Il bollettino dell'Osservatorio sulla legalità
n. 15/2025

L'OSLE ieri e oggi: le forme della legalità in mutamento

di Giuseppe Acocella e Giovanni D'Alessandro

L'Osservatorio sulla legalità (OSLE) nasce nel 2013 all'interno dell'Istituto di Studi Politici "S. Pio V" con l'obiettivo di promuovere una riflessione sistematica e documentata sui processi di trasformazione della legalità in Italia. La scelta d'istituire un osservatorio dedicato rispondeva all'esigenza di dotarsi di uno strumento capace di registrare e interpretare la distanza, talvolta considerevole, tra legalità formale e legalità praticata, interrogando al contempo le forme in cui la legalità può essere manipolata, compromessa o ristabilita.

L'OSLE ha assunto sin dall'inizio un orientamento metodologico fondato sull'analisi comparata dei fenomeni istituzionali, giuridici e sociali, nella consapevolezza che la legalità non è un principio astratto, bensì una trama di regole e comportamenti che dipende tanto dalla configurazione dell'ordinamento quanto dalle pratiche sociali condivise.

In questo quadro si colloca la pubblicazione del Bollettino dell'OSLE, che costituisce uno dei principali strumenti di lavoro dell'Osservatorio. Il Bollettino non è soltanto un resoconto dell'attività scientifica interna, ma un laboratorio permanente di discussione, in cui studiosi di diritto, filosofia politica, sociologia, storia delle istituzioni, comunicazione pubblica e politiche sociali collaborano alla ricostruzione interpretativa degli snodi della legalità contemporanea. La struttura del Bollettino riflette questa pluralità: le diverse sezioni sono affidate a studiosi responsabili di un settore disciplinare specifico oppure a esperti esterni, a cui è demandata la ricognizione di fenomeni emergenti, la lettura critica della produzione normativa e la valutazione degli effetti che mutamenti istituzionali o culturali esercitano sulla tenuta della legalità.

Già i primi numeri pubblicati davano conto di una linea di ricerca coerente. In essi si affrontavano le tensioni strutturali tra potere giudiziario e sistema politico, le difficoltà operative della pubblica amministrazione, le forme d'illegalità radicate nel tessuto sociale e le dinamiche di percezione della giustizia nella sfera pubblica. Questi primi fascicoli rivelavano una caratteristica che sarebbe rimasta costante negli anni successivi: l'intenzione di legare la ricostruzione concettuale alla dimensione fattuale, evitando sia l'astrazione teorica priva di riscontro sia la mera cronaca.

La continuità di questa impostazione ha permesso al Bollettino di attraversare le fasi di forte trasformazione che hanno interessato la democrazia costituzionale negli

ultimi anni, segnatamente durante e dopo la pandemia. L'analisi delle misure emergenziali, del rapporto tra autorità pubblica e libertà individuali, della produzione normativa accelerata e della ridefinizione dell'idea stessa di responsabilità ha attestato la capacità dell'OSLE d'interrogare la legalità come una forma storicamente situata di regolazione del potere e delle relazioni sociali e non come un insieme statico di garanzie.

Il Bollettino rappresenta un esercizio di osservazione continua della realtà istituzionale e sociale, condotto con strumenti concettuali che appartengono alla tradizione della cultura giuridica italiana e si misurano, allo stesso tempo, con fenomeni nuovi e in trasformazione. Ciò consente di leggere la legalità come un campo di tensione nel quale intervengono attori istituzionali, culture politiche e forme di legittimazione, senza ridurla a mero vincolo normativo.

La continuità del Bollettino negli anni successivi consente di osservare un progressivo affinamento della prospettiva di ricerca, segnato da una crescente attenzione ai nessi strutturali tra legalità, forma di governo e produzione normativa.

Segnatamente, a partire dal 2021 emergono con chiarezza alcuni temi ricorrenti: la crisi della magistratura e della sua legittimazione, il rapporto tra politica e potere giudiziario, l'impatto delle emergenze — sanitarie, securitarie o economiche — sulla configurazione delle libertà fondamentali e sulle tecniche di governo, nonché la tensione tra effettività del diritto e fiducia nelle istituzioni.

Il Bollettino n. 8/2021 segna un punto di svolta, poiché ha affrontato gli effetti della pandemia da Covid-19 come evento sanitario e, al contempo, come esperienza di rilievo costituzionale. Il ricorso diffuso a strumenti normativi emergenziali, l'accentramento delle funzioni decisionali, la giustificazione della compressione dei diritti fondamentali in nome dell'interesse pubblico e la trasformazione della comunicazione istituzionale in funzione regolativa vengono analizzati come indizi della fragilità delle coordinate che definiscono la legalità democratica. La pandemia diviene così il banco di prova di un equilibrio tra libertà e sicurezza che non può più darsi per acquisito.

Successivamente, il Bollettino n. 10/2022 ha affrontato la questione della crisi della magistratura in senso più diretto. La vicenda del c.d. "caso Palamara" e la percezione del ruolo dei magistrati nella sfera pubblica palesano come l'indipendenza del potere giudiziario, pur formalmente garantita, possa essere messa in discussione da dinamiche interne al corpo giudiziario e dal rapporto con i media. Ciò ha indotto e induce a interrogare il principio di legalità nella sua

dimensione normativa costituzionale e nella sua capacità di mantenere credibilità operativa. L'indebolimento della fiducia nelle istituzioni giudiziarie costituisce, in questa prospettiva, un sintomo della tensione tra giustizia come funzione e giustizia come potere e non un mero problema comunicativo.

Il Bollettino n. 11/2023 ha poi ampliato lo sguardo, individuando i nessi tra legalità e mutamenti sociali. Fenomeni quali la devianza minorile, le mobilitazioni giovanili nelle periferie urbane e le trasformazioni del linguaggio politico nei nuovi media vengono analizzati come indicatori di un mutamento profondo delle forme di socializzazione alla legalità. E non certo in chiave solo emergenziale.

La legalità appare non più garantita dall'autorità delle istituzioni, quanto dipendente da un processo d'internalizzazione di norme e pratiche che risulta oggi meno stabile e più frammentato. In tal senso, il richiamo alla "cultura della legalità" non è retorico. Piuttosto segnala la necessità di una riflessione sulle condizioni che rendono possibile la condivisione di regole comuni in una società pluralistica.

Nei Bollettini n. 12/2024 e n. 13/2024 emergono in modo crescente i temi legati alle tecnologie digitali, alla regolazione europea dell'intelligenza artificiale e alle forme con cui la trasformazione tecnologica incide sulle strutture della decisione pubblica. La questione non è presentata come problema meramente tecnico, né come esito meccanico del progresso tecnologico: essa riguarda la ridefinizione del rapporto tra autorità pubblica e capacità di previsione, tra autonomia individuale e architettura degli ambienti digitali, tra responsabilità politica e automatismi regolativi. Il digitale diventa così una dimensione in cui osservare la ridefinizione stessa della legalità e delle forme di esercizio del potere.

Attraverso questi passaggi, il Bollettino palesa un tratto metodologico distintivo, vale a dire l'attenzione alle transizioni, ai punti in cui l'ordinamento si misura con eventi o fenomeni che non sono ancora incasellati nelle categorie tradizionali. La legalità, in questo senso, non viene osservata come un insieme di norme, quanto come una forma di equilibrio tra potere, regole e consenso, continuamente sottoposta a tensione.

Il più recente sviluppo delle attività dell'Osservatorio si concentra sulle trasformazioni della legalità nell'età digitale. I Bollettini degli ultimi due anni rivelano come l'introduzione di tecnologie predittive, di sistemi automatizzati di decisione pubblica e di infrastrutture normative europee sempre più pervasive stia incidendo non tanto sui contenuti del diritto, quanto sulla forma stessa della legalità. Il problema non riguarda soltanto la possibilità di delegare funzioni

valutative o regolative a sistemi artificiali, ma anche la ridefinizione del rapporto tra certezza, responsabilità e controllo.
L'attenzione riservata al quadro regolatorio europeo — dal GDPR al *Digital Services Act*, dal *Digital Markets Act* sino all'*AI Act* — mette in luce, in particolare, una tensione strutturale tra il principio di precauzione e la tutela della libertà individuale. La spinta verso un'architettura preventiva della legalità tende a sovrapporre garanzia e controllo, difesa e gestione anticipata del rischio, con l'effetto di trasformare la protezione dei diritti in un dispositivo amministrativo di vigilanza. Il riferimento ai modelli di sorveglianza predittiva e alla possibilità di vietare o classificare come ad "alto rischio" alcuni usi dell'intelligenza artificiale dimostra come l'Europa si trovi oggi a ridefinire le condizioni stesse della libertà, nella misura in cui ciò che è tutelato è il contenuto dei diritti assieme alla forma con cui essi possono essere esercitati.
La legalità appare così collocata all'incrocio fra tre dimensioni: la normatività costituzionale, la razionalità amministrativa e le architetture tecnologiche dell'informazione. Ciò richiede di ripensare la funzione dell'interpretazione giuridica, la posizione delle corti e la responsabilità politica delle istituzioni. Si tratta di comprendere come la legalità, per restare principio politico oltre che giuridico, debba essere continuamente restituita alla sua dimensione di scelta e non ridotta a mera gestione, senza rivendicare una presunta purezza originaria della legge o aderire acriticamente alle logiche regolative del presente.
L'Osservatorio non assume la legalità come categoria statica, né come formula già data e applicabile *per deductionem*; la legalità è considerata come una pratica istituzionale e sociale, radicata nella storia costituzionale e nondimeno sempre esposta alle trasformazioni della società e del potere. Di fronte alle emergenze, ai mutamenti tecnologici, alle crisi di fiducia, il Bollettino si pone come luogo d'indagine critica, in cui la vigilanza sulla legalità non coincide con un guardiano morale o con un presidio ideologico, ma con la capacità di riconoscere i punti di torsione in cui la forma giuridica rischia di perdere memoria di sé.
Se le democrazie rappresentative attraversano oggi una fase di fragilità, lo spazio della legalità non può essere affidato né al tecnicismo regolativo né alla reazione emotiva. La legalità vive laddove si ricostruisce il legame tra regole e responsabilità, tra autorità e fiducia, tra istituzioni e coscienza della comunità.
È in questa direzione che s'inserisce anche il Bollettino attuale, dedicato alla trasformazione della legalità nell'ambiente digitale. L'attenzione rivolta alle forme

dell'intelligenza artificiale, ai sistemi decisionali automatizzati e alle nuove architetture regolative europee non è orientata a celebrarne le potenzialità né a denunciarne i rischi in tono allarmistico. Si tratta, piuttosto, di comprendere come la legalità si riconfiguri quando l'azione pubblica si articola attraverso flussi informativi, infrastrutture algoritmiche e dispositivi di classificazione preventiva. La digitalizzazione della vita collettiva modifica il rapporto tra regole, responsabilità e decisione, trasferendo in parte la razionalità del diritto su strumenti che operano per correlazione più che per giudizio.

Il Bollettino mette in evidenza come la sfida non ruoti attorno al contenimento della tecnologia né all'attribuzione ad essa di funzioni di governo. La questione riguarda piuttosto le condizioni che permettono di imputare correttamente le decisioni pubbliche in un contesto in cui i nessi tra causa ed effetto, tra individuo e azione, tra scelta e conseguenza appaiono meno immediati. In questo quadro, la legalità richiede un assetto che eviti tanto la riduzione a un catalogo di vincoli quanto l'estensione verso forme di controllo anticipatorio.

La democrazia deve confrontarsi con poteri che operano attraverso la previsione dei comportamenti e la modulazione degli ambienti informativi. Dentro questo scenario, la legalità diventa il luogo in cui chiarire che cosa significhi decidere, agire e rispondere in un ambiente digitale.

Il Bollettino mantiene, su questo terreno, una linea coerente: considera la legalità come dimensione attraverso cui si forma la convivenza politica, non come repertorio di formule. In tempi in cui l'esercizio del potere può assumere forme opache e la regolazione tende a sovrapporsi alla gestione del rischio, la cura della legalità diventa una condizione per preservare la leggibilità del sistema democratico.

L'edizione attuale offre così una riflessione sulle modalità con cui, anche nell'ecosistema digitale, la legalità può continuare a fornire il quadro entro cui la libertà trova il proprio spazio di azione. È questa, probabilmente, la necessità più esposta del presente: mostrare che la legalità costituisce l'elemento che permette alla libertà di dispiegarsi, e non un vincolo che ne limita la portata.

La legge è eguale per tutti?
di Giuseppe Acocella

Negli ultimi tempi il principio di legalità appare scosso da una nuova insidia dal sapore antico: la legge ingiusta. Se il dettato di una norma non corrisponde ai propri desideri, alle pulsioni profonde o alle proprie inclinazioni politiche basta bollare la norma con l'infamante definizione dl legge ingiusta per decretarne la inapplicabilità, in nome di principi di giustizia dal singolo individuo proclamati come irrinunciabili, e dunque superiori alla norma che si intende disapplicare. L'arbitrio individuale diventa così legislatore universale (in nome della coscienza personale, elevata a supremo legislatore) e il non meglio definito diritto umanitario globale (?) superiore ad ogni certezza del diritto.
Così, in nome della legge ingiusta la certezza del diritto (e delle leggi) perde la sua funzione di garanzia per ogni cittadino, a dispetto del suo storico ruolo di architrave dello Stato di diritto nell'età contemporanea. La rassicurante realtà del diritto eguale per tutti (scopo precipuo della democrazia e resa possibile dal fatto che le norme siano legittimamente prodotte in un regime democratico, e dunque modificabili da assemblee elette attraverso libere consultazioni a ciò deputate), è negata alla radice quando invece norme perverse – come mostrò il processo di Norimberga, generando così una svolta nella civiltà giuridica – possono legittimamente essere respinte e rifiutate ove assecondino l'arbitrio di un barbaro regime totalitario che le producesse, bollandole – una volta private della possibilità di modifica democratica -come leggi ingiuste frutto di regimi non legittimati da libere elezioni.
La Resistenza, che anche il nostro paese conobbe contro l'invasione nazifascista, – costituendo la premessa della democrazia costituzionale in Italia come in altre nazioni – entra in questa prospettiva del giudizio legittimo sulla legge ingiusta, non frutto dunque di arbitrio generato dalla presunzione individualistica, ma scelta di popolo nutrita dalla socialità della convinzione profonda che tutto si fondi sul principio di eguaglianza. Invece l'esasperato individualismo dei nostri tempi vuole mettere a tacere, addirittura oscurandoli, i diritti sociali (in specie dei lavoratori), sostituiti dall'esaltazione della tutela intollerante dei diritti individuali borghesi. La democrazia – che non tollera coniugazioni faziose, come quelle che dichiarano, in virtù di schieramenti di parte, illiberali assetti politici pur scaturiti da libere elezioni non manipolate – quando non ha attraversato la liberaldemocrazia, non ha potuto assumere i caratteri storici che generano Stato di diritto e suffragio universale. Se vi sono

democrazie, esse non possono essere illiberali (la cui definizione non può essere determinata a piacimento di chiunque sia politicamente schierato). La legalità è assicurata dai regimi liberaldemocratici adottanti procedure legittime.
L'arbitrio individuale si camuffa così, nel tentativo di nobilitarsi, come coscienza individuale, autorizzata da *sé* stessa a ergersi a giudice universale della pubblica e privata moralità in nome di un male inteso primato della politica, chiamato a rendere superiori alla legge anche la faziosità o le ragioni di schieramento politico. La coscienza può così coprire qualunque opzione (se una teoria politica dichiara che la proprietà è un furto può questo diventare negazione quotidiana delle leggi sul furto o sulla distruzione di beni privati?), assolvendosi, in quanto portatrice di moralità superiore alle leggi comuni. Il principio che recita che la legge è eguale per tutti viene in questo modo definitivamente liquidato, e diritto e legalità perdono significato e consistenza storica e logica.

La legalità come responsabilità sistemica: quando la prevenzione diventa tutela

di Gaia Fristachi

Rosa D'Ascenzo, Maria Rus, Delia Zarniscu, Teresa Sartori, Elisa Scavone, Ester Palmieri, Annalisa Rizzo, Silvana Bucci. Questi sono solo alcuni dei volti di donne che nel 2024 hanno perso la vita in seguito a violenza di genere in Italia. Dietro ogni nome c'è una storia interrotta, un futuro spezzato, una comunità che piange una perdita irreparabile. Secondo l'Osservatorio Nazionale Non Una di Meno, nel 2024 sono stati registrati 98 femminicidi, a cui si aggiungono almeno altri 53 tentati femminicidi.[1] Accanto a queste tragedie, si affiancano le storie di giovani vittime di bullismo e cyberbullismo. Leonardo, 15 anni, si è tolto la vita nel 2024 a causa delle molestie subite dai compagni di scuola. Stando ai dati diffusi da ESPAD®Italia, nel 2024, oltre 1 milione di studenti italiani tra i 15 e i 19 anni ha subito episodi di cyberbullismo (47%). Il dato segna un record negativo, registrando il suo valore più alto di sempre, con una percentuale poco più alta tra i ragazzi (35%) rispetto alle ragazze (29%).[2]

Le statistiche ci mostrano un quadro inquietante: mentre i delitti violenti generali in Italia hanno registrato un lieve calo, i femminicidi e le violenze giovanili sono in aumento. Questi dati emergono chiaramente dal lavoro dell'Osservatorio Regionale della Legalità della Toscana, presentato nel 2025, che sottolinea come i reati in ambito familiare e giovanile richiedano non solo interventi repressivi ma soprattutto strategie preventive.[3]

Questi numeri delineano un quadro che non può più essere letto come emergenza locale o circoscritta. Bensì trattasi di dinamiche diffuse in tutto il paese, che riflettono un indebolimento sistemico della legalità in contesti familiari, educativi e comunitari. È dunque l'intero ordinamento nazionale a essere chiamato a una riflessione profonda sulla capacità delle proprie istituzioni di garantire sicurezza, tutela e prevenzione.

Dal punto di vista giuridico, l'Italia dispone di strumenti normativi significativi: la Legge n. 69/2019

[1] I dati raccolti dall'associazione socio-politica sono consultabili al seguente indirizzo web: https://osservatorionazionale.nonunadimeno.net/anno/2024/.

[2] Silvia Biagioni, Corrado Fizzarotti, Sabrina Molinaro (a cura di), ESPAD® Italia 2023. Navigare il futuro: dipendenze, comportamenti e stili di vita tra gli studenti italiani, Pisa, Istituto di Fisiologia Clinica – CNR, Laboratorio di Epidemiologia e Ricerca sui Servizi Sanitari, 2024, ISBN 978-88-7958-072-4.

[3] Federica Cioni, «Legalità: Rapporto osservatorio regionale, delitti violenti in calo ma aumentano femminicidi e violenze in famiglia», In Consiglio, 10 giugno 2025, https://inconsiglio.it/comunicato-stampa/legalita-rapporto-osservatorio-regionale-delitti-violenti-in-calo-ma-aumentano-femminicidi-e-violenze-in-famiglia/ (consultato il 27 ottobre 2025).

(nota come "Codice Rosso") ha introdotto misure urgenti per proteggere le vittime di violenza domestica e di genere, mentre la Legge n. 71/2017 ha riconosciuto la specificità del cyberbullismo come nuova forma di violenza digitale. Tuttavia, la distanza tra norma e attuazione rimane ampia: molte vittime, soprattutto giovani, non denunciano per paura o isolamento, mentre le comunità spesso non dispongono di percorsi di supporto sufficienti.[4] Dunque, nonostante l'impianto legislativo sia robusto, persistono lacune applicative e frammentazioni territoriali: la legalità, in questo senso, deve affermarsi non solo come principio normativo, ma come obiettivo di effettività istituzionale e dunque non come mero strumento di repressione ma come imprescindibile valore preventivo e sistemico.

Se non affrontati con urgenza, i fenomeni di femminicidio e violenza giovanile rischiano di evolversi in forme più gravi, generando un circolo vizioso di violenza e marginalizzazione. Servono percorsi di formazione giuridica e civica nelle scuole, campagne di sensibilizzazione coordinate a livello nazionale e un rafforzamento dei protocolli interistituzionali per la protezione delle vittime e il recupero degli autori di reato. La legalità, per essere reale, deve permeare il tessuto sociale, e non restare confinata alle aule dei tribunali.

Secondo le proiezioni degli esperti, l'incidenza dei femminicidi potrebbe stabilizzarsi solo con interventi mirati che integrino protezione, prevenzione e supporto psicologico alle vittime. Per quanto riguarda la violenza giovanile, la diffusione dei dispositivi digitali e dei social network rende indispensabile un'azione educativa costante, capace di formare cittadini consapevoli del rispetto delle norme e della dignità altrui. Le normative attualmente vigenti, nonché i diversi disegni di legge attualmente in discussione, uniti a iniziative locali e comunitarie, rappresentano la chiave per costruire una legalità attiva, capace di proteggere oggi e di educare al rispetto delle regole per il futuro.

La violenza, in tutte le sue forme, è una violazione della legalità che ferisce la società nel suo cuore. Ogni femminicidio, ogni caso di (cyber)bullismo, rappresenta non solo un crimine, ma un campanello d'allarme sul valore della responsabilità individuale e collettiva. Solo un impegno congiunto tra istituzioni, famiglie, scuole e comunità può restituire forza al principio di legalità come fondamento della convivenza democratica. Ogni

[4] Silvia Brunori, Luca Caterino (a cura di), Sedicesimo Rapporto sulla violenza di genere in Toscana. Un'analisi dei dati dei Centri e delle Reti Antiviolenza – Anno 2024, Firenze, Regione Toscana – Direzione Sanità, Welfare e Coesione Sociale, Osservatorio Sociale Regionale, 2024, ISBN 979-12-81783-089.

nome che ricordiamo è un impegno che rinnoviamo: la legalità non è solo legge, ma cura delle persone, dei loro diritti e del loro futuro.

Valori civili e legalità

di Stefano Sepe

«C'era un paese che si reggeva sull'illecito. […] Questo sistema, articolato su un gran numero di centri di potere, aveva bisogno di mezzi finanziari smisurati […] e questi mezzi si potevano avere solo illecitamente». Così si esprimeva Italo Calvino su *La Repubblica* del 15 marzo 1980. Molto è cambiato nel Paese, ma poco nella cultura e nei valori civilmente considerati. La sconsolata riflessione del grande intellettuale non era inedita nella storia italiana, ma avveniva pochi anni dopo la stagione politica, originata dallo scandalo di "mani pulite", in ragione del quale si verificò il crollo dei partiti politici che avevano governato (al centro come in periferia) per quasi trent'anni dalla nascita della Repubblica.

Il panorama delle forze politiche, nonché quello dei "gruppi di potere" è profondamente mutato, ma non sono scomparsi quei guasti lamentati da Calvino. In Italia la corruzione ha cambiato volto, ma non la sostanza. Da tempo questo modello di illegalità passa attraverso la "rete": le mutande (con la "d") del 1982 sono state sostituite dalle password dei conti correnti. È noto che l'infiltrazione della malavita organizzata si è sempre più consolidata – da molti anni – nel mondo degli affari. Anche qui si è passati dalla lupara e dalle stragi mafiose, alla presenza nei consigli di amministrazione e nelle alte sfere del sistema pubblico.

È accertato che l'attuale posizionamento dei protagonisti della corruzione – non soltanto quella presente nelle varie mafie – è frutto del mutato livello culturale della malavita. Non soltanto coppole storte, ma presenza sempre più ricorrenti di posizioni di vertice, sia nel settore pubblico che in quello privato. Di fronte a siffatto panorama emerge con chiarezza l'esigenza di strategie che incidano sulle modalità di contrasto della corruzione. A tal fine vengono da tempo rafforzate, all'interno delle forze dell'ordine, strutture tecniche e operative con competenze specifiche in grado di individuare e intercettare i fenomeni dell'illegalità.

È quasi superfluo rammentare che il diffondersi dell'intelligenza artificiale, mentre offre vantaggi nella vita quotidiana, può facilitare penetranti ricadute e abusi, che sfuggono al controllo da parte dei poteri pubblici, costituendosi come attività illegali. Le *fake news* sono già diventate terreno di costruzione di verità fasulle, attraverso l'utilizzo dell'intelligenza artificiale. In proposito, il limite che separa la legalità dall'illegalità si prospetta (anzi, si propone già oggi) incerto, difficile da decifrare e da incasellare nelle fattispecie di ordine giuridico. Ne resta danneggiata pesantemente l'etica pubblica, che

rischia di essere scompaginata da fenomeni di "alterità" rispetto ai canoni definiti negli ordinamenti delle società democratiche.
Naturalmente, sarebbe fuorviante descrivere le ricadute dovute alle potenzialità dell'intelligenza artificiale come origine dell'uso distorto che può esserne fatto. In tale contesto l'azione di contrasto delle attività di corruzione – che vengono compiute con gli strumenti dell'intelligenza artificiale – si è sempre più orientata a individuare e colpire le "reti" di comunicazione delle attività illegali. In merito occorre prendere atto che uno dei punti più deboli delle strategie tese a controllare il corretto uso delle tecnologie più avanzate è riscontrabile nell'incapacità dei governi di operare efficacemente a creare i necessari anticorpi alla estensione illimitata dell'intelligenza artificiale, sia nelle attività materiali, sia nella definizione di criteri oggettivi nel rapporto legalità/illegalità. Il terreno sembra potersi definire in salita, poiché la percezione della diffusione di un "costume [in]civile", che soffoca l'etica e la morale, alimenta il discredito dei principi fondamentali delle democrazie.
Per arginare il dilagare delle pratiche (e delle mentalità) illegali vanno sorrette le iniziative delle associazioni di cittadini, tese a diffondere in particolare – tra i giovani nelle scuole – la cultura della legalità. Tale meritoria opera di attività meriterebbe un sostegno adeguato dalle Istituzioni, per evitare che la spinta verso l'educazione civile venga soffocata dalla mancanza di mezzi. Lo sforzo di maggiore impatto spetta al ceto politico, dal quale i cittadini pretendono onestà e rigore morale. Ciò nonostante, occorre distinguere il grano dall'oglio, evitando generalizzazioni che vanificano le migliori intenzioni, riducendo le proteste contro la politica a un populismo tanto chiassoso e becero quanto inefficace. Il recupero dei valori deve necessariamente prendere le mosse da un'opera ostinata e tenace di "cultura" della legalità. Considerato nel suo insieme, l'orizzonte non è del tutto limpido, poiché il sistema politico del nostro Paese non brilla per integrità e, nel migliore dei casi, ritiene sufficiente a risolvere il problema unicamente attraverso le leggi. Storicamente, riguardo al rapporto tra Istituzioni e cittadini, risulta significativa l'opinione di Teresa Filangieri, sorella di Gaetano, filosofo e giurista napoletano. Nel corso di uno scambio di opinioni con Johann Goethe, la gentildonna ebbe a sostenere: «se fate delle nuove leggi, ci procurate nuove preoccupazioni: dovremo escogitare il modo di trasgredire anche quelle, dopo che ci siamo sbarazzati delle vecchie».

Qualche considerazione sul c.d. "scudo democratico"

di Niccolò Ferracuti

La libertà di voto è oggi minacciata da nuove forme di destabilizzazione e da manipolazioni sempre più sofisticate (*deepfake*, CIB, *social bot*, *account* fasulli, etc.), che propagano disinformazione e interferiscono con la regolarità dei processi elettorali.

In pochi mesi, solo tra la fine del 2024 e l'inizio del 2025, abbiamo assistito ad alcuni fatti di notevole importanza, talora senza precedenti: l'annullamento del primo turno delle elezioni presidenziali in Romania ad opera della Corte costituzionale romena, a causa di accertate interferenze esterne; l'ondata di disinformazione che ha colpito la Germania in occasione delle elezioni federali; i sospetti di interferenza russa nello svolgimento delle elezioni in Moldavia; il *ban* di TikTok in Albania in vista delle elezioni presidenziali e negli Stati Uniti.

Sempre più spesso viene invocata quindi nel dibattito pubblico l'idea di erigere uno "scudo democratico", che ponga l'elettore online al riparo dalla disinformazione, neutralizzi le azioni eversive di terzi e garantisca all'utente-elettore le premesse per il naturale sviluppo della propria libertà di opinione, al riparo da indebite interferenze e manipolazioni.

Lo scudo per la democrazia rappresenta un punto programmatico della Commissione europea che, nella primavera del 2025, ha lanciato una consultazione pubblica per raccogliere *feedback* e idee. Anche in Italia il tema è salito prepotentemente alla ribalta. Il 30 aprile 2025 è stato presentato al Senato un pacchetto di proposte per l'istituzione di uno scudo democratico. Si tratta di un disegno di legge costituzionale e di una proposta di legge ordinaria ad esso collegata. In sintesi, la legge costituzionale interverrebbe sull'art. 61 Cost. per attribuire al Parlamento in seduta comune, in caso di accertate interferenze esterne, manipolazioni o disinformazione, il potere di deliberare l'interruzione delle elezioni, se in corso di svolgimento, o di annullarne gli esiti se già svolte con la loro conseguente ripetizione. La deliberazione, adottata con un voto a maggioranza qualificata dei due terzi degli aventi diritto, sarebbe comunque ricorribile dinanzi alla Corte costituzionale. La legge ordinaria, invece, porrebbe a carico delle "società dell'informazione" (tra cui le piattaforme digitali) l'obbligo di costituire dei "comitati di analisi", con il compito di monitorare e contrastare le attività di ingerenza esterna volte a manipolare il consenso politico del potere di verificare i contenuti diffusi e di rimuovere quelli ingannevoli, oltre a segnalare e bloccare utenti coinvolti in attività di disinformazione

ripetuta. Questi comitati risponderebbero all'AGCOM, che vigilerebbe sul rispetto degli obblighi da parte delle piattaforme, e al DIS (Dipartimento delle informazioni per la sicurezza). L'Autorità e il DIS relazionerebbero poi alle Camere e alla Presidenza del Consiglio dei ministri.

Più di recente, poi, la legge italiana che regola l'utilizzo dell'AI (legge n. 132/2025), la prima di questo genere approvata in uno Stato membro dell'UE, ha espressamente stabilito che: «L'utilizzo di sistemi di intelligenza artificiale non deve pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica e l'esercizio delle competenze e funzioni delle istituzioni territoriali sulla base dei principi di autonomia e sussidiarietà e non deve altresì pregiudicare la libertà del dibattito democratico da interferenze illecite, da chiunque provocate, tutelando gli interessi della sovranità dello Stato nonché i diritti fondamentali di ogni cittadino riconosciuti dagli ordinamenti nazionale ed europeo».

Ora, il principale problema dell'istituzione di uno scudo democratico è la sua concreta strutturazione e articolazione: esso, infatti, dovrebbe essere "calato" nell'ordinamento senza stravolgere o compromettere il sistema dei pesi e contrappesi previsto dalla Costituzione, a tutela del principio di separazione dei poteri. A ciò si aggiunge la difficoltà di definire in modo univoco concetti quali "disinformazione", "ingerenza esterna" o "manipolazione": un terreno fertile per arbitrarietà e abusi nei casi controversi. Il rischio, insomma, è quello di istituire una sorta di "ministero della verità" orwelliano, che stabilisca con ampia discrezionalità cosa è *fake news* o disinformazione e diventi un potenziale bavaglio per opinioni scomode o dissenso politico, al di fuori di ogni controllo giudiziario.

Insomma, l'istituzione di uno scudo democratico non può prescindere dalla garanzia di un equilibrato bilanciamento tra la tutela della libertà di voto e la protezione della libertà di pensiero.

Da questo punto di vista, si osserva come i due principali sistemi-guida dell'Occidente, rappresentati dagli Stati uniti e dall'Unione europea, stiano adottando approcci profondamente differenti. Da un alto, l'UE ha profuso negli ultimi anni un ingente sforzo regolatorio, culminato in una variegata normativa di *hard law* (DMA, DSA, *AI Act*, *microtargeting* a scopo politico-elettorale), che pone obblighi stringenti a carico delle piattaforme online in tema di moderazione dei contenuti, libertà di concorrenza, uso dell'intelligenza artificiale e pubblicità politica. Si tratta di un approccio rigoroso criticato da chi vi intravede un rischio di *overregulation*, con potenziali impatti

negativi anche sulla libertà di parola. Negli Stati Uniti, invece, le principali piattaforme digitali hanno anzi annunciato che dal 2025 abbandoneranno il sistema di fact-checking in favore un modello decentrato che privilegia il libero flusso delle informazioni, dove la moderazione dei contenuti è affidata alle community notes degli utenti, accusando i *fact-checkers* di essere politicamente orientati e di limitare la libertà di pensiero.

In questa cornice, bisogna però resistere a due tentazioni e mantenere uno sguardo orientato al futuro. Da un lato, occorre resistere all'idea che per preservare la libertà di voto occorrano misure anomale, che potrebbero eventualmente scalfire o sacrificare irragionevolmente altri diritti fondamentali e che potrebbero nel medio-lungo periodo produrre effetti altrettanto dannosi per la salute della democrazia. Dall'altro lato, quando si affronta il problema di come strutturare uno scudo a difesa della democrazia contro i fenomeni di disinformazione e interferenze esterne sui processi elettorali nazionali, occorre rinnegare l'idea che il contrasto tra diritti fondamentali sia irriducibile, metaforicamente riassumibile come una coperta corta. In altre parole, bisogna sfatare un falso mito: non è vero che la libertà di espressione sia ineluttabilmente destinata al totale sacrificio sull'altare della libertà di voto dell'elettore, e viceversa. Che, insomma, non possa essere trovato un equilibrio ottimale tra la tutela della libertà di voto, la moderazione dei contenuti e la libera circolazione delle idee e delle opinioni nelle piattaforme digitali, finalizzato ad evitare che le distorsioni cognitive degli utenti vengano sfruttate per manipolare l'opinione pubblica o interferire con il regolare svolgimento delle elezioni.

In questo senso, l'esperienza maturata in altri ordinamenti giuridici (il servizio *Viginum* in Francia, la *Psychological Defence Agency* in Svezia) dimostra che un equilibrio è possibile. In particolare, la strada sembra quella di un sistema di protezione multilivello, fondato sull'integrazione e sulla collaborazione tra una pluralità di attori (istituzioni, piattaforme digitali, enti intermedi, cittadini). Di fronte alla complessità delle interferenze digitali e delle minacce alla libertà di voto, la lotta alla disinformazione e alla manipolazione online non può gravare esclusivamente sul cittadino. È dunque essenziale promuovere una risposta sistemica che mantenga però come fulcro l'alfabetizzazione digitale, intesa non solo come acquisizione di competenze tecniche, ma come processo pedagogico e civico di consapevolezza, responsabilizzazione e partecipazione attiva del cittadino. Solo il coinvolgimento effettivo e la cooperazione coordinata di tutti gli attori sociali possono gettare le

basi per una democrazia digitale più solida e resiliente alle strategie di disinformazione e alle interferenze esterne.

La disciplina dell'IA in Italia ex lege 132/2025: profili antropocentrici e tutela dei diritti fondamentali nell'ecosistema digitale
di Tommaso Spasari

L'avvento pervasivo dei sistemi di intelligenza artificiale (IA) sta imponendo un ripensamento strutturale dei diritti, tradizionalmente dinamici e soggetti a costante adeguamento. Infatti, l'irruzione della tecnologia algoritmica avanzata nel contesto sociale contemporaneo ha innescato una "palingenesi dei diritti", richiedendo un profondo aggiornamento del quadro normativo di riferimento in risposta alle mutate dinamiche sociali e ai nuovi bisogni emergenti. In questo scenario di marcata trasformazione, il legislatore italiano ha rimodellato la disciplina vigente *in subiecta materia* con l'emanazione della legge 132/2025, approvata il 17 settembre 2025 ed entrata in vigore il 10 ottobre 2025, la quale si configura come la prima normativa nazionale interamente dedicata all'intelligenza artificiale (IA). La normativa *de qua* integra, senza sostituirlo, il regolamento europeo, vale a dire l'*AI Act*, approvato nel 2024, introducendo principî cardine quali la sicurezza, la trasparenza, la non discriminazione e la sostenibilità. L'asse portante di questa disciplina è il suo approccio metodologico saldamente antropocentrico, che esige la salvaguardia dei valori democratici e costituzionali, in linea con la dottrina che vede lo sviluppo tecnico – promosso dall'art. 9 Cost. – limitato dal contemperamento con la salute, la libertà e la dignità umana tutelati *ex* art. 41 Cost.

Alla luce di quanto sopra prospettato, la legge 132/2025 impone la necessità ineludibile dell'intervento umano nelle decisioni ritenute sensibili, un meccanismo volto a prevenire il *deskilling* professionale e la mera delega delle proprie competenze tecniche e specialistiche alla macchina. In proposito, nel settore sanitario l'uso dell'IA è legittimato per supportare validamente la diagnostica e le terapie, un ambito che si è progressivamente rivoluzionato grazie al *machine learning* nella diagnostica per immagini, nella chirurgia robotica e nella gestione delle cartelle cliniche digitalizzate. Tuttavia, ora la legge stabilisce categoricamente che la decisione clinica finale rimane sempre di competenza esclusiva del medico, rafforzando la centralità della persona e vietando ogni forma di discriminazione nell'accesso alle cure. Pertanto, in coerenza con l'esigenza di bilanciamento tra innovazione e tutela dei diritti fondamentali, lo *ius superveniens* promuove l'utilizzo dell'IA in sanità per supportare diagnosi e terapie. Inoltre, la normativa introduce un robusto quadro di misure per la protezione dei dati sensibili in un contesto di crescente utilizzo clinico e di ricerca.

Peraltro, si ammette il riutilizzo di dati sanitari privi di elementi identificativi diretti per finalità scientifiche e di interesse pubblico, subordinandolo all'adozione obbligatoria di presidi tecnici come l'anonimizzazione e la creazione di dati sintetici, in piena armonia con il GDPR e il Codice della Privacy.

Questo scenario riflette la tensione tra la necessità di sfruttare algoritmi potenti e la volontà del legislatore di privilegiare il controllo e il dominio pervasivo da parte dell'essere umano.

L'incremento esponenziale nell'adozione di dispositivi medici dotati di un apprezzabile grado di autonomia decisionale pone criticità non trascurabili in merito al regime di responsabilità penale del sanitario. L'attuale responsabilità penale, incentrata sull'articolo 590-sexies cod. pen., introdotto *ex lege* 24/2017, appare potenzialmente inadeguata a gestire l'errore causato dai sistemi di IA di ultima generazione. Infatti, questi sistemi, in particolare quelli basati sul *machine learning* o *deep learning*, operano tramite un'inferenza meramente probabilistica e si caratterizzano per una fisiologica opacità, rendendo l'iter logico che conduce all'esito non pienamente intellegibile, neppure al programmatore. Questa ermeticità e scarsa prevedibilità algoritmica non si allineano con il metodo tradizionale dell'epidemiologia clinica su cui si fonda la *evidence based medicine*. Quindi, la complessità causale che ne deriva rende estremamente difficile l'accertamento del nesso eziologico e del criterio di imputazione della colpevolezza, in particolare riguardo all'imperizia. Perciò, la dottrina ha paventato il rischio concreto che l'impossibilità di risalire la catena causale fino al produttore o al programmatore trasformi il medico utilizzatore dell'IA in un "capro espiatorio", limitando all'ultimo anello le conseguenze dell'evento lesivo cagionato dalla macchina.

Sebbene sia possibile escludere che lo stesso sistema informatico basato sull'IA possa divenire soggetto attivo del reato, in ossequio al principio di colpevolezza penale giacché *machina delinquere non potest*, comunque l'accettazione di una minima percentuale di eventi infausti potrebbe divenire in futuro inevitabile. Infatti, va precisato che gli errori algoritmici non presuppongono necessariamente un malfunzionamento, ma possono anche derivare da comportamenti acquisiti con l'esperienza e dovuti al modello di apprendimento automatico dell'IA. Ne discende che a fronte di questo orizzonte prossimo, diventerà cruciale il ripensamento della formazione sanitaria, che dovrà orientarsi alla comprensione dei limiti tecnici dei dispositivi. Inoltre, la tutela della libertà di autodeterminazione del paziente, prevista dalla L. 219/2017,

imporrà verosimilmente al medico di specificare – durante l'acquisizione del consenso informato – gli ambiti e i limiti del controllo umano sulla macchina, per rafforzare e mantenere quel rapporto di fiducia e di alleanza terapeutica che l'avvento tecnologico sottopone a nuove e imprevedibili criticità. Sulla scorta delle riflessioni sopra prospettate sarà quindi necessario gestire efficacemente l'inarrestabile progresso scientifico. Traendo le fila del discorso svolto sin qui, deve concludersi che l'attuale contesto tecnologico emergente implica l'urgenza di una rivisitazione anche del regime della responsabilità civile e penale – soprattutto in ambito sanitario – e lo sviluppo di sistemi di IA ibride che integrino strumenti specifici per garantire la necessaria intellegibilità e la costante verifica del loro corretto funzionamento operativo.

Il rapporto tra legalità e disinformazione nell'era digitale: una disamina filosofico-giuridica

di Giovanni D'Alessandro

1. La disinformazione digitale viene comunemente presentata come un problema d'illegalità che richiederebbe un rafforzamento dell'apparato normativo e dei meccanismi di *enforcement*. Questa rappresentazione, per quanto diffusa, misconosce la natura profonda del fenomeno. In realtà, la disinformazione nell'ambiente digitale manifesta il collasso della distinzione fatto/norma (*Sein/Sollen*): il presupposto epistemologico fondamentale su cui riposa l'intero edificio del diritto moderno, e la cui erosione – operata dall'infosfera – priva la legalità stessa del suo ancoraggio concettuale.

2. Mentre la norma giuridica prescrive il *dover essere* (indipendente dall'*essere*), il giudizio di legalità esige una doppia operazione: accertare il *quid facti* e sussumerlo nel *quid iuris* (la fattispecie normativa). Questa bipartizione riflette, del resto, una più generale separazione tra verità e validità che attraversa il pensiero moderno: la scienza si occupa del vero, il diritto del valido, e i due domini non si sovrappongono. Tale architettura concettuale richiede che i fatti siano, per così dire, già dati, costituiti in modo stabile *prima* dell'intervento della norma. Sebbene il diritto prescriva o vieti condotte, esso non crea i fatti sui quali quelle condotte s'innestano. E, sebbene la determinazione processuale del fatto presenti margini di contestazione – come attestato dalla "verità formale" di Carnelutti –, non s'intacca il presupposto di un piano fattuale distinto da quello normativo, ancorché la sua ricostruzione possa essere problematica.

La disinformazione digitale dissolve precisamente questo presupposto. Nell'infosfera, i "fatti" non preesistono alla loro mediazione, ma sono costituiti performativamente attraverso gli stessi meccanismi che dovrebbero limitarsi a rappresentarli. Un evento acquista consistenza fattuale solo se registrato, condiviso e viralizzato attraverso le piattaforme, in un processo governato da logiche algoritmiche di *engagement*, non di veridicità. Il fatto digitale è, quindi, sempre-già "normativo": incorpora fin dall'origine i criteri di valorizzazione che dovrebbero, invece, applicarsi a esso solo dall'esterno.

3. Questa situazione configura un cortocircuito epistemologico. Il diritto, intervenendo per regolare la disinformazione, si trova di fronte non a fatti da qualificare giuridicamente, ma a costruzioni discorsive la cui stessa fattualità è in questione. Si pensi al caso paradigmatico dell'affermazione "le elezioni sono state truccate": questa non è vera o falsa in senso meramente

corrispondentista. La sua efficacia o falsità dipende da una rete complessa di credenze collettive e pratiche istituzionali che sono esse stesse contestate. Nel momento in cui una quota significativa della popolazione accetta quella narrazione, essa produce effetti fattuali reali (manifestazioni, delegittimazione) che retroagiscono sulla situazione originaria.

Il diritto precipita così in una posizione paradossale, poiché per qualificare come "disinformazione" determinate affermazioni, deve pronunciarsi sulla loro verità fattuale. Facendo questo, però, abdica alla propria specifica differenza funzionale – la determinazione del lecito e dell'illecito – per assumere una funzione epistemica: la certificazione del vero. Diviene, in altri termini, un'istituzione di produzione della verità, non più soltanto di produzione della legalità. Come Foucault aveva mostrato, il potere moderno opera attraverso dispositivi di *veridizione* che stabiliscono i confini del dicibile. Ma nell'ambiente digitale questo processo assume una radicalità inedita. La norma giuridica che vieta la diffusione di *fake news* non si limita a regolare comportamenti, ma pretende di fissare il discrimine tra vero e falso in un contesto dove tali confini sono, per definizione, strutturalmente instabili.

4. Le risposte normative elaborate dall'Unione europea – si pensi al *Digital Services Act* – palesano tutta l'ambiguità di questa situazione. Da un lato, s'introducono meccanismi di trasparenza algoritmica e obblighi di *due diligence*; dall'altro, si evita accuratamente di definire giuridicamente cosa sia una "informazione falsa", rimettendo sostanzialmente alle piattaforme private il compito di determinare i contenuti ammissibili. Si crea così un sistema ibrido in cui le piattaforme esercitano una sovranità di fatto sulla verità, pur sotto la supervisione formale delle autorità pubbliche.

Questo assetto non rappresenta un mero compromesso pragmatico, ma testimonia l'impossibilità strutturale, per il diritto statale, di rivendicare un monopolio sulla determinazione della verità in ambito digitale. Le piattaforme non sono, infatti, semplici intermediari neutrali, ma infrastrutture epistemiche che, decidendo la rimozione o la permanenza di un contenuto, non applicano criteri giuridici *ex post* ma producono ontologicamente lo spazio discorsivo *ab origine*. La cosiddetta "legalità algoritmica" – intesa come insieme di principi di trasparenza, non discriminazione e contestabilità – tenta di ricondurre questo potere privato entro binari democratici, ma incontra un'aporia fondamentale: presuppone che l'algoritmo sia uno strumento esterno alla realtà sociale, neutralizzabile attraverso appropriate regolazioni. Sennonché l'algoritmo non è uno strumento, ma la

grammatica stessa attraverso cui l'infosfera si organizza. Renderlo "trasparente" non significa svelarne il funzionamento tecnico – operazione d'altronde sterile per i non addetti – ma comprendere come esso plasmi le nostre stesse categorie cognitive.

5. Si delinea così un'alternativa teorica radicale. O si accetta che il diritto, nell'ambiente digitale, debba incorporare una funzione epistemica che gli è tradizionalmente estranea, configurandosi come garante non solo della legalità ma anche della verità. Oppure si riconosce che la distinzione fatto/norma, su cui il diritto moderno si è costruito, richiede una riformulazione profonda.

La prima opzione conduce verso forme di autoritarismo epistemico difficilmente compatibili con i principi liberal-democratici. Se lo Stato o le sue emanazioni determinano ciò che è vero e ciò che è falso, ogni dissenso politico può essere tacciato di "disinformazione", come già praticato sistematicamente dai regimi illiberali per silenziare l'opposizione. La via della verità di Stato è incompatibile con il pluralismo.

La seconda opzione, che richiede un ripensamento del concetto stesso di legalità, impone che, se i fatti non sono più dati ma costituiti discorsivamente, la legalità non possa limitarsi a regolare condotte rispetto a fatti presupposti. Deve invece configurarsi come governo dei processi di costituzione della realtà sociale. Questo significa che il diritto dovrebbe occuparsi meno di vietare specifici contenuti – operazione inevitabilmente arbitraria – e più di garantire le condizioni procedurali affinché la verità possa emergere dal confronto pubblico. Ma come si garantiscono queste condizioni quando gli stessi spazi del confronto pubblico sono privatamente governati secondo logiche di profitto? La risposta non può essere semplicemente "più regolazione", perché la regolazione presuppone già ciò che deve essere garantito, e cioè un terreno comune di fatti condivisi. Siamo di fronte a un problema di costituzione, non di regolazione. Occorre ripensare lo spazio pubblico digitale non come un mercato di opinioni da regolare *ex post*, ma come un'infrastruttura costituzionale da costruire democraticamente.

6. Una via d'uscita potrebbe consistere nel riconcettualizzare la verità non come un dato epistemico pregiuridico, ma come un bene giuridico in senso proprio. Così come il diritto tutela beni quali la vita o la proprietà, potrebbe tutelare la veridicità dell'informazione non in quanto corrispondenza a fatti bruti, ma in quanto risultato di procedure pubbliche di verifica. La verità diverrebbe, in questa prospettiva, un prodotto istituzionale, non un presupposto naturale.

Questa soluzione esige però una trasformazione radicale delle

istituzioni epistemiche, dal momento che non basta regolare le piattaforme esistenti, ma occorre creare contro-istituzioni (sistemi di *fact-checking* partecipativo, piattaforme pubbliche non commerciali, meccanismi di certificazione distribuita) capaci di produrre verità in modo democratico.

Ciò, tuttavia, ci riporta al problema originario: come può il diritto prescrivere le procedure per la costituzione della verità senza presupporre già una distinzione tra vero e falso? Il circolo è vizioso e, forse, ineliminabile. L'errore sta nel pensare che si possa uscirne attraverso fondamenti ultimi – sia esso il fatto bruto, la norma pura, o la ragione universale. Il circolo va abitato, non spezzato.

La legalità nell'ambiente digitale richiede un modello diverso da quello fondato sulla semplice applicazione di norme a fatti predefiniti. Si tratta di un contesto in cui dinamiche tecnologiche e criteri giuridici si formano insieme, e in cui l'ordinamento deve essere in grado di riflettere sulle proprie categorie mentre le utilizza. Questa prospettiva implica istituzioni dotate di capacità di auto-osservazione e di aggiustamento continuo, procedure che tollerano la revisione e una cultura giuridica disposta a misurarsi con la complessità dell'infosfera senza affidarsi a schemi concettuali rigidi.

La disinformazione mette in luce un limite delle categorie con cui descriviamo il diritto nell'ambiente digitale. Non basta ampliare il catalogo delle regole, soprattutto dopo anni di interventi normativi a livello europeo e nazionale. Serve un modo diverso di concepire il legame tra diritto e mutamenti sociali. Un approccio capace di interpretare la verità come esito di pratiche collettive, di riconoscere il ruolo formativo degli artefatti digitali e di conservare l'ambizione normativa del diritto dentro un mondo in cui fatti e valori si intrecciano in modo nuovo.

Questa trasformazione invita a interrogare il diritto a partire dalle condizioni che la tecnica digitale ha introdotto nel nostro ambiente di vita. Ne deriva un compito teorico e pratico che richiede un salto culturale: un ripensamento delle categorie con cui orientiamo l'azione pubblica, da sviluppare attraverso una rinnovata responsabilità della cultura giuridica e politica, oggi chiamata a misurarsi con una realtà che non assomiglia più a quella per cui quelle categorie erano state create.

Inclusione artificiale: tecnologie, vulnerabilità e protezione dei diritti

di Federico Girelli

Negli ultimi anni l'intelligenza artificiale è divenuta un elemento strutturale dei sistemi economici, amministrativi e sociali. La sua integrazione non è più confinata a settori specialistici, ma riguarda attività ordinarie della vita quotidiana, dall'istruzione al lavoro, dalla mobilità ai servizi pubblici, fino all'accesso a prestazioni sanitarie e assistenziali. È in questo contesto che si colloca la recente legge 23 settembre 2025, n. 132, che definisce le linee guida nazionali in materia di intelligenza artificiale e si coordina con il Regolamento europeo sull'IA adottato il 13 giugno 2024 (c.d. *AI Act*).

L'ampiezza dei profili coinvolti si riflette anche nel procedimento legislativo: il disegno di legge è stato esaminato in più commissioni parlamentari, dalla sanità al lavoro, dalla cultura alla giustizia, segno della pervasività dell'oggetto. La Relazione illustrativa chiarisce l'intento generale, quello di promuovere lo sviluppo tecnologico senza pregiudicare i diritti fondamentali, e anzi orientando l'uso dell'IA verso finalità sociali, in particolare l'inclusione di individui e gruppi esposti a forme di vulnerabilità.

Questo riferimento è tutt'altro che accessorio. La possibilità che sistemi di IA incidano sulle condizioni di autonomia, partecipazione sociale, accesso ai servizi essenziali e capacità decisionali delle persone ha determinato l'esigenza di rendere esplicito, sul piano normativo, che l'innovazione tecnologica non può tradursi in nuove diseguaglianze o in forme di esclusione indiretta. Da qui la scelta, condivisa tanto dal legislatore europeo quanto da quello interno, di assumere la vulnerabilità come categoria giuridica rilevante e non solo come dato sociologico.

L'inquadramento della materia è dunque duplice, poiché se, da un lato , l'IA viene considerata fattore abilitante, capace di aumentare l'accessibilità e ridurre gli ostacoli alla partecipazione; dall'altro lato, è riconosciuto il rischio che strumenti automatizzati, se privi di adeguate garanzie, possano amplificare condizioni di fragilità preesistenti o introdurre nuove forme di marginalizzazione. La disciplina vigente muove, dunque, da un'esigenza di equilibrio, dal momento che non intende frenare l'innovazione, ma indirizzarla.

La centralità della vulnerabilità emerge con chiarezza nell'*AI Act*, nel quale non si qualifica la vulnerabilità come categoria astratta, ma come condizione situata, determinata dal contesto applicativo e dalle caratteristiche del soggetto coinvolto. Essa non coincide con una qualità personale o con uno *status* permanente; deriva piuttosto

dalla relazione tra chi utilizza o subisce l'esito di un sistema algoritmico e l'ambiente tecnologico in cui questo sistema opera.
Questa impostazione riflette la consapevolezza che gli effetti dell'IA non sono uniformi. Un medesimo strumento può rappresentare una risorsa per alcuni e un fattore di marginalizzazione per altri. L'attenzione alla vulnerabilità implica, dunque, che la regolazione non possa essere costruita esclusivamente sulla base di parametri tecnici di funzionamento dei sistemi, ma debba misurarsi con il modo in cui tali sistemi interagiscono con persone che dispongono di differenti livelli di competenza, autonomia e capacità di negoziazione degli esiti.
Ne deriva una distinzione tra accesso e fruizione della tecnologia. Garantire l'accesso a strumenti tecnologici non implica necessariamente garantire che essi siano utilizzabili come strumenti di effettiva inclusione. L'inclusione non è assicurata dal semplice ampliamento delle infrastrutture o dalla disponibilità di soluzioni digitali, ma richiede che queste siano configurate in modo da non presupporre condizioni di alfabetizzazione tecnologica o cognitiva che non sono uniformemente distribuite nella popolazione.
Su questo punto, la disciplina europea adotta un approccio orientato alla prevenzione dei rischi di discriminazione algoritmica. La discriminazione non è intesa come l'espressione di un'intenzione soggettiva, bensì come esito sistemico derivante da modelli di apprendimento che replicano o intensificano asimmetrie preesistenti. È in questa prospettiva che l'*AI Act* richiede valutazioni di impatto, *audit* indipendenti e misure di trasparenza modulata, con l'obiettivo di sottrarre l'algoritmosfera all'opacità che la renderebbe insindacabile.
La logica di fondo è che l'inclusione non consiste nell'adattare i soggetti ai sistemi, ma nel configurare i sistemi in modo da non produrre l'esclusione delle persone. La vulnerabilità diventa, in tal senso, uno strumento di lettura della struttura sociale che l'innovazione tecnologica tende a trasformare, e non un'etichetta protettiva riferita a categorie predeterminate.
L'assunzione della vulnerabilità come criterio di orientamento delle politiche sull'intelligenza artificiale implica un ripensamento del modo in cui i diritti fondamentali operano nell'ambiente digitale. Se, nella tradizione costituzionale europea, diritti come la *privacy*, la libertà personale, l'uguaglianza e l'autodeterminazione informativa hanno la funzione di delimitare l'intervento del potere pubblico e dei soggetti privati, nel contesto algoritmico essi dovranno essere interpretati tenendo conto della struttura tecnica dei processi decisionali automatizzati.

In particolare, la protezione dei dati personali e la libertà di comunicazione non possono essere ridotte alla dimensione del consenso o della trasparenza formale. L'effettività della tutela dipende dalla capacità degli individui di comprendere, controllare e contestare gli esiti dei processi decisionali automatizzati che li riguardano. Tuttavia, questa capacità non è distribuita in modo uniforme nella popolazione. Sono invece necessari competenze tecniche, padronanza delle interfacce digitali e, in molti casi, accesso a strumenti di tutela che non tutti possiedono. È in questo senso che la vulnerabilità non può essere trattata come un'eccezione, ma come un elemento strutturale di valutazione degli effetti dei sistemi di IA.

La questione non riguarda soltanto la tecnologia in sé, ma la posizione dell'individuo all'interno del processo in cui la tecnologia è utilizzata. Se un sistema algoritmico interviene nel definire l'accesso a un servizio essenziale o nel mediare l'interazione con l'amministrazione pubblica, il diritto non potrà limitarsi a garantire la correttezza procedurale del trattamento dei dati, ma dovrà assicurare che la persona non perda la possibilità di incidere sul processo decisionale. E la distanza tra chi decide e chi subisce la decisione tende a crescere quando il meccanismo decisorio è opaco o non contestabile; dunque, l'ordinamento è chiamato a evitare che tale distanza si stabilizzi o si accentui.

Da qui l'esigenza di un quadro che preservi un margine di intervento umano significativo e verificabile nelle decisioni che incidono sulla sfera individuale.

La garanzia giudiziale assume, in questa sede, nuovamente centralità. Ad esempio, la possibilità di sottoporre a scrutinio gli esiti di un processo automatizzato non può essere sostituita da verifiche interne agli stessi sistemi. Il diritto alla spiegazione, se inteso soltanto come accesso a descrizioni tecniche del modello, risulta insufficiente; occorre piuttosto un diritto alla revisione effettiva. Ciò implica che la dimensione della vulnerabilità si traduce in un'esigenza di controllo esterno e non di mera conformità procedurale.

L'inclusione è certamente definita anche dalla rimozione degli ostacoli all'accesso ai servizi digitali, ma solo in parte: diviene centrale la possibilità di mantenere una relazione non subalterna rispetto ai meccanismi decisionali in cui la tecnologia interviene.

La legge italiana n. 132/2025 recepisce l'impostazione del Regolamento europeo, ma la reinterpreta in relazione al funzionamento concreto dei servizi pubblici. L'accento non è posto sulla neutralità tecnologica, bensì sulla necessità di preservare le condizioni di autonomia e partecipazione dei soggetti nei contesti in cui

l'intelligenza artificiale interviene. Nel settore sanitario, la disciplina mira a evitare che gli strumenti di supporto algoritmico alla diagnosi e alla scelta terapeutica si traducano in una delega sostanziale del giudizio clinico. La responsabilità del medico non può essere ridotta a verifica formale degli output del sistema, poiché la relazione di cura rimane il luogo in cui la decisione acquista senso e legittimazione. La vulnerabilità si manifesta qui come possibile esito sistemico della riduzione del rapporto interpersonale a esito di processi automatizzati.

Analoghe considerazioni emergono nell'ambito dei servizi sociali e dell'inclusione lavorativa. L'uso di algoritmi per la valutazione dei bisogni o l'allocazione delle risorse non può consolidare profili amministrativi di fragilità che tendono a perpetuarsi nel tempo. Un sistema che classifica per assistere rischia di determinare, attraverso la classificazione, l'identità stessa dell'assistito. La vulnerabilità, in questo senso, può diventare un effetto della procedura, e non soltanto una condizione da proteggere.

Nei rapporti tra cittadini e amministrazione digitale, l'introduzione dell'IA è orientata all'efficienza e alla semplificazione. Tuttavia, il diritto deve assicurare che l'accesso a prestazioni e procedimenti non venga condizionato da competenze o risorse tecniche non uniformemente distribuite. Secondo l'approccio del regolamento e della legge nazionale, la garanzia risiederebbe nella possibilità che la tecnologia sia modulabile, comprensibile e contestabile.

Il tratto comune delle disposizioni nazionali è la definizione dell'intelligenza artificiale come elemento strutturale dell'azione pubblica e non come supporto esterno. In tale prospettiva, la vulnerabilità diventa una categoria giuridica che orienta la progettazione istituzionale.

La legge, pertanto, mira a configurare la tecnologia in modo coerente con i presupposti costituzionali della cittadinanza, ossia con la possibilità di partecipare e di essere riconosciuti come agenti nelle decisioni che concernono la propria vita e la vita pubblica.

L'"inclusione artificiale" designa intanto l'uso dell'IA per compensare fragilità ma, più in generale, l'inserimento della tecnologia all'interno di un quadro di garanzie che preservi la possibilità dell'individuo di non essere ridotto a destinatario passivo di processi algoritmici.

A quali condizioni l'intelligenza artificiale smetterà di produrre dipendenze e vulnerabilità, e potrà essere uno strumento di rafforzamento dell'autonomia delle persone?

L'innocenza sorvegliata. Chat Control e la logica del sospetto nell'Europa della sicurezza digitale

di Francesco Cirillo

La proposta comunemente nota come *Chat Control*[5] i colloca all'interno di una crescente attenzione da parte delle istituzioni europee al tema degli abusi sessuali su minori in ambiente digitale. La Commissione europea ha evidenziato come una parte significativa della diffusione di materiale pedopornografico avvenga attraverso canali di comunicazione privata, con particolare riferimento ai servizi di messaggistica istantanea, i quali rendono più complessa l'individuazione delle condotte penalmente rilevanti e la conseguente attività investigativa delle autorità. Il fenomeno non è nuovo, ma l'ambiente tecnologico ne ha forse modificato la scala e la visibilità: la memorizzazione permanente dei contenuti, la replicabilità indefinita dei materiali e la possibilità di instaurare contatti diretti con soggetti vulnerabili hanno ampliato l'accesso e la diffusione delle condotte illecite.

L'urgenza di un intervento è riconosciuta tanto dalla letteratura criminologica quanto dai lavori preparatori delle istituzioni europee. Il punto che richiede un esame più approfondito riguarda la struttura e il fondamento giuridico dello strumento proposto.

La disciplina elaborata dalla Commissione introduce per i fornitori di servizi di comunicazione la possibilità — e in alcuni casi l'obbligo — di adottare procedure automatizzate di analisi dei contenuti mediante strumenti algoritmici progettati per individuare immagini, testi o metadati associati a forme di abuso.

L'attivazione di questi meccanismi avviene senza una previa verifica specifica sui singoli utenti e senza un passaggio giurisdizionale autorizzativo. Il risultato è un sistema che applica il controllo in modo esteso all'intero insieme degli utilizzatori dei servizi.

La questione principale riguarda l'uso di queste tecniche in presenza di comunicazioni cifrate *end-to-end*. La documentazione istituzionale europea sostiene che la cifratura, pur rappresentando un presidio di sicurezza, limita l'accertamento degli abusi. Per questo motivo, l'analisi automatizzata viene descritta come uno strumento capace di aggirare la barriera tecnica, mantenendo formalmente intatto il meccanismo di protezione. Da qui nasce una tensione evidente: da un lato vi è l'esigenza di garantire la riservatezza delle comunicazioni,

[5] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori*, Bruxelles, 11 maggio 2022, COM(2022) 209 final.

tutelata in molti ordinamenti come valore costituzionale; dall'altro, l'obiettivo di rendere verificabili contenuti che circolano su canali cifrati.

In questa prospettiva il tema investe direttamente il quadro costituzionale che governa le limitazioni ai diritti fondamentali. Il diritto europeo riconosce la vita privata e la protezione dei dati personali come posizioni giuridiche primarie (artt. 7 e 8 CDFUE). Ogni restrizione richiede una base normativa chiara, finalità specifiche e un controllo di necessità e proporzionalità effettivamente verificabile. La sorveglianza delle comunicazioni trova spazio negli ordinamenti europei solo quando esiste un fondamento probatorio adeguato e quando l'applicazione della misura è sottoposta a un'autorità indipendente, di regola di natura giurisdizionale.

La proposta di *Chat Control* introduce un cambiamento significativo: il controllo sui contenuti viene attivato prima che emergano condotte illecite e si fonda sulla qualificazione preventiva dell'ambiente digitale come ambito esposto a rischio. La conseguenza è un sistema di verifica che non si concentra sul comportamento di singoli utenti, ma agisce sull'intera infrastruttura comunicativa. In questo schema, la tutela non segue un fatto accertato; diventa una componente ordinaria del funzionamento tecnico dei servizi.

Questo spostamento solleva una questione di compatibilità con il modello europeo di garanzia, costruito su limiti alla libertà comunicativa che devono essere eccezionali, verificabili e circoscritti. La protezione dei minori rappresenta un interesse essenziale, tuttavia ciò non esaurisce il problema: resta da stabilire se la struttura proposta rispetti i presupposti che, nell'ordinamento europeo, definiscono lo spazio d'azione delle istituzioni pubbliche e il ruolo della sfera privata nei contesti digitali.

Per valutare la portata della misura occorre distinguere due piani che nel dibattito vengono spesso confusi. Da un lato vi è l'Unione Europea come ordinamento giuridico, organizzato attorno ai Trattati, alla Carta dei diritti fondamentali e alla giurisprudenza della Corte di giustizia. Dall'altro, l'Unione come attore regolatorio, che elabora politiche, strategie e modelli amministrativi orientati alla gestione di fenomeni percepiti come critici. La distanza fra questi livelli non riguarda un dettaglio terminologico; incide sul modo in cui si stabiliscono la legittimità e i limiti dell'intervento pubblico.

L'Unione, considerata come ordinamento giuridico, si fonda sul principio delle competenze attribuite, sul controllo giurisdizionale sugli atti e su un uso costante del principio di proporzionalità. La limitazione dei diritti fondamentali è consentita solo in presenza di obiettivi legittimi e di misure

necessarie e strettamente adeguate. La Carta dei diritti fondamentali, in particolare negli articoli 7 e 8, vincola direttamente le politiche dell'Unione e, secondo parte della dottrina e della giurisprudenza, incide anche sul diritto degli Stati membri. Il diritto al rispetto della vita privata e quello alla protezione dei dati personali definiscono il perimetro entro cui si muove il legislatore europeo.

Se si guarda invece all'Unione come apparato di *policy*, emerge una logica differente. In questo ambito prevalgono la gestione del rischio, la prevenzione dei danni potenziali, la standardizzazione delle procedure e l'intervento anticipatorio. Le tecnologie non vengono considerate un contesto neutrale: lo spazio digitale è trattato come un ambiente esposto in modo strutturale a vulnerabilità che richiedono strumenti di identificazione e controllo prima dell'insorgenza di un illecito. Ne deriva una tutela che tende ad assumere forme di monitoraggio continuo o, quantomeno, ricorrente. In questa linea si collocano, con intensità variabile, il GDPR e la sua impostazione *by design* e *by default*, così come il *Digital Services Act* e l'*AI Act*.

La proposta di regolamento del 2022 appartiene a questo secondo modo di concepire l'intervento pubblico. La struttura dell'atto non segue la sequenza tipica dei modelli di garanzia, pensati per misure attivate in risposta a un comportamento illecito individuato in modo circostanziato. L'assunto di partenza è diverso: l'ambiente digitale viene trattato come un contesto che richiede controlli estesi perché la possibilità dell'abuso è considerata un tratto intrinseco del mezzo. L'intervento, dunque, non dipende da un soggetto definito in base a indizi o sospetti; deriva dalla configurazione stessa dello spazio comunicativo.

In questa cornice, la tutela dei diritti fondamentali non coincide più con una delimitazione esterna dei poteri pubblici. Diventa un elemento dell'architettura tecnica attraverso cui il potere opera. Il controllo non è attivato in presenza di uno specifico caso; è incorporato nel funzionamento delle infrastrutture digitali che rendono possibile la comunicazione.

Questa distinzione incide sulla qualificazione dell'intervento e sul suo rapporto con il quadro giuridico fondamentale dell'Unione. Quando la regolazione introduce forme di sorveglianza automatizzata che precedono l'accertamento individuale di una responsabilità, cambia l'assetto dei rapporti tra istituzioni e cittadini. Il punto è stabilire se l'Unione possa adottare strumenti che incidono sulla comunicazione privata senza ridefinire in modo esplicito il sistema di garanzie previsto dalle Costituzioni europee e dalla Carta dei diritti fondamentali.

La valutazione della proposta deve confrontarsi anche con la giurisprudenza della Corte di giustizia in materia di sorveglianza delle comunicazioni. A partire dalla sentenza *Digital Rights Ireland* (C-293/12 e C-594/12), la Corte ha chiarito che misure di conservazione generalizzata dei dati di traffico e di localizzazione prive di criteri selettivi risultano incompatibili con gli articoli 7 e 8 della Carta. Le decisioni successive, in particolare *Tele2 Sverige* (C-203/15 e C-698/15) e *La Quadrature du Net* (C-511/18, C-512/18 e C-520/18), hanno ribadito un orientamento costante: la sorveglianza preventiva delle comunicazioni richiede minacce gravi e determinate, collocate in un arco temporale definito, e l'intervento deve essere sottoposto al vaglio di un'autorità indipendente, di norma un giudice. L'uso di dispositivi tecnici operanti in via automatica non soddisfa questo standard di garanzia.

La giurisprudenza della Corte presenta un orientamento stabile: ogni interferenza nella sfera privata richiede un riferimento a circostanze concrete che giustifichino la misura. La possibilità di anticipare il controllo sulla base di un rischio generalizzato non rientra in questo schema. Il punto decisivo riguarda il rapporto tra obiettivo perseguito e strumenti impiegati. La protezione dei minori da abusi rappresenta una finalità legittima e di grande rilievo; tuttavia, la sua importanza non esonera dall'esame dei requisiti di necessità e proporzionalità così come definiti dalla Corte, requisiti che devono essere soddisfatti in ogni intervento che incide sulla libertà comunicativa.

Il quadro diventa più articolato se lo si osserva dalla prospettiva convenzionale. La Corte europea dei diritti dell'uomo, in pronunce come *Zakharov c. Russia* (2015) e *Big Brother Watch* (2021), ha ritenuto incompatibili con l'art. 8 CEDU i sistemi di sorveglianza privi di criteri di selettività e di un controllo giurisdizionale effettivo. Gli Stati membri dell'Unione restano vincolati a questo standard a prescindere dalle iniziative europee, e l'eventuale futura adesione dell'Unione alla Convenzione non incide sugli obblighi degli ordinamenti nazionali. La mancanza di selettività e l'assenza di un sospetto individualizzato costituiscono quindi elementi problematici sia nel diritto dell'Unione sia in quello convenzionale.

A questo punto occorre valutare il rapporto tra la proposta di regolamento e l'*AI Act*. Nel regolamento sull'intelligenza artificiale, l'Unione qualifica come pratiche ad alto rischio — e in alcuni casi vietate — le forme di sorveglianza algoritmica che incidono in modo significativo sulla libertà individuale e sulla riservatezza della vita privata. Rientrano fra le attività più problematiche il monitoraggio

sistematico dei comportamenti e l'analisi automatica di dati personali su larga scala.
Se si assume l'*AI Act* come quadro di riferimento, l'impianto tecnico previsto da *Chat Control* presenta tratti che si avvicinano a quelli collocati dal legislatore europeo nella categoria dell'alto rischio e, in certe configurazioni, a quelle condotte che il regolamento mira a escludere. Il punto critico non riguarda solo il contenuto delle due normative; emerge una differenza più profonda nel modo in cui viene concepito il ruolo della sorveglianza algoritmica. Nel regolamento sull'IA, essa appare come un fenomeno da contenere per preservare dignità e autonomia delle persone. Nella proposta relativa al contrasto degli abusi sessuali, la medesima infrastruttura tecnologica viene presentata come componente necessaria di un sistema di protezione.
Questa divergenza evidenzia una tensione interna al diritto dell'Unione. Quando la sorveglianza algoritmica preventiva è considerata, in linea generale, una pratica idonea a incidere sui diritti fondamentali, la sua introduzione obbligatoria richiede una giustificazione coerente con gli standard elaborati dalla Corte e con i principi che regolano le limitazioni alla libertà comunicativa.
Il tema non si esaurisce nel bilanciamento tra protezione dei minori e tutela della *privacy*. In gioco vi è la coerenza con cui l'ordinamento dell'Unione definisce le condizioni di esercizio del potere pubblico nell'ambiente digitale. Quando misure di sorveglianza algoritmica vengono escluse in un settore e introdotte in un altro senza un aggiornamento esplicito dei principi che regolano le limitazioni ai diritti fondamentali, l'effetto è un indebolimento delle garanzie e una trasformazione silenziosa del rapporto tra libertà e controllo.
La discussione sulla proposta di controllo delle comunicazioni si colloca all'interno di un quadro più ampio, quello dei rapporti tra l'ordinamento dell'Unione e gli ordinamenti costituzionali nazionali. L'integrazione europea richiede agli Stati membri il trasferimento di competenze e il riconoscimento del primato del diritto dell'Unione; questo trasferimento, tuttavia, trova un limite nella struttura costituzionale di ciascun ordinamento. La dottrina italiana dei controlimiti, la giurisprudenza tedesca sulla *Verfassungsidentität* e gli orientamenti di numerose corti costituzionali convergono nell'affermare che il riconoscimento del primato dipende dalla tutela di alcuni principi fondamentali degli Stati membri. Tali principi non rappresentano soltanto una eredità precedente all'adesione all'Unione: costituiscono il fondamento della legittimazione stessa della partecipazione all'ordinamento sovranazionale.

Le pronunce che in Italia hanno delineato la dottrina dei controlimiti, così come le decisioni del *Bundesverfassungsgericht*, non descrivono un antagonismo rispetto al processo di integrazione europea. Illustrano, piuttosto, la condizione che consente agli Stati di partecipare all'ordinamento sovranazionale: la presenza, nell'Unione, di un assetto giuridico compatibile con la struttura costituzionale interna. Quando questa compatibilità si incrina, a essere coinvolto non è il principio di cooperazione tra ordinamenti, ma il presupposto della primazia del diritto europeo.

La proposta esaminata tocca principi che le corti costituzionali europee hanno sempre considerato parte essenziale delle garanzie di libertà. Tra questi rientrano la presunzione di innocenza e il controllo giurisdizionale sugli atti che incidono sulla sfera privata, elementi che, negli ordinamenti europei, definiscono il funzionamento dello Stato di diritto e non semplici profili procedurali.

Una configurazione stabile dell'ambiente digitale come spazio soggetto a controllo preventivo modificherebbe il ruolo della comunicazione privata: da luogo ordinario dell'autodeterminazione individuale si trasformerebbe in un ambito il cui accesso è regolato da decisioni di natura amministrativa o tecnica.

In questa prospettiva, il dibattito su *Chat Control* riguarda il modo in cui il potere pubblico si struttura nell'ecosistema digitale. Se la protezione dei minori richiede misure rafforzate, tali misure devono collocarsi all'interno del quadro di garanzie che sorregge l'ordinamento europeo e che ne legittima l'azione.

Resta aperto un interrogativo: fino a che punto l'Unione potrà adottare strumenti di controllo tecnologico senza ridefinire, in modo esplicito e deliberato, le condizioni della propria legittimità? Su questo punto, forse, dovrà concentrarsi la futura discussione istituzionale e politica.

Il Comitato tecnico-scientifico dell'OSLE

- ***Giuseppe Acocella***, Coordinatore dell'Osservatorio;
- ***Giovanni D'Alessandro,*** sezione "Legalità e Costituzione";
- ***Mariangela Barletta***, sezione "Legalità e diritto internazionale";
- ***Carmine De Angelis***, sezione "Istituzioni e federalismo";
- ***Antonio Scoppettuolo***, sezione "Comunicazione";
- ***Diego Forestieri***, sezione "Società";
- ***Giorgio Ridolfi***, sezione "Fondamenti Culturali";
- ***Stefano Sepe***, sezione "Pubblica Amministrazione";
- ***Gaia Fristachi, Francesco Cirillo***, sezione "Legalità e tecnologie emergenti";

Per proporre un contributo per la newsletter scrivere a: redazione@osle.it