other AI tools for managerial prerogatives relies, incidentally or purposely, on data feeding BVS. Yet, the Act bases the Exclusion on two pillars, one of which is its assumption that BVS impose minor risks by unjustifiably comparing them to biometric identification systems, while the other is that the sole use of BVS is confirmation of identity.

This contribution, further, highlighted some of the most significant implications of the Exclusion the scope of high-risk AI system provided for in Point 1 (a) of Annex III, namely being that exclusion from the consequential scope of the heighted protection attached to this category of high-risk systems, depriving, therefore, BVS from being independently assessed before being put in the market, designed with a proactive and effective human review mechanism, and provider-level transparency requirement regulated by (43.1), (14), and (13) of the Act, respectively.

That established, this article calls for the re-classification of the BVS as high-risk AI system, provided the same level of regulation as biometric identification systems provided for under point 1 (a) of Annex III by appreciating the actual significant level of risks which the affected persons might incur, especially in contexts where livelihood and human dignity is at stake.

Since the AI Act is not a stand-alone piece of legislation, and should be considered carefully in respect of existing EU law, I am currently working on a complementary article examining whether the GDPR, as the regulation governing data, and the PWD, as the directive governing platform work,, collectively or separately, adequately fill the regulatory gaps identified by in the AI Act's regulation of BVS of pre-market independent assessment, proactive and effective human oversight, and provider-level transparency, created by the Exclusion from the scope of high-risk AI under point 1 (a) of Annex III. Preliminary analysis of the said instruments suggests that neither of them might fill the gap created by the Exclusion. Especially, since neither the GDPR nor the PWD provide system-level regulation with pre-market requirements. The PWD, is even more disappointing, because even though it is a sector-specific directive providing enhanced protection especially in the Context of Algorithmic Management, it permits biometric data processing for identity confirmation purposes in the context of platform work.