Capitolo XXII
PRINCIPI GENERALI DELL'AI: ACCURATEZZA, ROBUSTEZZA E CIBERSICUREZZA
Commento all'art. 15

Niccolò Panigada

1. *L'art. 15 nel contesto del sistema di requisiti per i sistemi di IA ad alto rischio.*

L'art. 15 del Regolamento europeo sull'intelligenza artificiale si colloca all'interno del Capo III, Sezione 3, dedicato ai requisiti per i sistemi di IA ad alto rischio, e rappresenta una disposizione di chiusura del complesso di obblighi tecnici e organizzativi imposti ai fornitori e, in parte, agli utilizzatori di tali sistemi.

La sua posizione sistematica non è neutra: essa segnala come accuratezza, robustezza e cibersicurezza costituiscano il punto di sintesi di una regolazione che, pur espressa in linguaggio tecnico, è funzionalmente orientata alla prevenzione dei rischi per i diritti fondamentali.

Nel disegno complessivo dell'AI Act, i requisiti dall'art. 8 all'art. 15 configurano un vero e proprio modello di regolazione *ex ante* del rischio, che si distacca dalle tradizionali tecniche di responsabilità *ex post* tipiche del diritto. L'art. 15, in particolare, opera come norma di garanzia trasversale, destinata a permeare l'intero ciclo di vita del sistema di IA, dalla progettazione alla messa in servizio, fino all'uso concreto.

Accuratezza, robustezza e cibersicurezza non sono requisiti isolati né gerarchicamente posti su piani diversi, ma si pongono in stretta relazione funzionale con gli altri obblighi previsti dal Regolamento. È necessario, pertanto, svolgere una lettura sistematica di tale articolo, soprattutto in riferimento agli altri principi che caratterizzano il Capo III della Sezione 3: si pensi alla qualità dei dati e la *governance* dei *dataset* di cui all'art. 10, che incidono direttamente sull'accuratezza dei risultati; alla documentazione tecnica e la tracciabilità degli artt. 11 e 12, che rendono verificabili le prestazioni del sistema; alla trasparenza e l'informazione agli utenti dell'art. 13, che presuppongono un livello minimo di affidabilità del sistema; alla sorveglianza umana, di cui all'art. 14, che assume significato solo in presenza di sistemi sufficientemente robusti e sicuri.

In questa prospettiva, l'art. 15 non introduce meri standard di performance, ma contribuisce a delineare un dovere di affidabilità tecnologica, inteso come presupposto per la legittimità dell'impiego dell'IA in contesti giuridicamente sensibili.

La disposizione risponde, infatti, a una logica di anticipazione della tutela, volta a evitare che decisioni automatizzate o semi-automatizzate producano effetti lesivi irreversibili sui diritti degli individui.

Dal punto di vista del diritto europeo, l'art. 15 può essere letto come espressione di una nuova forma di normatività tecnica costituzionalmente orientata, nella quale requisiti apparentemente neutrali incorporano valutazioni assiologiche riconducibili ai principi di dignità della persona, eguaglianza sostanziale, legalità e prevedibilità dell'azione pubblica e privata, sicurezza giuridica.

In tal senso, accuratezza, robustezza e cibersicurezza diventano condizioni di compatibilità dell'IA con lo Stato di diritto, soprattutto quando tali sistemi sono impiegati in settori ad alta incidenza sui diritti fondamentali, quali l'amministrazione pubblica, la giustizia, la sicurezza, la sanità e il lavoro.

2. *Le definizioni.*

2.1. *Il concetto di accuratezza: tra performance tecnica, affidabilità decisionale e tutela dei diritti fondamentali.*

Tra i requisiti previsti dall'art. 15, l'accuratezza occupa una posizione centrale e, al contempo, problematica. Il Regolamento non fornisce una definizione univoca e quantitativa del concetto, limitandosi a richiedere che i sistemi di IA ad alto rischio raggiungano livelli di accuratezza adeguati alla loro finalità e siano progettati in modo da ridurre il rischio di risultati errati.

Questa scelta normativa riflette una consapevole opzione di elasticità regolativa,

ma solleva rilevanti interrogativi sul piano giuridico. L'accuratezza, infatti, non può essere ridotta a un mero indicatore statistico o ingegneristico: essa assume una dimensione giuridica, in quanto incide direttamente sulla qualità delle decisioni che producono effetti giuridicamente rilevanti.

Dal punto di vista tecnico, l'accuratezza misura il grado di corrispondenza tra l'*output* del sistema e un risultato considerato corretto. Tuttavia, nel contesto dell'AI Act, essa deve essere valutata in relazione al contesto applicativo e agli interessi giuridici coinvolti. Un livello di accuratezza accettabile in un sistema di valutazione dell'affidabilità creditizia può risultare del tutto inadeguato in un ambito diverso come, ad esempio, quello della selezione del personale.

In questi casi, l'errore algoritmico non è un mero inconveniente tecnico, ma può tradursi in una lesione diretta di diritti fondamentali, in particolare del principio di eguaglianza e di non discriminazione. L'accuratezza diventa, così, un presidio contro decisioni arbitrarie o sistematicamente distorte, soprattutto quando tali distorsioni colpiscono gruppi vulnerabili o minoranze ed è necessario che venga valutata sulla base delle specifiche circostanze del caso concreto [1].

Sotto questo profilo, l'art. 15 si inserisce nel solco di una più ampia evoluzione del diritto europeo, che tende a riconoscere la necessità di standard di affidabilità rafforzati per gli strumenti tecnologici che incidono sull'esercizio dei diritti [2]. L'accuratezza non è più solo una qualità desiderabile, ma un obbligo giuridico funzionale alla tutela dei diritti.

Particolarmente rilevante è il rapporto tra accuratezza e principio di proporzionalità. Il Regolamento sembra presupporre che il livello di accuratezza richiesto debba essere commisurato a diversi fattori come la gravità dei potenziali impatti negativi, la natura automatizzata o assistiva della decisione, il grado di discrezionalità residua dell'operatore umano.

Ne deriva una concezione relazionale e contestuale dell'accuratezza, che si discosta da approcci rigidi e puramente quantitativi. Tuttavia, questa impostazione comporta il rischio di una indeterminatezza applicativa, demandando in larga misura a standard tecnici, linee guida e prassi delle autorità di vigilanza la concreta definizione delle soglie accettabili. In quest'ottica risulta importante tenere sempre in considerazione la necessità di non circondare l'intelligenza artificiale di quell'«aura di particolare esattezza e accuratezza» [3] che estrometterebbero

[1] H. NOLTE, M. RATEIKE, M FINK, *Robustness and Cybersecurity in the EU Artificial Intelligence Act*, in *ArXiv :2502.16184v1 [cs.AI]*, 22 febbraio 2025.

[2] Si pensi ad esempio all'attenzione data dall'art. 5, lett. d) del Regolamento UE 2016/679 (c.d. GDPR) all'esattezza e all'aggiornamento dei dati personali necessari per un loro corretto trattamento.

[3] Espressione di R. RORDORF, *Quale giustizia al tempo dell'intelligenza artificiale*, in *Questione giustizia,* 26 gennaio 2026.

del tutto il giudizio della persona umana [4]. Per queste ragioni è fondamentale che l'utente conosca il livello di accuratezza del sistema di IA che utilizza e le modalità con cui tale livello viene calcolato e aggiornato durante il suo ciclo di vita [5].

Dal punto di vista giuridico, l'accuratezza può essere letta come una declinazione tecnologica del dovere di buona amministrazione e di correttezza decisionale, applicabile tanto ai soggetti pubblici quanto ai privati che esercitano un potere di fatto sugli individui mediante sistemi di IA.

In questa prospettiva, l'accuratezza non tutela solo l'interesse individuale a una decisione "corretta", ma contribuisce a preservare la legittimazione complessiva dell'uso dell'IA in una società democratica fondata sul rispetto dei diritti fondamentali [6].

2.2. *La robustezza dei sistemi di IA: resilienza tecnica e prevenzione dell'errore sistemico.*

Nel quadro dell'art. 15 del Regolamento europeo sull'intelligenza artificiale, la robustezza può essere definita come la capacità di un sistema di IA di mantenere prestazioni affidabili e conformi alla sua finalità anche in presenza di condizioni avverse, variabili o non previste, incluse imperfezioni dei dati, contesti operativi mutevoli e interazioni improprie o abusive [7].

Si tratta di una nozione che trascende la mera stabilità tecnica del sistema e assume una chiara valenza giuridica, in quanto strettamente connessa alla prevenzione di decisioni errate, arbitrarie o imprevedibili che possono incidere sui diritti fondamentali.

Anche con riferimento alla nozione di robustezza il Regolamento non fornisce una definizione positiva e puntuale, ma ne delinea i contorni attraverso una serie di obblighi funzionali, imponendo che i sistemi di IA ad alto rischio siano progettati e sviluppati in modo tale da funzionare in modo coerente rispetto alla loro

---

[4] I.P. DI CIOMMO, *La prospettiva del controllo nell'era dell'Intelligenza Artificiale. Alcune osservazioni sul modello Human In The Loop,* in *Federalismi*, n. 9/2023, p. 68 ss.

[5] In questo senso si veda F. GALLI, G. CONTISSA, G. SARTOR, *I sistemi di AI ad alto rischio,* in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'Intelligenza artificiale,* Luiss University Press, Roma, 2025, p. 168.

[6] Secondo alcuni il rispetto del requisito dell'accuratezza sarà garantito dal Comitato Europeo per l'intelligenza artificiale che attraverso propri provvedimenti dovrà dare coerenza alle varie discipline; in questo senso si v. F. LORÈ, *I sistemi di IA*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il Regolamento europeo sull'intelligenza artificiale*, Maggioli, Rimini, 2024, p. 409.

[7] A. TOCCHETTI *et al.*, *AI robustness: a human-centered perspective on technological challenges and opportunities*, in *ACM Computing Surveys*, 57(6), 2024, p. 1 ss.

finalità dichiarata; reagire adeguatamente a input anomali o incompleti; evitare comportamenti inattesi o deviazioni significative delle prestazioni nel tempo.

Questa impostazione conferma come la robustezza non debba essere intesa esclusivamente in termini di resistenza tecnica al guasto, ma come un requisito volto a garantire la continuità della legalità tecnologica del sistema.

Dal punto di vista tecnico, la robustezza si riferisce alla capacità del sistema di tollerare errori, rumore nei dati, variazioni ambientali e condizioni operative non ideali. Tuttavia, nel contesto dell'AI Act, essa assume una dimensione ulteriormente qualificata: un sistema non è robusto solo se "non si rompe", ma se non produce risultati giuridicamente inaccettabili quando opera ai margini delle condizioni per cui è stato originariamente addestrato.

In questa prospettiva, la robustezza si distingue dall'accuratezza, pur essendo con essa strettamente interrelata. Mentre l'accuratezza misura la correttezza media o attesa degli *output*, la robustezza riguarda la stabilità delle prestazioni nel tempo e nello spazio, nonché la capacità del sistema di evitare errori gravi in situazioni anomale.

Un sistema altamente accurato in condizioni ideali, ma incline a fallimenti improvvisi o distorsioni significative in contesti reali, non può essere considerato robusto ai sensi dell'art. 15.

Sotto il profilo giuridico, la robustezza assume rilievo quale presidio contro l'errore sistemico, ossia contro quelle forme di malfunzionamento strutturale che non si manifestano come eventi isolati, ma come *pattern* ripetuti e prevedibili di errore.

Tali errori sono particolarmente problematici quando incidono su diritti fondamentali, poiché possono colpire in modo sproporzionato determinati gruppi di individui, generando discriminazioni indirette o trattamenti differenziati non giustificati.

La robustezza, in questo senso, impone che il sistema mantenga un comportamento coerente e non distorsivo anche al variare delle caratteristiche degli utenti o dei contesti applicativi. La mancanza di robustezza può tradursi in una forma di arbitrarietà tecnologica incompatibile con i principi dello Stato di diritto.

Un ulteriore profilo qualificante della robustezza riguarda la prevedibilità del comportamento del sistema, elemento essenziale per la legalità dell'azione amministrativa e, più in generale, per l'esercizio di poteri che incidono sulla sfera giuridica degli individui.

Un sistema di IA che reagisce in modo imprevedibile a input marginali o a variazioni minime del contesto compromette la possibilità di controllo umano effettivo e rende difficoltosa la contestazione delle decisioni adottate.

In tale ottica, la robustezza si pone in rapporto di complementarità con gli obblighi di sorveglianza umana previsti dall'art. 14 dell'AI Act: solo sistemi

sufficientemente robusti consentono un intervento umano significativo e informato, evitando che l'operatore si trovi di fronte a comportamenti opachi o erratici.

Infine, la robustezza assume rilievo anche sul piano della responsabilità giuridica. Essa può essere intesa come criterio di valutazione della diligenza tecnica e organizzativa del fornitore del sistema di IA. L'assenza di misure idonee a garantire la robustezza può costituire un indice di negligenza nella progettazione o nella gestione del rischio, con conseguenze rilevanti in termini di imputazione della responsabilità per danni derivanti dall'uso del sistema.

In conclusione, la robustezza, così come delineata dall'art. 15, rappresenta un ponte concettuale tra ingegneria del software e diritto, traducendo esigenze di stabilità tecnica in garanzie giuridiche contro l'arbitrarietà tecnologica. Essa contribuisce a definire i confini entro i quali l'uso dell'IA può considerarsi compatibile con i principi fondamentali dell'ordinamento europeo, rafforzando l'idea che l'affidabilità dei sistemi di IA non sia un mero requisito tecnico, ma una condizione di legittimità democratica.

2.3. *La cibersicurezza come requisito giuridico: protezione contro attacchi, manipolazioni e interferenze esterne.*

Nel contesto dell'art. 15 del Regolamento europeo sull'intelligenza artificiale, la cibersicurezza può essere definita come l'insieme delle misure tecniche e organizzative volte a proteggere i sistemi di IA da accessi non autorizzati, attacchi informatici, manipolazioni dei dati e interferenze esterne capaci di comprometterne il funzionamento, l'integrità e l'affidabilità [8].

Si tratta di una nozione che, pur affondando le proprie radici nel diritto della sicurezza informatica, assume nel quadro dell'AI Act una specifica qualificazione giuridica, in quanto funzionalmente orientata alla tutela dei diritti fondamentali potenzialmente incisi dall'uso dell'IA.

Il Regolamento richiede che i sistemi di IA ad alto rischio siano progettati e sviluppati tenendo conto di minacce ragionevolmente prevedibili alla sicurezza informatica, includendo sia attacchi deliberati sia vulnerabilità accidentali. In questo senso, la cibersicurezza non è concepita come una protezione meramente reattiva, ma come un requisito strutturale e preventivo, da integrare sin dalle fasi iniziali del ciclo di vita del sistema.

---

[8] Similmente nel diritto costituzionale il concetto di sicurezza è stato collegato a quello di ordine pubblico o quale componente del diritto rispetto a cui la sicurezza è richiesta, in questo senso si veda C. LOTTA, Governance *della rete, accesso a internet e cybersicurezza*, Editoriale Scientifica, Napoli, 2024, p. 177 ss.

Dal punto di vista sistematico, la cibersicurezza si colloca in una posizione di cerniera tra la dimensione tecnica dell'affidabilità del sistema e la dimensione giuridica della protezione dei diritti. Un sistema di IA vulnerabile ad attacchi informatici non compromette solo la continuità del servizio o la riservatezza dei dati, ma rischia di produrre decisioni alterate o manipolate, con effetti diretti sulla sfera giuridica degli individui.

In tale prospettiva, la cibersicurezza si distingue, pur essendo strettamente connessa, dalla robustezza. Mentre quest'ultima attiene principalmente alla capacità del sistema di reagire a condizioni operative avverse o impreviste, la cibersicurezza riguarda la resistenza del sistema a interferenze intenzionali, volte a modificarne il comportamento o a sfruttarne le vulnerabilità.

La distinzione è concettualmente rilevante: un sistema può essere robusto rispetto a errori accidentali, ma al contempo fragile rispetto ad attacchi mirati che ne alterino gli *output* o ne compromettano i meccanismi di controllo.

Dal punto di vista dei diritti fondamentali, la rilevanza della cibersicurezza è particolarmente evidente in relazione alla protezione dei dati personali, alla tutela della vita privata e alla sicurezza degli individui. Gli attacchi ai sistemi di IA possono infatti manifestarsi in diversi modi come, ad esempio, in accessi illegittimi che compromettono dati sensibili, in manipolazioni dei *dataset* di addestramento o dei parametri del modello, in alterazioni degli *output* decisionali in modo selettivo o discriminatorio.

In tali ipotesi, il rischio non è solo quello di una violazione della riservatezza, ma quello di una compromissione dell'equità e della legalità delle decisioni automatizzate, con conseguente lesione del principio di eguaglianza e del diritto a un trattamento equo.

La cibersicurezza assume, inoltre, una valenza specifica nei contesti in cui i sistemi di IA sono impiegati per l'esercizio di funzioni pubbliche o para-pubbliche. In tali ambiti, la vulnerabilità del sistema può tradursi in una minaccia alla fiducia dei cittadini nelle istituzioni e alla stessa legittimazione dell'azione pubblica.

Ne deriva che la sicurezza informatica dei sistemi di IA non può essere considerata un interesse esclusivamente del fornitore o dell'utilizzatore, ma un bene giuridico di rilevanza collettiva, strettamente connesso al corretto funzionamento dello Stato di diritto.

Sotto il profilo normativo, l'art. 15 AI Act si inserisce in un quadro europeo già articolato in materia di cibersicurezza, dialogando con la disciplina sulla sicurezza delle reti e dei sistemi informativi [9] e con il Regolamento generale sulla

[9] Si pensi ad esempio alla Direttiva 2013/40/UE del Parlamento europeo e del Consiglio sugli attacchi contro i sistemi di informazione che ha portato alla modifica di alcune fattispecie

protezione dei dati (c.d. GDPR). Tuttavia, il contributo specifico dell'AI Act consiste nel riconoscere che la vulnerabilità informatica di un sistema di IA può avere effetti sostanziali sui diritti, indipendentemente dalla presenza di una violazione dei dati in senso stretto.

In questa prospettiva, la cibersicurezza diventa un criterio di valutazione della legittimità dell'uso dell'IA, imponendo ai fornitori un dovere rafforzato di prevenzione delle minacce e di aggiornamento continuo delle misure di sicurezza [10].

La previsione di un obbligo di protezione contro interferenze esterne contribuisce a ridurre il rischio che l'IA diventi uno strumento di abuso, manipolazione o controllo arbitrario, sia da parte di attori privati sia da parte di soggetti terzi.

In conclusione, la cibersicurezza, così come configurata dall'art. 15, non rappresenta un mero requisito tecnico accessorio, ma una condizione essenziale per la tutela dei diritti fondamentali nell'ecosistema dell'intelligenza artificiale. Essa rafforza l'idea che l'affidabilità dell'IA non possa prescindere dalla sua protezione contro minacce esterne e che la sicurezza informatica debba essere considerata parte integrante del costituzionalismo digitale europeo.

3. *L'interrelazione tra accuratezza, robustezza e cibersicurezza e il loro ruolo nella prevenzione di violazione dei diritti.*

Accuratezza, robustezza e cibersicurezza, pur essendo concetti distinti sul piano tecnico, sono configurati dall'art. 15 del Regolamento europeo sull'intelligenza artificiale come requisiti intrinsecamente interconnessi, la cui efficacia dipende dalla loro applicazione congiunta e coordinata. Il legislatore europeo non li concepisce come standard autonomi, ma come componenti complementari di un'unica architettura di garanzia, finalizzata a ridurre il rischio che i sistemi di IA ad alto rischio producano effetti lesivi sui diritti fondamentali.

Sul piano funzionale, e riassumendo quanto già sostenuto, l'accuratezza rappresenta la condizione minima di affidabilità dell'*output* decisionale; la robustezza assicura la stabilità e la coerenza di tale *output* al variare delle condizioni operative; la cibersicurezza protegge il sistema da interferenze esterne in grado di alterarne il comportamento.

---

del nostro codice penale. Un intervento di più ampio respiro da parte dell'Unione europea si è poi avuto con la Direttiva 2022/25555 (c.d. NIS 2).

[10] In questo modo il campo dell'intelligenza artificiale diventa l'ambito entro cui è possibile sviluppare nuove tecniche per contrastare le future minacce informatiche; così F. AMENDOLA, P. SFERLAZZA, *Intelligenza artificiale e cybersicurezza*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il Regolamento europeo sull'intelligenza artificiale*, cit., p. 280.

L'assenza o l'insufficienza di uno solo di questi requisiti è idonea a compromettere l'effettività degli altri, generando una vulnerabilità sistemica che può tradursi in decisioni errate, arbitrarie o manipolate.

Questa interrelazione emerge con particolare evidenza se si considera che un sistema accurato, ma non robusto, rischia di produrre risultati inattendibili in contesti reali complessi; allo stesso modo, un sistema robusto ma vulnerabile sotto il profilo della cibersicurezza può essere deliberatamente indotto a fornire *output* distorti; infine, un sistema sicuro e robusto, ma strutturalmente inaccurato, continuerà a generare decisioni ingiuste o discriminatorie.

Ne deriva che la tutela dei diritti fondamentali non può essere affidata a un singolo parametro tecnico, ma richiede una valutazione integrata dell'affidabilità complessiva del sistema di IA.

Dal punto di vista giuridico, tale interrelazione consente di leggere l'art. 15 come una disposizione volta a prevenire non tanto il singolo errore, quanto il rischio strutturale di violazione dei diritti. Il legislatore europeo sembra muovere dalla consapevolezza che, nel contesto dell'IA, il danno non deriva necessariamente da un malfunzionamento occasionale, ma dalla combinazione di fattori tecnici che, se non adeguatamente governati, possono produrre effetti sistematici e difficilmente reversibili.

In questo senso, accuratezza, robustezza e cibersicurezza svolgono una funzione di prevenzione *ex ante* delle violazioni, anticipando la tutela rispetto al momento in cui il diritto leso potrebbe essere fatto valere in sede giurisdizionale. Tale impostazione risulta particolarmente significativa alla luce delle difficoltà, spesso evidenziate in dottrina, di accertare e dimostrare *ex post* il nesso causale tra decisione algoritmica e lesione del diritto, soprattutto in presenza di sistemi complessi o opachi.

L'interazione tra i tre requisiti contribuisce, inoltre, a rafforzare la prevedibilità e controllabilità delle decisioni automatizzate, elementi essenziali per la salvaguardia del principio di legalità e del diritto a un ricorso effettivo. Un sistema che opera in modo accurato e protetto da interferenze esterne consente infatti una maggiore tracciabilità delle scelte decisionali e una più agevole individuazione delle responsabilità in caso di errore.

Sotto questo profilo, l'art. 15 può essere letto come una norma che, pur non disciplinando direttamente i rimedi giurisdizionali, contribuisce indirettamente a renderli effettivi, riducendo il rischio che le decisioni algoritmiche si sottraggano al controllo giuridico. L'affidabilità tecnica del sistema diventa così un presupposto della giustiziabilità delle decisioni automatizzate.

Particolarmente rilevante è anche il ruolo che l'interrelazione tra accuratezza, robustezza e cibersicurezza svolge nella prevenzione delle discriminazioni. Errori

sistematici, instabilità del modello o manipolazioni dei dati possono colpire in modo sproporzionato determinati gruppi di individui, producendo effetti incompatibili con il principio di eguaglianza.

L'art. 15, letto in combinazione con gli altri requisiti del Capo III, contribuisce a costruire un argine normativo contro la cristallizzazione tecnologica delle disuguaglianze, imponendo standard di affidabilità che tengano conto della pluralità dei contesti e degli utenti.

In definitiva, l'interrelazione tra accuratezza, robustezza e cibersicurezza consente di qualificare l'art. 15 come una norma di garanzia sistemica, che traduce in requisiti tecnici operativi le esigenze di tutela dei diritti fondamentali proprie del costituzionalismo europeo.

Tali requisiti non esauriscono, evidentemente, il problema della legittimità dell'IA, ma rappresentano un fondamento imprescindibile per un uso della tecnologia compatibile con i valori democratici, confermando l'idea che, nell'era dell'intelligenza artificiale, la protezione dei diritti passa anche, e sempre più, attraverso la qualità e la sicurezza delle infrastrutture tecnologiche.

Riferimenti bibliografici.

AMENDOLA F., SFERLAZZA P., *Intelligenza artificiale e cybersicurezza*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il Regolamento europeo sull'intelligenza artificiale*, Maggioli, Rimini, 2024.

DI CIOMMO I.P., *La prospettiva del controllo nell'era dell'Intelligenza Artificiale. Alcune osservazioni sul modello Human In The Loop,* in *Federalismi*, n. 9/2023.

GALLI F., CONTISSA G., SARTOR G., *I sistemi di AI ad alto rischio,* in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'Intelligenza artificiale,* Luiss University Press, Roma, 2025.

LORÈ F. *I sistemi di IA*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il Regolamento europeo sull'intelligenza artificiale*, Maggioli, Rimini, 2024.

LOTTA C., Governance *della rete, accesso a internet e cybersicurezza*, Editoriale Scientifica, Napoli, 2024.

NOLTE H., RATEIKE M., FINK M., *Robustness and Cybersecurity in the EU Artificial Intelligence Act*, in *ArXiv :2502.16184v1 [cs.AI]*, 22 febbraio 2025.

RORDORF R., *Quale giustizia al tempo dell'intelligenza artificiale*, in *Questione giustizia,* 26 gennaio 2026.

TOCCHETTI A. *et al.*, *AI robustness: a human-centered perspective on technological challenges and opportunities*, in *ACM Computing Surveys*, 57(6), 2024.