# La tutela delle funzioni dell'Autorità di vigilanza e di notifica nel quadro normativo delineato dal DDL sull'intelligenza artificiale

*The Protection of the Functions of the Market Surveillance and Notifying Authorities within the Regulatory Framework Outlined by the Italian Draft Law on Artificial Intelligence*

Dalila Federici

Dottoressa di ricerca in Diritto penale nell'Università La Sapienza di Roma

Sommario: 1. Premessa - 2. La *governance* dell'AI: autorità di vigilanza e di notifica - 3. Le sanzioni amministrative previste per la violazione degli obblighi dichiarativi e certificatori dell'AI Act - 4. La legislazione interna in tema di mancata comunicazione alle Autorità di vigilanza e di notifica - 5. L'applicabilità degli illeciti penali già vigenti - 6. Rilievi conclusivi: l'opportunità di creazione di nuove figure di reato.

**ABSTRACT**

Il presente contributo esamina il processo di attuazione a livello nazionale del Regolamento (UE) 2024/1689 sull'intelligenza artificiale (AI Act), con particolare attenzione alla tutela penale delle funzioni delle Autorità di vigilanza e di notifica. Dopo aver esaminato la legislazione unionale in tema di obblighi dichiarativi e certificatori, nonché le sanzioni amministrative previste dall'AI Act, ci si sofferma sulla possibilità di applicare gli illeciti penali già vigenti alle condotte che ostacolano le funzioni di vigilanza e di notifica. Nelle conclusioni si vaglia, infine, l'opportunità della creazione di nuove figure di reato, anche alla luce della delega conferita al Governo in materia penale.

***

*The paper examines the implementation of Regulation (EU) 2024/1689 on artificial intelligence (AI Act) within the Italian legal system, with a particular focus on the criminal law protection of the functions assigned to the Market Surveillance and Notifying Authorities. After analysing the EU framework concerning declaratory and certification obligations, and the administrative sanctions provided by the AI Act, the paper explores the possibility of applying existing criminal offences to conduct that*

*obstructs the exercise of these functions. Finally, it considers the advisability of introducing new criminal offences, also in light of the legislative delegation granted to the Government in the field of criminal law.*

## 1. Premessa

È ormai noto che l'intelligenza artificiale (AI) si sta diffondendo in ogni settore della società contemporanea, con ricadute che andranno oltre ciascun ambito di studi [1].

La disciplina della stessa ad opera dell'Unione europea (Regolamento 2024/1689 c.d. AI Act) è per tale ragione di tipo "trasversale" e riguarda sia le condizioni che le modalità di utilizzo[2] .

Il Regolamento persegue la finalità di incentivare lo sviluppo dell'AI garantendo ai cittadini e alle imprese di «disporre di un contesto normativo prevedibile e contare su efficaci misure di salvaguardia che proteggano i loro diritti e le loro libertà fondamentali» [3]. In quest'ottica, come si vedrà, gli Stati sono

---

[1] H.A. KISSINGER-E. SCHMIDT-D. HUTTENLOCHER, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, Mondadori, 2024, *passim.*

[2] Per un commento approfondito al Regolamento si rinvia a R. PETRUSO-G. SMORTO, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *La nuova giur. civ. comm.*, 2024, p. 991; G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli, 2024, p. 32 ss.; V. CALAPRICE, *Il Regolamento europeo (c.d. AI Act)*, in AA.VV., *Manuale sull'intelligenza artificiale*, R. Razzante (a cura di), Giappichelli, 2024, p. 17 ss.; G. ZICCARDI, *Una lettura dell'*Artificial Intelligence Act*: norme, etica, adempimenti, attuazione*, AA.VV., *Intelligenza artificiale. Diritto, giustizia, economia ed etica*, Giappichelli, 2025, p. 15 ss. Per una panoramica sull'evoluzione della legislazione europea v. F. PALMIOTTO, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in *European Journal of Risk Regulation*, 17 gennaio 2025; G. NATALE, *Il nuovo regolamento europeo AI Act*, in *Diritto di internet*, 2024, p. 201 ss.; M. VEALE-F. ZUIDERVEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 2021, p. 97 ss.
Si segnala che recentemente (il 26.12.2024) anche la Corea del Sud ha approvato un testo legislativo che regola in modo orizzontale l'AI licenziando il *Basic Act on the Development of Artificial Intelligence and the Establishment of Trust* (*AI Basic Act*), che sarà in vigore a gennaio 2026 (la notizia è disponibile sul sito https://biz.chosun.com/en/en-it/2024/12/26/66W2Z3RX6FE7FMPXMR73T26SKY/?utm_source=substack&utm_medium=email ).

[3] Così si legge nella comunicazione della Commissione dal titolo «*L'intelligenza artificiale per l'Europa*», 25.4.2018 COM (2018) 237 final, p. 16. Gli altri modelli di regolamentazione rinvenibili sono quelli anglosassone e quello cinese. Il primo è improntato ad una normazione minima, lasciando all'autonomia privata e alle linee guida etiche il compito di disciplinare il settore. Il modello cinese è invece più centralizzato e diretto ad una regolamentazione verticale (per un approfondimento sul tema si rinvia a F. CABITZA-A. ROSSETTI, *Regole per l'intelligenza artificiale*, in AA.VV., *Aspetti Giuridici della società dell'informazione*, S. Ricci-A. Rossetti (a cura di), Giuffrè Francis Lefebvre, 2024, p. 64 ss.). Una disciplina simile è rinvenibile anche nella Convenzione quadro del Consiglio d'Europa sull'"Intelligenza Artificiale e i diritti umani, la democrazia e lo Stato di Diritto" (primo trattato internazionale che obbliga giuridicamente gli Stati a prevenire e mitigare i rischi legati all'uso dell'AI, adottato a maggio 2024, ma non ancora in vigore), che non sarà oggetto della presente analisi perché ricalca sostanzialmente il Regolamento.

chiamati a designare o individuare un'Autorità di notifica e un'Autorità di vigilanza del mercato. La prima è responsabile dell'istituzione e dell'attuazione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione di conformità[4], nonché per il loro monitoraggio. La seconda è l'autorità nazionale chiamata a svolgere le attività e ad adottare le misure di vigilanza del mercato a norma del Regolamento (UE) 2019/1020.

L'efficacia del Regolamento è stata rimandata nel tempo per consentire, da un lato, agli Stati membri di adeguarsi a quanto ivi prescritto e, dall'altro, alla Commissione di emanare atti delegati. Esso sarà quindi applicabile a partire da ventiquattro mesi dopo la sua entrata in vigore, salvo alcune specifiche eccezioni (art. 113)[5]. La scelta si è rivelata opportuna poiché, essendo il Regolamento direttamente applicabile, in assenza di una siffatta previsione gli Stati membri si sarebbero trovati sprovvisti di un'adeguata disciplina di attuazione. Infatti, nonostante i Regolamenti siano direttamente applicabili e obbligatori in tutti i loro elementi, non è detto che siano "autosufficienti", richiedendo talvolta, per la loro corretta applicazione, l'adozione di misure con successivi atti da parte degli Stati membri o dell'Unione stessa (per un approfondimento in tema di sanzioni cfr. *infra* § 3)[6].

L'Italia sta provvedendo all'adeguamento del sistema interno con il disegno di legge n. 1146 (n. 1146-A nella versione emendata)[7], contente «Disposizioni e

---

[4] La valutazione di conformità ai sensi del Regolamento è la procedura atta a dimostrare che i requisiti richiesti dalla normativa relativi ad un sistema AI ad alto rischio sono stati soddisfatti.

[5] Alcuni obblighi saranno applicabili già da sei mesi dopo la pubblicazione in Gazzetta, mentre altri solo nel 2030.

[6] G. STROZZI-R. MASTROIANNI, *Diritto dell'Unione Europea. Parte istituzionale*, Giappichelli, 2023, p. 299; R. ADAM-A. TIZZANO, *Manuale di diritto dell'Unione Europea*, Giappichelli, 2024, p. 193 ss.; R. BARATTA, *Il sistema istituzionale dell'Unione Europea*, Wolters Kluwer, 2022, pp. 201-202. La Corte di Giustizia in *Eridania* (Cfr. CGUE, 27 settembre 1979, *Eridania*, C-230/70) ha affermato che il divieto di recepimento del Regolamento non sussiste quando esso lascia agli Stati membri il compito di adottare atti necessari affinché le disposizioni dello stesso possano correttamente ed effettivamente applicarsi; secondo CGUE, 11 febbraio 1971, *Fleischkontor*, C-39/70 la misure nazionali sono ammissibili per colmare eventuali lacune dell'atto unionale purché non ne modifichino la portata o il contenuto; infine, in CGUE, 11 gennaio 2001, *Azienda agricola Monte Arcosu c. Regione Autonoma della Sardegna*, C-403/98, in A. ADINOLFI, *Materiali di diritto dell'Unione Europea*, Giappichelli, 2024, pp. 205-206, si è affermato che quando un Regolamento richiede per la sua applicazione l'adozione di normativa nazionale, lo Stato membro ha l'obbligo di emanarla; la mancanza di tale adozione però non può essere fatta valere dai privati dinanzi ai giudici nazionali (par. 29).

[7] Per un commento si veda, S. DE FLAMMINEIS, *Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del d.d.l. 1146/2024*, in *Sistema penale*, 2024, p. 5 ss.; G. CASSANO, *Note minime sul D.D.L. in materia di Intelligenza Artificiale*, in *Diritto di internet*, 2024, p. 387 ss.; G. BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, *Dir. pen. e proc.*, 2024, p. 991 ss.; G. BARONE, *La regolamentazione italiana dell'intelligenza artificiale: dove eravamo rimasti?*, in *Dir. pen.*

delega al Governo in materia di intelligenza artificiale» approvato dal Senato, emendato dalla Camera (A.C. n. 2316) e nuovamente trasmesso al Senato (n. 1146-B), con il quale sono state individuate l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) quali Autorità nazionali per l'intelligenza artificiale. Si è altresì conferita una delega al Governo in materia penale che ha subito una sostanziale modifica nella versione del testo emendato.

Il presente contributo intende quindi indagare come l'Italia si sta conformando a quanto prescritto dal Regolamento con specifico riguardo alla possibilità e all'opportunità di tutelare le funzioni delle autorità che saranno chiamate a vigilare, in senso ampio, sull'AI.

Si chiarisce subito che, come noto, il Regolamento non può prevedere direttamente fattispecie incriminatrici o introdurre obblighi di criminalizzazione [8], di talché l'effetto nel diritto penale potrà esplicarsi, da un lato, se il Parlamento italiano, discrezionalmente, nella sua potestà legislativa in materia penale, deciderà di introdurre specifiche fattispecie incriminatrici; dall'altro, per effetto dell'applicabilità al "sistema AI" di illeciti penali già esistenti.

Il campo di studio non riguarda quindi se (e come) sia possibile commettere un reato con l'uso di strumenti tecnologici legati all'intelligenza artificiale, di cui già si è cominciato da tempo a discutere [9], quanto piuttosto se il diritto penale

---

*e proc.*, 2025 p. 703 ss.; L. SCOLLO, *L'intelligenza artificiale entra nel codice penale, ivi,* p. 693 ss. Con specifico riguardo all'attività giudiziaria v. M. CERASE, *L'intelligenza artificiale generativa e la giustizia penale: riflessioni di aggiornamento,* in AA.VV., Liber amicorum *per Giorgio Lattanzi,* G. Fidelbo – E. Gallucci (a cura di), Giuffrè Francis Lefebvre, 2025, p. 543 ss.

[8] È assolutamente pacifico che la competenza dell'Unione europea in materia penale può essere esclusivamente indiretta. Invero, ai sensi dell'art. 83 TFUE il Parlamento e il Consiglio dell'Unione europea possono introdurre solo mediante Direttiva norme minime relative alla definizione dei reati e delle sanzioni. Per un approfondimento cfr. M. DONINI, *Diritto penale. Parte generale*, Giuffrè Francis Lefebvre, 2024, p. 899 ss.; V. MANES, *Il giudice nel labirinto*, Dike, 2012, p. 108 ss. e nella manualistica si veda, G. MARINUCCI-E. DOLCINI-G.L. GATTA, *Manuale di Diritto Penale. Parte Generale*, Giuffrè, 2024, p. 54 ss.; G. FIANDACA-E. MUSCO, *Diritto penale. Parte Generale*, Zanichelli, 2019, p. 68 ss.

[9] In generale v. F. CONSULICH, Flash Offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. e proc. pen.*, 2022, p. 1015 ss.; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. inf. e dell'informatica*, 2021, p. 317 ss.; N. MAZZACUVA, *Alcune riflessioni su intelligenza artificiale e diritto penale sostanziale*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, U. Ruffolo (a cura di), Giappichelli, 2021, p. 287 ss. L. D'AMICO, *La misura della (im)prevedibilità. Modelli di imputazione della responsabilità al tempo dell'intelligenza artificiale,* E.S.I., 2025; M. GIUCA, *La responsabilità penale dell'intelligenza artificiale: dubbi, perplessità e prospettiva,* in *Riv. it. dir. e proc. pen.*, 2025, p. 143 ss. A. MATTARELLA, *Diritto penlae e nuove tecnologie: dalla Convenzione Oni contro i reati informatici alle sfide dell'intelligenza artificiale,* in *Dir. pen. e proc.*, 2025, p. 250 ss. Si pensi poi ad esempio agli studi sulle macchine a guida autonoma (cfr. *ex multis* R.M. VADALÀ, *La questione penale delle auto a guida autonoma in prospettiva comparata*, in *Legislazione*

possa intervenire a tutela delle funzioni di regolazione e controllo dell'AI (notifica e vigilanza). In caso di risposta affermativa, si vaglierà anche il più opportuno schema di incriminazione.

Prima di approfondire ulteriormente, si deve premettere una breve ricostruzione della normativa in materia di intelligenza artificiale.

**2. La *governance* dell'AI: autorità di vigilanza e di notifica**

L'intelligenza artificiale è definita dall'AI Act all'art. 3 come: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» [10]. Essi sono tecnicamente denominati sistemi di *machine learning*, ossia di apprendimento automatico [11] e la loro caratteristica è quella di essere un sistema (*learner*) programmato da un essere umano, che modifica autonomamente i parametri e i percorsi da seguire per il raggiungimento dello scopo (tale procedimento è chiamato "apprendimento") [12]. L'AI è priva di "coscienza", nel senso che essa non può riflettere su ciò che scopre né è in grado di spiegare allo sviluppatore come ha raggiunto un determinato risultato [13]. Sono

*Penale*, 13.11.2023; M. LANZI, Self-driving cars *e responsabilità penale. La gestione del «rischio stradale» nell'era dell'intelligenza artificiale*, Giappichelli, 2023; R. COMPOSTELLA, *Auto a guida autonoma e diritto penale*, Editoriale Scientifica, 2024 e, nella letteratura straniera, v. D.M. VINCENTE-R.S. PEREIRA-A.A. LEAL, *Legal Aspects of Autonomous Systems. A comparative Approach*, Springer, 2024) oppure all'uso dell'intelligenza artificiale nel *trading* (F. CONSULICH, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca Borsa e titoli di credito*, 2018, p. 195 ss. e più in generale sul trading algoritmico v. J. CHAN, *Automation of Trading Machine for Traders*, Palgrave Macmillian, 2019, p. 45 ss.).

[10] In dottrina si è osservato però che in realtà non esiste una definizione di AI universalmente accettata ma essa ricomprende una serie di concetti più disparati che sono difficili da definire (in questo senso e per un approfondimento sulle possibili definizioni v. A. HAUSELMANN, *Disciplines of AI: An Overiew of Approaches and Techniques*, in AA.VV., *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*, B. Custers-E. Villaronga (a cura di), Springer, 2022, p. 44 ss.).

[11] Così F. CABITZA-A. ROSSETTI, *Regole per l'intelligenza artificiale*, cit., p. 62 ss.

[12] L'algoritmo di apprendimento può essere a sua volta "supervisionato", nel senso che l'essere umano determina il tipo di risultato da produrre, ovvero "non supervisionato", nel senso che si chiede alla macchina di rintracciare il miglior risultato possibile (cfr. L. TOMASSINI, *Intelligenza artificiale, impresa, lavoro*, in AA.VV., *XXVI lezioni di diritto dell'intelligenza artificiale*, U. Ruffolo (a cura di), Giappichelli, 2021, p. 44).

[13] H.A. KISSINGER-E. SCHMIDT-D. HUTTENLOCHER, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, cit., p. 67 ss.; F. FAGGIN, *Irriducibile. La coscienza, la vita, i computer e la nostra natura,* Mondadori, 2022, p. 136 ss., il quale evidenzia che l'intelligenza che viene attribuita alle macchine è in realtà l'intelligenza del loro programmatore.

quindi gli esseri umani a dover verificare se l'AI ha prodotto l'esito desiderato.

In questo contesto, seppur è vero che i sistemi di intelligenza artificiale possono sviluppare dei comportamenti inaspettati è altrettanto vero che la maggior parte dei modelli si addestrano in una fase diversa da quella dell'operatività, il che consente di farli rimare "statici" una volta conclusa la fase di addestramento [14]. Ovviamente ciò non significa che un sistema di intelligenza artificiale non si comporterà in modo inaspettato se inserito in un contesto nuovo, piuttosto che è possibile ridurre il margine di errori o devianze con una corretta programmazione e collaudo [15]. Da ciò discende la possibilità di regolamentarne l'uso e, come vedremo, anche quella di valutare la conformità di un sistema rispetto a quanto prescritto dalla legge.

Ciò premesso, l'AI Act ha quale obiettivo quello di rafforzare la capacità industriale dell'Unione, garantendo però il rispetto dei diritti umani e la sicurezza dei prodotti.

L'idea di fondo è che i sistemi AI si prestano a violare i diritti e le libertà fondamentali e, per tale ragione, è opportuno che i rischi siano prevenuti attraverso una disciplina organica. In quest'ottica, si sono divisi i sistemi AI in base al rischio di compromissione dei diritti dell'uomo ai quali corrisponde un diverso complesso di regole da seguire [16].

La prima categoria comprende le pratiche AI che presentano rischi "inaccettabili" (art. 5) e per tale ragione sono vietate nel mercato dell'Unione[17].

---

[14] Si veda ancora H.A. KISSINGER-E. SCHMIDT-D. HUTTENLOCHER, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, cit., p. 73.

[15] Spiegano H.A. KISSINGER-E. SCHMIDT-D. HUTTENLOCHER, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*, cit., p. 74 che l'AI è vincolata dal suo codice in tre modi diversi, esso infatti stabilisce: i parametri delle possibili azioni; la funzione-obiettivo; infine, gli *input* da riconoscere ed analizzare.

[16] Per un approfondimento si rinvia a G. BARONE, *Artificial Intelligence Act: un primo sguardo al regolamento che verrà*, cit., p. 1047 ss.; M. EBERS, '*Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*', in *European Journal of Risk Regulation*, 2024, p. 7; N. MUFTIC, *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation*, in *Artificial Intelligence and Normative Challenges*, A. Kornilakis-G. Nouskalis-V. Pergantis-T. Tzimas (a cura di), Springer, 2023, p. 86 ss.; A. MANGIONE, *Intelligenza artificiale, attività d'impresa e diritto penale*, Giappichelli, 2024, p. 194 ss. Per un commento critico sul rischio "accettabile", v. J. LAUX-S. WACHTER-B. MITTELSTADT, *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in *Regulation & Governance*, 2024, 18, pp. 3-32; E per un commento prima dell'entrata in vigore del Regolamento, cfr. G. RESTA, *Cosa c'è di 'europeo' nella proposta di regolamento UE sull'intelligenza artificiale?*, in *Il dir. dell'informazione e dell'informatica*, 2022, p. 338 ss.; G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pub.*, 2022, p. 1092 ss.

[17] Sul punto cfr. T. PIETRELLA, *Intelligenza artificiale: rischio di manipolazione ed esigenze di criminalizzazione*, in AA.VV, *Transizioni e tutela penale*, M. Gambardella (a cura di), Giappichelli,

La seconda riguarda i sistemi ad alto rischio (artt. 6 e 7), che possono essere utilizzati purché rispettino una serie di requisiti specifici e sono caratterizzati per la presenza di obblighi per i fornitori e per gli utilizzatori[18]. Tali sistemi includono una varietà di tecnologie che impattano direttamente sulla società e sulle persone, come ad esempio quelle impiegate in infrastrutture essenziali o nella sicurezza dei prodotti o ancora in campo creditizio, potendo quindi rappresentare una minaccia diretta al bene vita, salute o ad altri diritti fondamentali.

Infine, i sistemi a rischio limitato (art. 50), che prevedono solo alcuni obblighi di trasparenza.

La decisione europea di disciplinare l'intelligenza artificiale si compone anche di un articolato sistema di *governance*, necessario al fine di garantire la corretta applicazione e attuazione del Regolamento[19].

Anche gli Stati membri svolgono un ruolo centrale nella *governance.* Ai sensi del considerando n. 153 ciascuno Stato membro dovrà designare almeno una Autorità di notifica e una di vigilanza del mercato, come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del Regolamento. L'idea è quella che la gestione del rischio dell'uso dell'AI sia controllata da

---

2025, p. 101 ss.; F. P. LEVANTINO – I. NEROINI REZENDE, *Rischio inaccettabile: usi proibiti,* in *La disciplina dell'intelligenza artificiale,* O. Pollicino – F. Donati – G. Finocchiaro – F. Paolucci (a cura di), cit., p. 159 ss.

[18] Si segnala inoltre che in tale contesto i c.d. standard svolgono un ruolo importante. In particolare, gli articoli 40 e 41 dell'AI Act rimandano a standard armonizzati e specifiche comuni la definizione concreta dei requisiti di sicurezza e affidabilità, tra cui la gestione dei rischi, la qualità dei dati, la trasparenza, la supervisione umana, l'accuratezza, la robustezza e la sicurezza informatica. Per un approfondimento sul tema si rinvia *amplius* a C. FRATTONE, *Reasonble AI and other creatures. What role for AI standards in liability litigation?,* in *Journal of Law, Market & Innovation,* 2022, p. 15 ss.

[19] Già prima dell'adozione dell'AI Act, con la decisione n. C/2024/1459 del 24 gennaio 2024, la Commissione ha istituito un apposito Ufficio per l'AI che ha quale compito quello di assisterla nella preparazione di atti di esecuzione e delegati, incoraggiare ed elaborare un codice di buone prassi e contribuire alla cooperazione internazionale con Paesi terzi (art. 2). L'Ufficio è dotato anche di competenze specifiche – prevalentemente di monitoraggio – rispetto all'AI per finalità generali (in tale settore la Commissione ha competenze centralizzate) e ai modelli AI per finalità generali che presentano ampie dimensioni con rischi sistemici. Il Regolamento costituisce anche un Consiglio per l'AI composto da un rappresentante di ciascuno Stato membro, che ha quale compito quello di fornire consulenza ed assistenza alla Commissione e agli Stati. Alla Commissione e al Consiglio è affiancato un Forum, composto da portatori di interessi. Si prevede altresì la costituzione della Commissione di un Gruppo di esperti scientifici anch'essa con compiti consulenziali. Sul punto si veda R. PETRUSO-G. SMORTO, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *La nuova giur. civ. comm.*, 2024, p. 1003; C. NOVELLI-P. HACKER-J. MORLEY-J. TRONDAL-L. FLORIDI, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *European Journal of Risk Regulation*, 5 maggio 2024. Sulla *governance* funzionale alla tutela dei diritti fondamentali cfr. F. DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'intelligenza artificiale,* in AA.VV., *La disciplina dell'intelligenza artificiale,* O. Pollicino – F. Donati – G. Finocchiaro – F. Paolucci (a cura di), Giuffrè Francis Lefevbre, 2025, p. 44 ss.

un'autorità di vigilanza[20].

Ai sensi del 156° considerando le Autorità di vigilanza del mercato designate a norma del Regolamento AI devono disporre di tutti i poteri di esecuzione previsti da quest'ultimo e dal Regolamento (UE) 2019/1020, nonché esercitare i loro poteri e svolgere le loro funzioni in modo indipendente, imparziale e senza pregiudizi. Infatti, ai sensi dell'art. 3, n. 26, l'Autorità di vigilanza del mercato è definita come l'autorità nazionale che svolge le attività e adotta le misure a norma del Regolamento citato.

L'Autorità di notifica è invece definita dall'art. 3, n. 19, come l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio. L'Autorità di notifica è destinataria della domanda di notifica da parte degli organismi di valutazione della conformità (art. 29). Gli organismi di valutazione che soddisfano tutti i requisiti dell'art. 31 del Regolamento e presentano la suddetta domanda divengono "organismi notificati". Essi svolgono la funzione di verificare la conformità dei sistemi AI ad alto rischio secondo le procedure di valutazione prescritte dall'art. 43. Si specifica che, ai fini della valutazione di conformità, il fornitore può optare o per una valutazione interna (di cui all'allegato VI) o per un controllo "esterno" affidato all'organismo notificato di cui all'allegato VII[21].

La scelta del legislatore è stata dunque quella di individuare nel "fornitore" il soggetto chiamato a garantire che il sistema sia conforme al Regolamento[22].

Ai sensi dell'art. 70 dell'AI Act, gli Stati membri devono quindi designare una nuova Autorità di notifica e una di vigilanza del mercato o attribuire i poteri a un'autorità già esistente. Il Regolamento all'art. 74 comma 6 prescrive però che per i sistemi di AI ad alto rischio immessi sul mercato, posti in servizio o usati da istituti finanziari, l'Autorità di vigilanza del mercato è l'Autorità nazionale responsabile della vigilanza finanziaria, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di AI siano direttamente collegati

---

[20] In questo senso B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, Giappichelli, 2025, p. 711.

[21] Inoltre, è prescritto che nel dimostrare la conformità di un sistema ad alto rischio il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII al ricorrere di una serie di casi. Vi sono poi talune deroghe previste nei successivi commi dell'art. 43 a cui si rimanda per un approfondimento.

[22] R. PETRUSO-G. SMORTO, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, cit., p. 997.

alla fornitura di tali servizi [23].

Sempre ai sensi dell'art. 74, per i sistemi di AI ad alto rischio collegati ai prodotti disciplinati dalla normativa di armonizzazione dell'Unione (allegato I, sezione A), l'Autorità di vigilanza del mercato sarà quella che è già stata designata ai sensi della normativa predetta (ad esempio, in Italia, per i dispositivi medici, il Ministero della Salute).

L'Italia, come anticipato, sta adempiendo agli obblighi imposti dal Regolamento con il disegno di legge n. 1146 (1146-A nella versione emendata) approvato al Senato, emendato alla Camera (A.C. n. 2316) e nuovamente in discussione al Senato (1146-B).

Ai sensi dell'art. 20 del d.d.l. A.S. n. 1146-B, sono designate quali Autorità nazionali per l'intelligenza artificiale l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN). La prima è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale; la seconda, anche ai fini di assicurare la tutela della cybersicurezza [24], è responsabile per la vigilanza dei sistemi di intelligenza artificiale, ivi incluse le attività ispettive e sanzionatorie, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. Ai sensi dell'art. 24 A.S. n. 1146-B lettere a), b), c) e d) del comma 2, introdotte in sede referente dal Senato, si è data delega al Governo di disporre l'adeguamento del diritto nazionale in materia di poteri, anche sanzionatori, delle autorità nazionali competenti.

Per la vigilanza sugli strumenti finanziari saranno invece competenti, in forza dell'applicazione diretta del Regolamento, la Consob, la Banca d'Italia e l'IVASS. Infatti, nel testo definitivo del d.d.l. approvato dal Senato il 20 marzo 2025, è stato previsto che resta ferma l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689. Si badi bene però che la vigilanza, svolta ai sensi di tale articolo, riguarderà la conformità del prodotto AI e non il mercato ai sensi del T.U.F. o gli enti creditizi ai sensi del

[23] Tale scelta sembrerebbe riflettere quella più ampia dell'Europa verso un approccio informato al principio della c.d. neutralità tecnologica. Recentemente tale principio è stato enunciato nel Regolamento 2023/1114 del 31 maggio 2023 relativo ai mercati delle cripto attività, ove è stato affermato al considerando n. 9 che gli atti legislativi dell'Unione in materia di servizi finanziari dovrebbero essere guidati dal principio «stessa attività, stessi rischi, stesse norme» e dal principio della neutralità tecnologica.

[24] Come definita dall'art. 1, comma 1, del d.l. 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

T.U.B. o sulle assicurazioni ai sensi del C.A.P. (Codice delle Assicurazioni Private).

In conclusione, allo stato attuale, le Autorità di possibile interesse per il presente lavoro possono essere individuate nell'AgID e ACN (quali autorità generali di notifica e di vigilanza) e in quella di vigilanza finanziaria che è svolta da Consob, Banca d'Italia e IVASS; oltre a quelle competenti per i prodotti che sono oggetto di normativa armonizzata. A questi si dovrebbero aggiungere anche gli organismi notificati, la cui qualificazione giuridica come autorità pubblica è dubbia e verrà affrontata nel prosieguo.

## 3. Le sanzioni amministrative previste per la violazione degli obblighi dichiarativi e certificatori dell'AI Act

Il Regolamento impone specifici obblighi ad una molteplicità di soggetti (i fornitori; gli importatori; i distributori e i *deployer*) in tema di comunicazione all'autorità di vigilanza e di notifica.

Alcuni di tali obblighi ai sensi dell'AI Act sono già ricollegati in caso di violazione all'irrogazione di una sanzione amministrativa pecuniaria; al contempo è previsto che gli Stati membri debbano stabilire le regole relative alle sanzioni e alle altre misure di esecuzione (che possono includere anche avvertimenti e misure non pecuniarie), applicabili in caso di violazione dell'*AI Act* da parte degli operatori.

Ai sensi dell'art. 99 del Regolamento è prevista la sanzione pecuniaria amministrativa fino a 15.000.000 euro, o se l'autore dell'illecito è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, quando sono violati una serie di obblighi ed in particolare, per quel che attiene all'oggetto della presente ricerca: gli obblighi dei fornitori sulla dichiarazione di conformità UE (art. 16)[25]; l'obbligo dei rappresentati autorizzati a norma dell'art. 22 di fornire su richiesta una copia del mandato alle Autorità di vigilanza del mercato; gli obblighi degli importatori a norma dell'art. 23, in tema di falsificazioni[26]; gli

[25] Ai sensi dell'art. 47 il fornitore compila una dichiarazione di conformità UE per ciascun sistema di AI ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di AI ad alto rischio è stato immesso sul mercato o messo in servizio. La dichiarazione di conformità UE identifica il sistema di AI ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti.

[26] Qualora questi abbiano motivo sufficiente di ritenere che un sistema di AI ad alto rischio

obblighi dei distributori a norma dell'art. 24[27], tra cui rientrano quelli di cooperazione con l'Autorità nazionale competente; gli obblighi dei *deployer* a norma dell'art. 26, tra i quali, si annovera l'informare senza ritardo l'Autorità di mercato competente in caso di incidenti; infine, gli obblighi informativi gravanti sugli organismi notificati di cui agli artt. 33 e 34[28].

Ai sensi dell'art. 99 è poi previsto uno specifico illecito punito con la sanzione amministrativa pecuniaria fino a 7.500.000 euro o, se l'autore dell'illecito è un'impresa, fino all'1% del fatturato totale mondiale annuo dell'esercizio precedente, in caso di fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta.

Si rinvengono poi alcuni obblighi che sembrerebbero privi di apposita sanzione. Ad esempio, quelli rivolti ai fornitori di tipo informativo, ai sensi degli artt. 20, 21 e 55[29]; oppure quello sulla corretta redazione e trasmissione della documentazione tecnica del modello AI e sul suo processo di addestramento ai sensi dell'art. 53; infine, quello di segnalazione di incidenti gravi all'Autorità di vigilanza ai sensi dell'art. 73[30].

---

non sia conforme al Regolamento, ovvero sia falsificato o sia accompagnato da una documentazione falsificata, non lo immettono sul mercato fino a quando non sia stato reso conforme.

[27] I distributori che devono mettere a disposizione sul mercato un sistema di AI ad alto rischio verificano che esso rechi la necessaria marcatura CE e che sia accompagnato da una copia della dichiarazione di conformità UE e dalle istruzioni per l'uso. Su richiesta motivata di un'autorità nazionale competente, forniscono tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema. L'art. 24 prevede poi un obbligo generico di collaborazione con le autorità nazionali competenti.

[28] La sanzione è prevista anche per la violazione delle prescrizioni relative agli organismi notificati di cui all'art. 31.

[29] Ai sensi dell'art. 20, i fornitori devono adottare le necessarie misure correttive nel caso in cui un sistema non sia conforme al Regolamento e di informare, se necessario, l'Autorità di vigilanza del mercato e l'organismo notificato e ai sensi dell'art. 21, i fornitori di sistemi di AI ad alto rischio, su richiesta motivata di un'autorità competente, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di AI ad alto rischio ai requisiti prescritti. Aggiuntivamente, per quelli che presentano un "rischio sistemico", ai sensi dell'art. 55, tra i vari obblighi, i fornitori tengono traccia, documentano e riferiscono senza indebito ritardo all'Ufficio per l'AI e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio.

[30] La segnalazione è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente grave o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che il fornitore o, se del caso, il *deployer*, è venuto a conoscenza dell'incidente grave. Il periodo per la segnalazione di cui al primo comma tiene conto della gravità dell'incidente. A seguito della comunicazione di un incidente grave a norma del paragrafo 1, il fornitore svolge senza indugio le indagini necessarie. Ciò comprende una valutazione del rischio dell'incidente nonché misure correttive. Il fornitore coopera con le autorità competenti e, se del caso, con l'organismo notificato interessato durante le indagini di

Un altro obbligo informativo verso l'Autorità di notifica che sembrerebbe non prevedere una specifica sanzione è quello rivolto agli organismi notificati (art. 45).

Ed ancora, in riferimento alla dichiarazione di conformità UE, è previsto che se questa non è redatta o è redatta in modo difforme, ai sensi dell'art. 83, l'Autorità di vigilanza del mercato, chiede ai fornitori di porre fine alla non conformità contestata. Se la non conformità permane, l'Autorità adotta misure appropriate e proporzionate per limitare o proibire la messa a disposizione sul mercato del sistema di AI ad alto rischio o per garantire che sia richiamato o ritirato dal mercato senza ritardo. In questo caso quindi la sanzione non è pecuniaria ma di tipo interdittivo/sospensivo.

Traendo delle prime conclusioni dall'analisi del Regolamento e del sistema sanzionatorio ivi previsto, si può affermare che non esiste uno specifico illecito amministrativo che tuteli in via generale le funzioni delle autorità coinvolte. Piuttosto la tutela delle stesse è "frammentata" in una serie di disposizioni che sanzionano le mancate comunicazioni o la falsificazione dei documenti a loro diretti.

Prima di procedere all'analisi delle disposizioni interne, deve evidenziarsi che la traduzione italiana del Regolamento impiega in riferimento all'ente, al posto della parola "illecito", qui adoperata, quella di "reato" (si legge testualmente: «*o, se l'autore del reato è un'impresa*»). Nel sistema italiano però, come noto, gli enti non possono commettere illeciti penali in senso stretto. Invero, le società possono rispondere soltanto in via "amministrativa" di un reato commesso dalla persona fisica ai sensi del d.lgs. n. 231 del 2001, qualora il soggetto attivo sia incardinato nell'ente (apicale o sottoposto), il reato sia commesso nel suo interesse o vantaggio e l'ente versi in "colpa d'organizzazione" [31].

---

cui al primo comma e non svolge alcuna indagine che comporti una modifica del sistema di AI interessato in un modo che possa incidere su un'eventuale successiva valutazione delle cause dell'incidente, prima di informare le autorità competenti di tale azione. L'Autorità di vigilanza del mercato, quando informata, adotta le misure appropriate di cui all'art. 19 del Regolamento (UE) 2019/1020 entro sette giorni dalla data di ricevimento della notifica di cui al par. 1 dell'art. in esame e segue le procedure di notifica previste da tale Regolamento.

[31] In generale sulla responsabilità da reato della persona giuridica, v. AA.VV., *Responsabilità da reato degli enti*, vol. I, *Diritto sostanziale*, G. Lattanzi-P. Severino (a cura di), Giappichelli, 2020; M. GAMBARDELLA, *Condotte economiche e responsabilità penale*, Giappichelli, 2020, p. 76 ss.; A. ALESSANDRI-S. SEMINARA, *Diritto penale commerciale*, vol. I, *I principi generali*, Giappichelli, 2025, p. 89 ss.; AA.VV., *Commentario al decreto sulla responsabilità da reato degli enti d.lgs. 231/2001*, G. Stampanoni-L.N. Meazza (a cura di), Pacini Giuridica, 2024. Sulla specifica riconducibilità del "sistema 231" alla materia penale, si veda *ex multis*, tra i più recenti, FE. MAZZACUVA, *L'ente premiato. Il diritto punitivo nell'era delle negoziazioni: l'esperienza angloamericana e le prospettive di riforma.* Giappichelli, 2020, p. 123 e ss. Sulla "colpa" dell'ente A. FIORELLA-A. VALENZANO, *Colpa*

Inoltre, a far propendere per la soluzione della natura amministrativa della responsabilità è anche il fatto che l'illecito è contenuto in un Regolamento che, avendo effetti diretti, come detto, non può introdurre nel nostro sistema fattispecie incriminatrici. A rafforzare tale conclusione è il dato letterale secondo il quale «*la non conformità è soggetta…a sanzioni amministrative pecuniarie*».

Quanto all'applicazione di queste, a seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che esse siano inflitte dai tribunali nazionali competenti o da altri organismi. Il Regolamento ha però cura di specificare che l'esercizio da parte dell'Autorità di vigilanza del mercato dei poteri attribuitile è soggetto a garanzie procedurali adeguate in conformità al diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

L'affermazione apre all'interrogativo sulla natura della sanzione amministrativa. Infatti, il principio del giusto processo – *ex* art. 6 CEDU e art. 47 Carta dei diritti fondamentali dell'Unione europea – è applicabile solo in procedimenti di carattere "penale", da intendersi come procedimenti che conducono ad una sanzione afflittivo-punitiva secondo i noti criteri Engel [32], e non anche ai procedimenti civili o amministrativi. Su tale riflessione si tornerà nelle conclusioni quando ci si interrogherà sull'opportunità dell'intervento penale.

**4. La legislazione interna in tema di mancata comunicazione alle Autorità di vigilanza e di notifica**

---

*dell'ente e accertamento. Sviluppi attuali in una prospettiva di diritto comparato*, Sapienza Università Editrice, 2016; A. ORSINA, *La responsabilità da reato dell'ente: tra colpa di organizzazione e colpa di reazione*, Giappichelli, 2024; M. COLACURCI, *L'illecito "riparato" dell'ente. Uno studio sulle funzioni della compliance penalistica nel d.lgs. 231/2001*, Giappichelli, 2022, p. 196 ss.

[32] Corte EDU, Plenaria, 8 giugno 1976, caso n. 5100/71, *Engel e altri c. Paesi Bassi* e anche Corte EDU, 21 febbraio 1984, *Öztürk c. Germania*. Sull'evoluzione della giurisprudenza convenzionale in tema di "materia penale", da ultimo, cfr., A. TRIPODI, Ne bis in idem europeo *e doppi binari punitivi: profili di sostenibilità del cumulo sanzionatorio nel quadro dell'ordinamento multilivello*, Giappichelli, 2022, p. 117 ss.; L. MASERA, *La nozione costituzionale di materia penale*, Giappichelli, 2018; AA.VV., *La "materia penale" tra diritto nazionale ed europeo*, M. Donini-L. Foffani (a cura di), Giappichelli, 2018; V. MANES, *Profili e confini dell'illecito para-penale*, in *Riv. it. dir. e proc. pen.*, 2017, p. 988 ss.; V. MANES-M. CAIANIELLO, *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*, Giappichelli, 2020, p. 173 ss.; M. DONINI, Septies in idem. *Dalla "materia penale" alla proporzione delle pene multiple nei modelli italiano ed europeo*, in *Cass. pen.*, 2018, p. 2284 ss. Si vedano altresì le osservazioni di F. PALAZZO-F. VIGANÓ, *Diritto penale. Una conversazione*, il Mulino, 2018, p. 60 ss. Per una panoramica esaustiva delle sentenze della Corte EDU, della Corte di Giustizia dell'Unione europea e della Corte costituzionale sul tema della "materia penale", cfr. M. DONINI, *Diritto penale. Parte generale*, cit., p. 34 ss.

Come anticipato al paragrafo precedente, è previsto che gli Stati membri debbano stabilire le regole relative alle sanzioni e alle altre misure di esecuzione (che possono includere anche avvertimenti e misure non pecuniarie), applicabili in caso di violazione dell'AI Act da parte degli operatori. Le sanzioni previste devono essere effettive, proporzionate e dissuasive [33].

Questa disposizione, rivolta agli Stati membri, è frequente nei Regolamenti [34]. Ad esempio, nei medesimi termini si rinviene all'art. 50 del Regolamento 2023/1230, c.d. macchine; oppure all'art. 18 del Regolamento 2024/1106, in tema di manipolazione del mercato nell'energia all'ingrosso; ed ancora nel Regolamento (CE) 1223/2009, la cui disciplina di attuazione è contenuta nel d.lgs. 4 dicembre 2015, n. 204 recante "Disciplina sanzionatoria per la violazione del Regolamento (CE) 1223/2009 sui prodotti cosmetici".

Infatti, anche se il Regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile (*ex* art. 288, comma 2, TFUE), tale caratteristica non esclude che, affinché possa efficacemente operare, la normativa debba essere integrata per mezzo di atti ulteriori, anche statali (art. 291 TFUE) [35].

Gli Stati membri, in alcuni casi, sono cioè chiamati a garantire che il Regolamento venga applicato efficacemente per mezzo di misure sanzionatorie, la cui individuazione, quanto alla tipologia, è rimessa alla discrezionalità di quest'ultimi.

Poiché ai sensi dell'art. 83 TFUE la competenza in materia penale dell'Unione è esercitabile solo in via indiretta, cioè per mezzo di direttive, possiamo escludere che le misure a cui fa riferimento il Regolamento abbiano carattere penale. Infatti, avendo questo effetti diretti non può prevedere reati o obblighi di criminalizzazione di specifiche condotte. Di talché, le misure da introdurre possono essere intese quali amministrative in "senso stretto" (pecuniarie, ablative, interdittive/sospensive) e più in generale ogni altra attività di

---

[33] Esse tengono conto degli interessi delle PMI, comprese le *start-up*, e della loro sostenibilità economica.

[34] In questo senso, R. ADAM-A. TIZZANO, *Manuale di diritto dell'Unione Europea*, cit., p. 193 ss. Si chiarisce che in realtà anche laddove non sia esplicitamente previsto, ai sensi dell'art. 4, par. 3, comma 2, TUE gli Stati membri devono prendere «ogni misura di carattere generale o particolare atta ad assicurare l'esecuzione degli obblighi […] conseguenti agli atti delle istituzioni dell'Unione».

[35] CGUE, 27 settembre 1979, *Eridania*, cit., par. 33; CGUE, 30 novembre 1978, *Bussone*, par. 32. In dottrina, nella manualistica, cfr. R. ADAM-A. TIZZANO, *Manuale di diritto dell'Unione Europea*, cit., p. 193 ss.; G. STROZZI-R. MASTROIANNI, *Diritto dell'Unione Europea. Parte istituzionale*, cit., p. 297.

*enforcement* posta in essere dalle autorità amministrative indipendenti volte a scongiurare la produzione o la messa in uso di sistemi AI non conformi al Regolamento (avvertimenti/richieste di modifica).

A ciò si dovrebbe però poter aggiungere la facoltà dello Stato, nell'esercizio del potere legislativo, di ritenere opportuna la sanzione penale per condotte contrastanti con l'AI Act. Un esempio è il citato d.lgs. n. 204 del 2015, il quale ha previsto, tra gli altri, all'art. 3 la sanzione della reclusione e della multa per la violazione degli obblighi derivanti dal Regolamento 1223/2009 in materia di sicurezza dei prodotti cosmetici [36]. In questo senso, non è il Regolamento che obbliga lo Stato membro all'introduzione di un reato, ma è lo Stato stesso che ritiene adeguato il presidio penale.

Questo caso va invero distinto da quello in cui un Regolamento facoltizza un determinato comportamento e che, quindi, rendendolo lecito in via diretta sul territorio dell'Unione, preclude agli Stati membri di sanzionarlo (in qualsiasi forma), come ad esempio è avvenuto con il reato di raccolta di denaro per scommesse [37]. E va distinto anche dai c.d. obblighi di criminalizzazione che discendono dall'art. 117, comma 1, Cost. secondo il quale il legislatore deve rispettare i «vincoli derivanti dall'ordinamento comunitario» e gli «obblighi internazionali»[38].

---

[36] Il decreto legislativo in realtà prevede un sistema composito di illeciti penali (delitti e contravvenzioni) e amministrativi per la violazione del Regolamento in questione.

[37] Per una ricostruzione della giurisprudenza della Corte di Giustizia sul tema v. V. MANES-M. CAIANIELLO, *Introduzione al diritto penale europeo*, Giappichelli, 2020, p. 11 ss. Da ultimo sull'argomento è intervenuta anche un'importante decisione della Corte costituzionale (v. Corte cost., 4 febbraio 2025, n. 7).

[38] Sul punto si è di recente pronunciata la Corte costituzionale con sentenza n. 95 del 2025 in tema di abuso d'ufficio la quale ha precisato che le due categorie di obblighi sono equiparate quanto agli effetti vincolanti per il legislatore statale e regionale, impregiudicata restando soltanto la diversa estensione dei limiti di tali vincoli (così come precisati dalla Corte costituzionale a partire dalle sentenze n. 348 e n. 349 del 2007): il nucleo dei principi fondamentali dell'ordinamento costituzionale e dei diritti inalienabili della persona umana, rispetto ai vincoli derivanti dall'ordinamento comunitario (oggi, dell'Unione europea); l'intero corpus delle norme di rango costituzionale, rispetto agli obblighi di diritto internazionale pattizio. L'effetto della violazione degli obblighi unionali e internazionali da parte della legge, statale o regionale che sia, è però identico, e consiste nella illegittimità costituzionale della stessa, da dichiararsi da parte di questa Corte – salva naturalmente la possibilità per il giudice comune, rispetto al solo diritto dell'Unione europea dotato di effetto diretto, di disapplicare la legge nazionale o regionale che risulti con esso incompatibile (sul tema, da ultime, anche per ulteriori riferimenti alla giurisprudenza recente in materia, sentenza n. 31 del 2025, punto 4.1. del Considerato in diritto; ordinanza n. 21 del 2025, punto 6 del Considerato in diritto; sentenza n. 7 del 2025, punti 2.2.2. e 2.2.3. del Considerato in diritto; sentenza n. 1 del 2025, punto 3 del Considerato in diritto; sentenza n. 181 del 2024, punto 6.5. del Considerato in diritto). In dottrina tra i più recenti v. uno per tutti E. MAZZANTI, *Il problema degli obblighi convenzionali di tutela penale. Gli effetti espansivi della penalità derivanti dalla protezione dei diritti umani,* Giappichelli, 2025.

Ovviamente, lo Stato, nella scelta delle misure che ritiene più opportune, deve agire non in contrasto con la normativa europea.

Il legislatore italiano sta dando "attuazione" al Regolamento mediante il disegno di legge ora di nuovo in esame in Senato (n. 1146-B del 2025).

Ai sensi dell'iniziale disegno di legge A.S. n. 1146, si prevedono due disposizioni di interesse per il penalista.

La prima è l'originario art. 25 (Capo V "Disposizioni penali") in cui ci si limitava: i) all'introduzione di una circostanza aggravante comune, qualora il reato sia commesso mediante sistemi di intelligenza artificiale; ii) all'introduzione del nuovo reato di illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale; iii) e all'inserimento nel codice penale di circostanze aggravanti ad effetto speciale legate all'impiego di sistemi di intelligenza artificiale nella commissione del fatto[39]. Nel disegno di legge A.S. n. 1148-B, ovverosia nel testo emendato e approvato dalla Camera, la disposizione è ora collocata all'art. 26, la quale riproduce il precedente articolo 25, stabilendo però la soppressione della maggior parte delle circostanze aggravanti.

La seconda è quella di cui al primigenio art. 22, con cui si conferisce una delega al Governo. Esso è chiamato ad adottare, entro dodici mesi dalla data di entrata in vigore della legge, uno o più decreti legislativi per definire organicamente la disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite. In particolare, ai sensi del comma 5 del d.d.l. n. 1146, alla lett. b), il Governo dovrà introdurre una o più autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, nonché ulteriori fattispecie di reato, punite a titolo di dolo, dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'utilizzazione di sistemi di intelligenza artificiale e che non siano adeguatamente tutelabili mediante interventi su fattispecie già esistenti[40].

Nel testo emendato (A.C. 2316 e A.S. 1146-B), la delega al Governo in materia penale, ora all'art. 24, si presenta più circoscritta. Si prevede infatti che esso dovrà

---

[39] Sul punto cfr. L. SCOLLO, *L'intelligenza artificiale entra nel Codice penale,* cit., p. 698.

[40] Si veda anche il Dossier disponibile sul sito ufficiale del Senato: *https://www.senato.it/leg/19/BGT/Schede/Ddliter/dossier/58262_dossier.htm*.

introdurre autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato. Come si può notare, da un lato, viene eliminata la delega che prevedeva la possibilità per il Governo di introdurre ulteriori fattispecie di reato dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'uso dell'AI; dall'altro, le fattispecie che il Governo potrà introdurre non saranno più meramente incentrate sull'omessa adozione o adeguamento per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, ma sarà altresì necessario che tale omissione abbia determinato il pericolo concreto per la vita o l'incolumità pubblica o la sicurezza dello Stato (evocando così un modello di illecito di evento di pericolo)[41].

Non si rinviene invece alcuna menzione specifica sulla possibilità di introdurre una fattispecie penale per l'ostacolo e le false dichiarazioni alle autorità o per le false attestazioni riguardanti i sistemi AI. Nel prossimo paragrafo si indagherà, quindi, se esistono già degli illeciti applicabili e, in caso di risposta negativa, se sia opportuno introdurne di nuovi.

**5. L'applicabilità degli illeciti penali già vigenti**

Dopo aver illustrato le sanzioni amministrative introdotte dall'AI Act e la proposta di legge di nuovo in esame in Senato, deve ora valutarsi se la violazione degli obblighi sopra descritti possa configurare un illecito penale già esistente nel nostro ordinamento o se altrimenti ne sia opportuna la previsione.

Esistono invero molteplici illeciti posti a tutela delle funzioni delle Pubbliche Autorità di vigilanza e, in particolar modo, di quelle di Consob e Banca d'Italia.

Il diritto penale può infatti proteggere non solo beni empirico-fattuali ma anche funzioni, che riguardano aspetti specifici dell'agire pubblico come, ad esempio, le funzioni di gestione o di controllo di determinate attività [42]. In questo

[41] Su tale modello di illecito, con particolare riferimento ai delitti contro l'incolumità pubblica, si veda per tutti A. GARGANI, *Il danno qualificato dal pericolo. Profili sistematici e politico-criminali dei delitti contro l'incolumità pubblica*, Giappichelli, 2005, *passim*. Più di recente su tale schema di incriminazione cfr. M. POGGI D'ANGELO, *Modelli relazionali di pericolo nei reati economici*, Giappichelli, 2025, p. 260.

[42] Sulla tutela di funzioni cfr. T. PADOVANI, *Tutela di beni e tutela di funzioni nella scelta tra delitto,*

senso, si possono costruire reati con strutture diverse: quelli che prevedono la sanzione per l'attività svolta in mancanza di autorizzazione o in difformità alla stessa oppure illeciti che si sostanziano nell'omissione o nelle false dichiarazioni alla pubblica Autorità [43].

Secondo la dottrina, la legittimazione della tutela di funzioni deriva dal fatto che la protezione giuridica è apprestata in realtà a beni di tipo sostanziale, al cui servizio sono poste le suddette funzioni, di talché sono tali beni a legittimare un modello di tutela che presidi anche sul versante penale l'esercizio di talune attività [44].

In questo senso, seppur l'oggetto di tutela degli illeciti che si analizzeranno nel presente paragrafo è di tipo funzionale-istituzionale, ovverosia la correttezza nei rapporti tra ente controllato ed ente controllante [45], il bene giuridico protetto sottostante è il corretto funzionamento del mercato e la trasparenza dell'informazione [46].

Il quesito che ci si pone è se gli illeciti già esistenti potranno essere adoperati per sanzionare condotte di ostacolo alle funzioni delle Autorità sulla vigilanza AI o se invece bisognerà apprestare una tutela specifica.

Si deve partire dal dato che la tutela della vigilanza ad oggi in vigore è incentrata su illeciti che attengono a comunicazioni di tipo "economico" e quindi a funzioni di vigilanza spiccatamente finanziarie. Ci si riferisce all'art. 2638 c.c. o agli illeciti previsti nel d.lgs. 24 febbraio 1998, n. 58 (Testo unico delle disposizioni in materia di intermediazione finanziaria).

L'art. 2638 c.c. si colloca non a caso tra gli illeciti societari e si compone di due

---

*contravvenzione e illecito amministrativo*, in *Cass. pen.*, 1987, p. 670 ss.

[43] Sul primo tipo di illecito si veda ampiamente M. GAMBARDELLA, *Il controllo del giudice penale sulla legalità amministrativa*, Giuffrè, 2002, p. 199 ss.

[44] D. PULITANÒ, *Diritto penale*, Giappichelli, 2023, p. 91. Secondo A. VALLINI, *Antiche e nuove tensioni tra colpevolezza e diritto penale artificiale*, Giappichelli, 2003, p. 95 ss. la sanzione penale interviene a supportare la scelta amministrativa che ha risolto un "conflitto di interessi", che non poteva essere sciolto a monte dal legislatore.

[45] In questo senso Cass., sez. V, 8 novembre 2002, n. 1252, in *C.E.D.*, 224113-01.

[46] Attraverso il bene giuridico finale è possibile selezionare le condotte penalmente rilevanti, ricomprendendo solo quelle informazioni che sono funzionali all'interesse alla cui tutela l'Autorità è preposta per legge (in questo senso rinvia L. CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, in F. Consulich (a cura di), *Reati in materia bancaria e finanziaria*, in *Trattato teorico-pratico di diritto penale*, diretto da F. Palazzo-C.E. Paliero-M. Pelissero, Giappichelli, 2024, p. 337). La giurisprudenza, nell'affermare che il bene giuridico finale tutelato è il mercato, ha cura però di specificare che tuttavia questo non entra direttamente nell'alveo della protezione penale approntata dalla disposizione in commento (Cass., sez. V, 20 settembre 2024, n. 40738, in *C.E.D.*, 287228-01 non massimata sul punto).

fattispecie autonome di reato: il primo comma, prevede il delitto di false comunicazioni alle Autorità di vigilanza; il secondo comma, il vero e proprio delitto di ostacolo alle funzioni di vigilanza [47]. Per quanto attiene al primo comma, esso è un reato di mera condotta e di pericolo concreto; si articola in due distinte modalità di condotta volte all'ostacolo delle funzioni di vigilanza (fine specifico): l'esposizione di fatti non rispondenti al vero e l'occultamento, attraverso mezzi fraudolenti, di informazioni che dovevano essere comunicate [48]. Diverso è invece il ruolo dell'ostacolo al secondo comma dell'art. 2638 c.c. (illecito a forma libera); esso non caratterizza l'elemento soggettivo, ma assurge a vero e proprio evento [49]. Entrambe le fattispecie devono poi essere commesse da soggetti attivi qualificati (o ad essi parificati *ex* art. 2639 c.c.), che possono individuarsi, in estrema sintesi, nei soggetti che ricoprono una carica sociale apicale o di controllo (amministratori, sindaci, ecc.) o nei soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti.

Ci si interroga primariamente se le Autorità di vigilanza, le Autorità di notifica e gli organismi notificati possano considerarsi "pubbliche Autorità di vigilanza".

Ebbene, la vigilanza, che può esplicarsi in vari modi, può intendersi sia come

---

[47] Sull'illecito di cui all'art. 2638 c.c. si rinvia a L. CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, in F. Consulich (a cura di), *Reati in materia bancaria e finanziaria*, in *Trattato teorico-pratico di diritto penale*, diretto da F. Palazzo-C.E. Paliero-M. Pelissero, Giappichelli, 2024, p. 325 ss.; M. GAMBARDELLA, *Condotte economiche e responsabilità penale*, Giappichelli, 2020, p. 157 ss.; N. MAZZACUVA-E. AMATI, *Diritto penale dell'economia*, Wolters Kluwer, 2023, p. 142 ss.; S. SEMINARA, *Diritto penale commerciale*, vol. II. *I reati societari*, Giappichelli, 2021, p. 168 ss.; A. TRIPODI, sub *Art. 2638*, in A. Perini (a cura di), *Commentario del Codice civile e codici collegati Scialoja-Branca-Galgano*, Libro V, *Disposizioni penali in materia di società, di consorzi e di altri enti privati*, Zanichelli, 2018, p. 619 ss.; E. MONTANI, *Le attività di ostacolo*, in A. Alessandri (a cura di), *Reati in materia economica*, Giappichelli, 2017, p. 197 ss.; E. MUSCO-M.N. MASULLO, *I reati societari*, Giuffrè, 2022, p. 209 ss.; D.C. AMBROSETTI-E. MEZZETTI-M. RONCO, *Diritto penale dell'impresa*, Zanichelli, 2022, p. 210 ss.; D. FEDERICI-M. POGGI D'ANGELO, *La tutela penale e amministrativa dell'attività di vigilanza della Consob e il diritto al silenzio: nuove prospettive di bilanciamento anche alla luce del recente strumento degli "impegni"*, in *Cass. pen.*, 2024, p. 3760 ss.; L. MESSORI, *L'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza. Orientamenti (e disorientamenti) giurisprudenziali nell'applicazione dell'art. 2638 c.c.*, in *Arch. pen. web*, 20 ottobre 2020; D. FEDERICI, *L'art. 2638 c.c. dalla protezione di beni alla tutela di funzioni: prodotto del diritto penale moderno o erede dei* délits obstacle*?*, in *Cass. pen.*, 2020, p. 2735 ss.; G.A. MESSINA, *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza*, in G. Canzio-L. Lupária Donati (a cura di), *Diritto e procedura penale delle società*, Giuffrè, 2022, p. 665 ss.; G. LOVECCHIO MUSTI, *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638)*, in A. Rossi (a cura di), *Reati societari*, Utet, 2005, p. 242 ss.

[48] In giurisprudenza v. Cass., sez. V, 12 novembre 2015, in *C.E.D.*, 267169-01.

[49] Cass., sez. V, 16 marzo 2023, n. 21878, in *C.E.D.*, 284753-01; Cass., sez. V, 12 novembre 2015, n. 6884/16, in *Giur. it.*, 2016, p. 1482, con nota di A. ROSSI, *L'art. 2638 c.c.: problematici dati normativi e problematiche applicazioni giurisprudenziali;* e in *Cass. pen.*, 2016, p. 3409 ss., con nota di G. STAMPANONI BASSI, *Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza: problematiche in tema di concorso di reati;* Sez. V, 30 aprile 2025, n. 20174, in *C.E.D. Cass.*, n. 288134-01.

attività di verifica della conformità di agire rispetto alle regole, sia tradursi in poteri di amministrazione attiva, quali richiesta di documenti o informazioni [50].

Le Autorità prese in considerazione dalla fattispecie *ex* art. 2638 c.c. sono: pubbliche, dotate di poteri autoritativi, indipendenti (sia dal potere esecutivo sia dagli interessi sui quali vigilano), a legittimazione "legale" e "funzionale" [51].

Ciò premesso, il delitto codicistico ricomprende solo le autorità (c.d. garanti) che svolgono una funzione di vigilanza in senso tecnico, ad esclusione di quelle di regolazione dei servizi di pubblica utilità [52].

L'Autorità di vigilanza del mercato (ACN, Consob, Banca d'Italia e IVASS in materia di credito, mercati finanziari e assicurazioni) e l'Autorità (AgID) di notifica sembrerebbero poter avere tali caratteristiche: sono infatti pubbliche, indipendenti e dotate di poteri autoritativi.

Quanto invece agli organismi notificati, ci si deve domandare se possano annoverarsi tra le "pubbliche Autorità di vigilanza", poiché essi, seppur devono garantire carattere di indipendenza e autonomia, non sono "autorità pubbliche" sotto il profilo formale.

Come noto, tuttavia, secondo la giurisprudenza in tema di reati contro la P.A., al fine di individuare quando una determinata attività possa essere qualificata come pubblica, si deve verificare se essa è disciplinata da norme di diritto pubblico, essendo indifferente la connotazione soggettiva dell'agente [53]. Aderendo a tale giurisprudenza, la Cassazione ha affermato che si ritengono tali quei soggetti a cui sono demandate le funzioni pubbliche e che operano nel contesto di esse, potendosi dunque qualificare "pubbliche Autorità di vigilanza" quelle che eseguono controlli caratterizzati da finalità pubbliche [54].

---

[50] F. DI LASCIO-F. SAVO AMODIO, *L'attività di vigilanza e controllo*, in AA.VV., *L'analisi e gli strumenti per la qualità della regolazione. Annuario 2020*, G. Mazzantini-L. Tafani (a cura di), Editoriale Scientifica, 2021, p. 163 ss. Gli Autori precisano che l'organizzazione e lo svolgimento dell'attività di vigilanza da parte delle autorità indipendenti è generalmente caratterizzato da un forte grado di eterogeneità. La vigilanza è poi strutturale (o preventiva) e prudenziale (o successiva) (v. L. CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, cit., p. 333 ss.).

[51] In questo senso ancora, v. L. CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, cit., p. 333 ss.

[52] L. CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, cit., p. 333. In giurisprudenza, cfr. Cass., sez. V, 20 settembre 2024, n. 40738, non massimata sul punto.

[53] Cass., sez. un., 13 luglio 1998, n. 10086, Citaristi, in *Giur. it.*, 1999, p. 354 ss., con nota di A. BARGI, *Ribadita dalle sezioni unite la prevalenza delle regole della "giusta decisione"*. Per un approfondimento sulla nozione di pubblico ufficiale *ex* artt. 357 ss., cfr. A. PANTANELLA, Sub art. 357, in AA.VV., *Codice Penale. Rassegna di giurisprudenza e di dottrina*, vol. III, Giuffrè, 2022, p. 357 ss.; M. M. MAIELLO, *Il controllo penale sull'attività amministrativa. Un percorso tra modelli dell'agire amministrativo e confini dell'intervento punitivo,* Giappichelli, 2025, p. 108 ss.

[54] Così, Cass., sez. III, 29 maggio 2013, n. 28614, in *C.E.D.*, 257142-01.

Per rispondere quindi all'interrogativo bisognerà attendere la regolazione primaria e secondaria che verrà prevista per tali organismi nel prossimo futuro [55]. Vanno esclusi invece i casi in cui la vigilanza è affidata *ex* art. 74 AI Act ad autorità come il Ministero della salute, non essendo quest'ultimo indipendente dal potere esecutivo.

Ciò premesso, ci si interroga, seppur in via limitata alle sole Autorità di vigilanza di natura pubblica, se la disposizione *ex* art. 2638 c.c. possa ricomprendere, quantomeno testualmente, tutte le possibili condotte che ostacolano la vigilanza AI in senso ampio.

Per quanto attiene ai soggetti attivi, nulla sembrerebbe ostare all'applicazione del reato, poiché fornitori, *deployer*, importatori, ecc., sono sottoposti per legge (secondo il Regolamento) alle autorità pubbliche di vigilanza o comunque tenuti ad obblighi nei loro confronti.

Indubbiamente, però, il primo comma dell'art. 2638 c.c. è inapplicabile al settore AI, perché le comunicazioni omesse o false devono riguardare la situazione economica, patrimoniale o finanziaria dei soggetti sottoposti a vigilanza. Il secondo comma, essendo a forma libera, si presta invece a ricomprendere una quantità di condotte assai più ampia.

Il dato letterale sembrerebbe consentire la sussunzione sotto tale fattispecie di qualsiasi condotta ostacolante, anche se non può non lasciare perplessi l'impiego di un reato tipicamente "societario" per tutelare funzioni di Autorità che non hanno nulla a che fare con tale settore.

La vigilanza dell'Autorità di mercato sarà infatti svolta in conformità del Regolamento (UE) 2019/1020, che attiene alla sicurezza dei prodotti e non ad informazioni di tipo finanziario/economico. La "vigilanza" in senso ampio, che dovrà svolgere l'Autorità di notifica, ha invece ad oggetto l'operato degli organismi notificati, quindi anche in questo caso informazioni estranee all'ambito sopra indicato. Invero, le mancate comunicazioni, l'ostruzionismo, le falsità avranno ad oggetto informazioni completamente disomogenee rispetto a quelle per le quali attualmente viene applicato l'art. 2638 c.c.

---

[55] Attualmente esiste già un meccanismo di certificazione dei prodotti che avviene per mezzo di organismi notificati. La lista degli organismi, tra i quali si annoverano sia società private sia organismi "pubblici" come l'Inail o le Università, è consultabile sul sistema "NANDO" al sito *https://web gate.ec.europa.eu/single-market-compliance-space/notified-bodies/notified-body-list?filter=countryId:380,notificationStatusId:1*.

E ciò è vero anche nel caso in cui la vigilanza sia svolta nel settore finanziario, creditizio, o assicurativo, poiché, seppur l'autorità competente è la Consob, la Banca d'Italia o l'IVASS, la supervisione che effettueranno avrà ad oggetto la conformità dei sistemi.

Alla medesima conclusione deve giungersi per gli altri illeciti posti a presidio, nel dettaglio, delle funzioni di Consob e Banca d'Italia, presenti nel Testo Unico finanziario, che sono interamente rivolti a vigilanza di tipo economico-finanziario. Stesso dicasi per l'art. 306 del Codice delle Assicurazioni Private che disciplina l'ostacolo alle funzioni dell'IVASS.

Anche tutte le fattispecie nel codice penale di falso mal si attagliano al caso di specie, in quanto sanzionano attestazioni in atti pubblici.

Con esclusivo riguardo all'obbligo del marchio CE (art. 48) che deve accompagnare il prodotto ad alto rischio insieme alla dichiarazione di conformità UE (art. 47), qualora sia apposto falsamente o il soggetto si rifiuti di fornire la documentazione attestante la regolarità di apposizione, la condotta potrebbe essere sanzionata, secondo l'attuale orientamento giurisprudenziale, ai sensi dell'art. 515 c.p. [56].

Avendo escluso, almeno ad una prima lettura (e in assenza di giurisprudenza, stante la non ancora entrata effettiva in vigore di tale compendio normativo) di una fattispecie penale applicabile, ci si interroga nel prossimo paragrafo sull'opportunità di una sua creazione.

## 6. Rilievi conclusivi: l'opportunità di creazione di nuove figure di reato

Si è osservato che la tutela dei diritti umani coinvolti nell'uso dell'intelligenza artificiale potrebbe efficacemente concretizzarsi nella sanzione penale collegata all'inosservanza di obblighi derivanti da norme *extra*-penali o ordini dell'autorità, secondo il modello c.d. ingiunzionale[57].

---

[56] La giurisprudenza ha affermato che la mancata consegna da parte di colui che pone in vendita prodotti che recano il marchio CE nel corso di un controllo della documentazione che attesta la regolarità dell'apposizioni di tale marchio integra l'omissione di una condotta richiesta agli operatori economici e costituisce un comportamento significativo, in assenza di elementi contrari dell'irregolarità dell'apposizione (Cass., sez. III, 26 settembre 2019, n. 50783, in *C.E.D.*, 277688-01; Cass., sez. III, 25 giugno 2024, *ivi*, n. 287180-01).

[57] Con specifico riferimento all'oggetto di indagine si veda in questo senso L. ROMANÒ, *La responsabilità penale al tempo di chatgpt: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa,* in *Sistema penale online,* 17 maggio 2023. Più di recente cfr. B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., p. 711 la quale propone la criminalizzazione, secondo un modello

Invero i beni coinvolti sono di grande rilevanza, tale da giustificare un intervento penalistico considerato che l'immissione sul mercato, la messa in servizio e l'uso di sistemi AI possono comportare rischi e pregiudicare interessi pubblici e diritti fondamentali dell'uomo (considerando n. 5). La *ratio* stessa dell'intera scelta di regolamentazione risiede, ai sensi del primo considerando, nell'assicurare un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione, compresi la democrazia, lo stato di diritto e la protezione dell'ambiente contro i possibili effetti nocivi dei sistemi AI.

A ciò si aggiunga, di tutta evidenza, anche la sicurezza del mercato azionario quando l'AI è adoperata per investire.

La protezione delle funzioni dei soggetti che sono chiamati a verificare il rispetto delle condizioni del Regolamento è allora giustificabile alla luce degli importantissimi beni finali che si andrebbero a proteggere.

Ciò però non significa, come si dirà, che tale rango di tutela sia necessario, potendo ad una prima valutazione ritenersi sufficientemente dissuasiva quella approntata per mezzo degli illeciti amministrativi previsti nel Regolamento.

Ad ogni modo, qualora si volesse introdurre una fattispecie penale, il modello di illecito al quale si fa rifermento è quello che attiene alle false dichiarazioni alle Autorità o agli organismi notificati perché il Regolamento sull'intelligenza artificiale, nonostante abbia previsto l'istituzione di un'Autorità di notifica e degli organismi notificati che rilasciano certificati di conformità dei modelli AI ad alto rischio, comunque non ha stabilito per l'immissione sul mercato alcuna autorizzazione, rendendo la certificazione "volontaria"[58]. Sicché, in assenza di una procedura amministrativa obbligatoria di rilascio di certificazioni, non è possibile costruire un illecito che sanzioni il soggetto per aver operato in assenza o in mancanza di certificato.

Si potrebbe allora introdurre un reato costruito secondo il modello di condotta, ormai noto, riassumibile nella formula «esporre fatti rilevanti non rispondenti al vero o omettere fatti rilevanti», ampiamente adoperato in numerosi illeciti aventi ad oggetto obblighi informativi o certificatori. Si pensi non solo alle false

ingiunzionale, dell'omessa comunicazione all'autorità di vigilanza delle lesioni e dei decessi derivanti dai sistemi di intelligenza artificiale.

[58] La procedura della valutazione di conformità ai sensi dell'art. 43 dell'AI Act, infatti, può essere anche "interna" ai sensi dell'allegato VI oltre che "esterna" con il coinvolgimento di un organismo notificato, di cui all'allegato VII.

comunicazioni sociali *ex* art. 2621 c.c., ma anche al falso in attestazioni fallimentare (art. 236-*bis*, legge fall/art. 342 c.c.i.) o a quello sul c.d. *Superbonus* (art. 28-*bis*, legge n. 25 del 2022).

A questo si potrebbe aggiungere anche un illecito, sempre a modello ingiunzionale, che colleghi la sanzione al mancato rispetto dei provvedimenti dell'autorità tra i quali si annovera il potere di ritiro o richiamo di un sistema di intelligenza artificiale pericoloso. Si ricorda ad esempio che in riferimento alla dichiarazione di conformità UE, è previsto che se questa non è redatta o è redatta in modo difforme, ai sensi dell'art. 83, l'Autorità di vigilanza del mercato, chiede ai fornitori di porre fine alla non conformità contestata. Se la non conformità permane, l'Autorità adotta misure appropriate e proporzionate per limitare o proibire la messa a disposizione sul mercato del sistema di AI ad alto rischio o per garantire che sia richiamato o ritirato dal mercato senza ritardo. Nel caso di mancato rispetto dell'ordine di ritiro si potrebbe quindi prevedere una specifica sanzione penale[59], non sembrando tale condotta potersi ricondurre al vigente art. 650 c.p. Invero l'art. 650 c.p. per la sua applicazione richiede che l'ordine sia dato per ragioni di giustizia, sicurezza pubblica, ordine o igiene lasciando quindi esclusi altri possibili tipi di ordine.

La creazione di un tale tipo di illecito potrebbe del resto rientrare nel perimetro della delega conferita al Governo secondo la quale si dovranno introdurre autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato. Fuori dal perimetro della delega rimarrebbero invece i casi in cui il soggetto ometta di adempiere ma da tale omissione non derivi un siffatto pericolo.

Si rileva, inoltre, che l'assenza di una disposizione penale sembrerebbe non in linea con le scelte operate in tutti gli altri settori ove l'Autorità vigila su aspetti rilevanti della vita umana ed economica del nostro paese. Come detto, l'AI comporterà uno stravolgimento della società e sarà impiegata in modo diffuso in settori nevralgici come la sanità, i trasporti, la finanza e molti altri. Pensare quindi

[59] Propone tale soluzione. B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., p. 715.

di lasciare alcune condotte prive di una sanzione penale appare una scelta non conforme a quanto finora fatto nelle altre materie. Basti pensare alle figure di reato che vengono introdotte ogniqualvolta i soggetti sono gravati, come in questo caso, di obblighi dichiarativi o sono sottoposti a vigilanza (ad esempio nel settore della cybernetica, dell'edilizia, ecc.).

Dall'altro lato, però, gli illeciti amministrativi introdotti dal Regolamento, come anticipato, sembrano assumere un carattere fortemente afflittivo, considerata l'entità della sanzione e lo scopo della stessa. Se venisse effettivamente riconosciuta natura afflittiva a tali illeciti, la creazione di fattispecie penali rischierebbe di introdurre un nuovo sotto-sistema a doppio binario come quello tributario e degli abusi di mercato, di cui sono noti i problemi di compatibilità con i diritti umani, aventi ad oggetto il divieto di doppio giudizio e il rispetto delle garanzie del giusto processo, nonché del canone di proporzionalità complessiva della sanzione[60]. Questi sono peraltro i temi recentemente discussi in Senato che hanno portato al conferimento di una delega al Governo per la riorganizzazione del sistema sanzionatorio e del doppio binario in materia di abusi di mercato (l. 5 marzo 2025, n.21, modificata dalla l. 11 marzo 2025, n. 28).

In conclusione, qualora si scelga di impiegare lo strumento penale per tutelare

---

[60] In tema di *ne bis in idem* e abusi di mercato cfr. AA.VV., Ne bis in idem *e procedimento sanzionatorio Consob al vaglio della Corte europea dei diritti dell'uomo. Ancora sull'adattamento dell'ordinamento italiano alla Convenzione europea?*, E. Desana-P. Montalenti-M. Salvadori (a cura di), Editoriale Scientifica, 2016; D. GUIDI, *Abuso di informazioni privilegiate. Modelli di configurazione dell'illecito e prospettive evolutive*, Giappichelli, 2024, p. 419 e ss.; S. SEMINARA, Insider trading: ne bis in idem, *nozione di informazione privilegiata e accertamento probatorio*, in *Giur. comm.*, 2024, p. 173 ss.; F. D'ALESSANDRO, Market Abuse, in M. Cera-G. Presti (diretto da), *Il Testo Unico Finanziario*, Zanichelli, 2020, p. 2238 ss.; M. PERASSI-R. D'AMBROSIO, *Le sanzioni amministrative*, in M. Cera-G. Presti (diretto da), *Il Testo Unico Finanziario*, Zanichelli, 2020, p. 2308 ss.; F. ANNUNZIATA, *La disciplina del mercato mobiliare*, Giappichelli, 2020, p. 467 ss.; E. BINDI-A. PISANESCHI, *Sanzioni Consob e Banca d'Italia. Procedimenti e doppio binario al vaglio della Corte Europea dei Diritti dell'Uomo*, Giappichelli, 2018; M. SCOLETTA, *Il doppio binario sanzionatorio alla luce del vincolo europeo del* ne bis in idem, in *Reati in materia bancaria e finanziaria*, F. Consulich (a cura di), Giappichelli, 2024, p. 292; FR. MAZZACUVA, Ne bis in idem *e diritto penale dell'economia*, in *Il* ne bis in idem, A. Mangiarancina (a cura di), 2021, p. 205 ss.; N. MADIA, Ne bis in idem *europeo e giustizia penale. Analisi sui riflessi sostanziali in materia di convergenze normative e cumuli punitivi nel contesto di uno sguardo d'insieme*, Wolters Kluwer-Cedam, 2020. Con particolare riferimento al rapporto tra decreto di archiviazione e procedimento amministrativo negli abusi di mercato, v. S. SEMINARA, Insider trading: ne bis in idem, *nozione di informazione privilegiata e accertamento probatorio*, in *Giur. comm.*, 2024, p. 173/II ss. In generale in tema di *ne bis in idem*, v. L. BIN, *Le ambiguità del* ne bis in idem *di fronte a un caso di doppio binario stato-regioni*, in *Giur. cost.*, 2023, p. 1873 ss.; M. SCOLETTA, *Il principio di* ne bis in idem *e i modelli punitivi "a doppio binario"*, in *Dir. pen. cont. trimestrale*, 2021, p. 180 ss.; F. VIGANÒ, Ne bis in idem *e pluralità di sistemi sanzionatorio per lo stesso fatto*, in *Riv. soc.*, 2023, p. 189 ss.; A.F. TRIPODI, Ne bis in idem europeo *e doppi binari punitivi. Profili di sostenibilità del cumulo sanzionatorio dell'ordinamento multilivello*, Giappichelli, 2022.

in modo più effettivo i diritti umani sottoposti a rischio di violazione per l'uso dei sistemi AI, tale strumento dovrà essere sapientemente raccordato agli illeciti amministrativi introdotti dal Regolamento, al fine di garantire gli altrettanto fondamentali diritti umani in tema di giusto processo e proporzionalità della sanzione.