Apr/2026

CAMMINO DIRITTO

Rivista Giuridica

RASSEGNA ARTICOLI GIURIDICI
- SETTORE RICERCA -

MENSILE ONLINE

RIEPILOGO DATI PER IL DEPOSITO PRESSO IL MINISTERO DEI BENI ARTISTICI E CULTURALI - SERVIZIO II - PATRIMONIO BIBLIOGRAFICO E DIRITTO D'AUTORE

Denominazione della Rivista Scientifica: **Cammino Diritto**
ISSN: 2532-9871 - Codice CINECA: E243140 - Rivista ANVUR
Registrazione: Tribunale di Salerno n° 12/2015
Periodicità: Periodico (on-line)
Sede: Via Rosa Jemma 50 84091 Battipaglia (SA)

Editore: CAMMINO DIRITTO Srl
ISP (Internet Service Provider): aruba.it – www.camminodiritto.it
Indirizzo web: https://www.camminodiritto.it
Indirizzo e-mail: direzione@camminodiritto.it

Tutti i contributi pubblicati in questo questo fascicolo hanno superato una procedura di peer review, attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori, individuati secondo criteri di competenza tematica e di rotazione all'interno dei membri del Comitato scientifico. Ciascun lavoro soggetto alla procedura viene esaminato in forma anonima da un revisore

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

Indice dei contenuti

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

PARTICOLARE TENUITÀ DEL FATTO E REATI DI VIOLENZA A PUBBLICO UFFICIALE: IL PARADOSSO SISTEMICO DOPO LA SENTENZA DELLA CORTE COSTITUZIONALE

La sentenza n. 172/2025 della Corte costituzionale rappresenta un punto di svolta nella disciplina dell'art. 131-bis c.p., dichiarando irragionevole l'esclusione assoluta dei reati di violenza e resistenza a pubblico ufficiale dall'ambito della particolare tenuità del fatto. La Corte interviene su un quadro normativo disarmonico, nel quale la riforma Cartabia aveva reso applicabile l'esimente al più grave art. 338 c.p., lasciandola invece preclusa per fattispecie meno gravi, generando un'inversione assiologica. Il contributo analizza la decisione alla luce dei principi di ragionevolezza, coerenza sistemica e funzione rieducativa della pena, evidenziando le ricadute dogmatiche e le prospettive evolutive dell'istituto.

autore **Aldo Andrea Presutto**

Abstract ENG

The judgment of the Italian Constitutional Court No. 172 of October 15, 2025, marks a paradigmatic shift in the regulation of the defense of de minimis offenses (particolare tenuit?del fatto), declaring the constitutional illegitimacy of the absolute exclusion of crimes of violence and resistance against public officials (Articles 336 and 337 of the Criminal Code) from the scope of application of the defense under Article 131-bis of the Criminal Code. The decision addresses a systemic paradox generated by uncoordinated legislative stratifications: the admissibility of the defense for the more serious crime (Article 338 of the Criminal Code) and its simultaneous exclusion for less serious crimes. This article conducts a meticulous analysis of the decision, examining its dogmatic

ISSN 2532-9871 rivista Camminodiritto - https://rivista.camminodiritto.it - ragionline

La funzione rieducativa della pena e le sue implicazioni sistematiche; {URL} #160;Funzione rieducativa e proporzionalità della pena: un binomio inscindibile; 7. Analisi critica e questioni aperte; {URL} : profili critici; {URL} #39;assorbimento della questione subordinata: un'occasione mancata; {URL} #39;indeterminatezza della "particolare tenuità del fatto"; {URL} #39;autorità pubblica e garanzie individuali; 8. Conclusioni: La sentenza 172/2025 come momento di transizione.

1. Introduzione: il contesto della questione e la sua rilevanza sistemica

{URL}

La sentenza n. 172/2025 della Corte costituzionale trae origine da un procedimento penale instaurato presso il Tribunale ordinario di Firenze, prima sezione penale, con ordinanza di rimessione datata 24 maggio 2024[1]. Il caso presenta caratteristiche che trascendono la dimensione meramente individuale per assurgere a paradigma di una tensione sistematica di più ampia portata, investendo questioni fondamentali concernenti la coerenza interna dell'ordinamento penale e il rapporto tra discrezionalità legislativa e sindacato costituzionale.

Il fatto oggetto del giudizio principale può essere sintetizzato come segue: A. M., donna incensurata, di corporatura minuta, affetta da patologia oncologica in stadio avanzato, ha posto in essere una serie di condotte qualificabili come violenza nei confronti di un agente della Polizia di Stato, consistenti nel toccare ripetutamente il torace dell'operatore con l'indice della mano destra e, infine, nell'infliggergli uno schiaffo al volto di modesta intensità.[2] La dinamica fattuale, lungi dal configurare un'aggressione sistematica o connotata da particolare intensità lesiva, si colloca nel contesto di una manifestazione politica svoltasi nell'ottobre 2019, allorché l'imputata, intendendo accedere al luogo ove si svolgeva il raduno, veniva fermata dall'operatore di polizia in ragione del raggiungimento della capienza massima della struttura ospitante.

Il Tribunale rimettente, procedendo a una riqualificazione giuridica del fatto (originariamente contestato come resistenza ex art. 337 cod. pen.) nella più grave fattispecie di violenza a pubblico ufficiale ex art. 336 cod. pen., ha ritenuto sussistere pienamente i presupposti sostanziali per l'applicazione della causa di non punibilità per particolare tenuità del fatto di cui all'art. 131-bis cod. pen. Tuttavia, il giudice a quo si è trovato impedito da un ostacolo normativo di carattere formale: l'art. 131-bis, terzo comma, cod. pen., nella sua attuale configurazione, esclude tassativamente l'applicabilità dell'esimente ai delitti ex artt. 336 e 337 cod. pen., quando commessi nei confronti di ufficiali o agenti di pubblica sicurezza nell'esercizio delle proprie funzioni.[3]

{URL}

Il Tribunale rimettente ha sollevato una questione principale di legittimità costituzionale, riferita all'art. 3 Cost., nella quale denuncia la violazione del principio di ragionevolezza

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - pa rodino online

derivante dall'esclusione assoluta della causa di non punibilità per i delitti ex artt. 336 e 337 cod. pen., a fronte dell'ammissibilità dell'esimente per altri titoli di reato di gravità pari o superiore.

La questione investe il nucleo essenziale del principio di ragionevolezza, articolato nella giurisprudenza costituzionale in una duplice accezione: da un lato, come "ragionevolezza-congruità", ossia coerenza tra mezzi e fini perseguiti dal legislatore; dall'altro, come "ragionevolezza-coerenza", ossia assenza di contraddizioni interne nell'ordinamento giuridico.[4] È precisamente questa seconda accezione che viene in rilievo nel caso di specie: il Tribunale rimettente denuncia non l'inadeguatezza dei mezzi rispetto ai fini, bensì l'incoerenza interna della disciplina normativa, la quale ammette l'esimente per il reato più grave (art. 338 cod. pen.) e la esclude per i reati meno gravi (artt. 336-337 cod. pen.).

In via subordinata, il Tribunale ha sollevato un'ulteriore questione riguardante la circostanza aggravante della commissione della violenza nel corso di manifestazioni pubbliche (art. 339 cod. pen.), che rimane assorbita dalla fondatezza della questione principale.

{URL} #160; La rilevanza della questione nel contesto della riforma del 2022

Ciò che conferisce particolare pregnanza sistematica alla questione è il fatto che essa si inserisce in un contesto normativo radicalmente trasformato rispetto a quello vigente al momento della precedente pronuncia della Corte costituzionale sulla medesima materia. La sentenza n. 30 del 2021[5] si era pronunciata su una questione analoga in un quadro normativo nel quale il delitto di cui all'art. 338 cod. pen. rimaneva escluso dal perimetro applicativo della causa di non punibilità, in ragione del suo massimo edittale superiore al limite allora vigente di cinque anni di reclusione.

Tuttavia, la riforma operata dal {URL} ({URL}), ha determinato una vera e propria "cesura paradigmatica" nella disciplina dell'istituto, traslocando il criterio di selezione dell'ambito applicativo dell'esimente dal massimo edittale (non superiore a cinque anni di reclusione) al minimo edittale (non superiore a due anni di reclusione)[6]. Tale modificazione—che apparentemente potrebbe sembrare di natura meramente tecnica—ha prodotto conseguenze sistematiche di straordinaria portata, determinando l'automatica inclusione nel perimetro applicativo dell'esimente di numerosi titoli di reato precedentemente esclusi, tra cui il delitto ex art. 338 cod. pen., punito con la reclusione da uno a sette anni.

Tale mutamento normativo non è stato accompagnato da una corrispondente ricalibrazione delle eccezioni nominative previste dal terzo comma dell'art. 131-bis cod. pen.; al contrario, l'eccezione nominativa relativa ai delitti ex artt. 336 e 337 cod. pen. è

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ragionio online

stata ribadita e confermata, determinando così una situazione che la Corte costituzionale non esita a qualificare come "manifestamente irragionevole": il reato più grave (art. 338 cod. pen.) rimane ammesso all'esimente, mentre i reati meno gravi (artt. 336-337 cod. pen.) ne rimangono esclusi.[7]

2. L'evoluzione normativa della causa di non punibilità

{URL} #39;istituto (2015-2019)

La causa di non punibilità per particolare tenuità del fatto rappresenta una delle innovazioni più significative della legislazione penale italiana del secondo decennio del ventunesimo secolo. L'istituto è stato introdotto mediante il {URL} [8] il quale ha recepito la delega legislativa contenuta nella legge 28 aprile 2014, n. 67, nell'ambito di un più ampio disegno riformatore volto alla deflazione processuale e punitiva del sistema penale italiano.

La ratio legis sottesa all'introduzione dell'esimente rimanda a una duplice finalità: da un lato, una finalità di carattere pragmatico-deflattivo, consistente nella riduzione del carico di procedimenti penali concernenti fatti di minima offensività; dall'altro, una finalità di carattere assiologico-garantista, consistente nella valorizzazione del principio di offensività quale limite alla punibilità penale.[9]

La formulazione originaria dell'art. 131-bis cod. pen. presentava una struttura relativamente lineare, fondata su tre criteri fondamentali: (a) un criterio oggettivo-edittale: l'applicabilità dell'esimente era subordinata alla previsione, per il reato in questione, di una pena edittale massima non superiore a cinque anni di reclusione; (b) un criterio oggettivo-fattuale: il giudice doveva valutare, in concreto, la "particolare tenuità" del fatto, considerando sia le "modalità della condotta" sia l'"esiguità del danno o del pericolo"; (c) un criterio soggettivo-comportamentale: l'esimente era esclusa qualora il comportamento dell'autore risultasse "abituale".[10]

Un aspetto particolarmente rilevante della configurazione originaria consisteva nell'assenza di eccezioni nominative basate sul titolo di reato: l'esclusione della punibilità non era preventivamente preclusa per determinate categorie di delitti, ma operava in relazione a tutti i reati che rispettassero il limite edittale massimo, salva la presenza di specifiche circostanze di fatto che ne impedivano l'applicazione.

{URL} : l'introduzione delle eccezioni nominative (2019-2020)

Una significativa frattura nella coerenza strutturale dell'istituto si verifica con il {URL} [11] Tale intervento normativo si inserisce in un contesto politico-criminale caratterizzato da una crescente enfatizzazione della tutela dell'autorità pubblica.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ragionio online

Mediante l'art. 16, comma 1, lett. b), del suddetto decreto-legge, viene introdotta—per la prima volta nella storia dell'istituto—un'eccezione nominativa specificamente riferita ai delitti di cui agli artt. 336 e 337 cod. pen., stabilendo che "l'offesa non può essere ritenuta di particolare tenuità quando si procede per i delitti di cui agli articoli 336 e 337 del codice penale commessi nei confronti di un pubblico ufficiale nell'esercizio delle proprie funzioni".[12] Tale innovazione rappresenta una scelta di politica criminale di straordinaria rilevanza, poiché introduce una logica radicalmente diversa rispetto a quella sottesa alla configurazione originaria dell'istituto.

La legittimità costituzionale di tale scelta è stata sottoposta al vaglio della Corte costituzionale mediante la già citata sentenza n. 30 del 2021, che aveva dichiarato non fondate le questioni sollevate, ritenendo non manifestamente irragionevole l'esclusione basata sulla natura plurioffensiva dei delitti in questione.[13]

{URL} : il cambio di paradigma nella struttura dell'esimente

Una cesura profonda nella disciplina della causa di non punibilità si determina mediante l'art. 1, comma 1, lett. c), del {URL} #39;efficienza del processo penale".[14] Tale intervento legislativo muta radicalmente il paradigma sotteso alla definizione dello spazio operativo dell'esimente.

La modificazione cruciale consiste nella traslazione del criterio edittale di selezione dell'ambito applicativo dell'esimente: si passa dal limite del massimo edittale (pena detentiva non superiore nel massimo a cinque anni) al limite del minimo edittale (pena detentiva non superiore nel minimo a due anni).[15] Tale operazione determina un effetto di grande ampiezza: l'inclusione automatica nell'area applicativa della causa di non punibilità di molti titoli di reato che, anteriormente, ne erano esclusi in ragione del massimo edittale superiore a cinque anni.

È precisamente nell'ultimo caso che emerge con evidenza cristallina il paradosso logico-sistematico denunciato dal Tribunale rimettente: mentre il delitto ex art. 338 cod. pen.—più grave, come testimoniato dalla forbice edittale più severa (da uno a sette anni)—viene ammesso all'esimente per effetto della riforma del 2022, il delitto ex art. 336 cod. pen.—meno grave (da sei mesi a cinque anni)—rimane escluso per effetto dell'eccezione nominativa.[16]

{URL} #39;aggravante a effetto speciale

Nel breve lasso di tempo intercorso tra la riforma del 2022 e la sentenza della Corte costituzionale in esame, il legislatore è nuovamente intervenuto sulla materia mediante il {URL} [17]

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ragionamento ordina

Mediante l'art. 19, comma 1, lettere a) e b), del suddetto decreto-legge, è stata introdotta un'aggravante a effetto speciale nei delitti ex artt. 336 e 337 cod. pen., consistente nell'aumento della pena "fino alla metà" qualora il fatto di violenza sia commesso nei confronti di ufficiali o agenti di pubblica sicurezza nell'esercizio delle proprie funzioni.[18]

La Corte costituzionale, nella sentenza n. 172/2025, prende esplicitamente in considerazione tale sobvenienza normativa e ne esamina le implicazioni rispetto al giudizio di ragionevolezza. In particolare, la Corte osserva che, sebbene l'aggravante a effetto speciale rilevi ai fini della determinazione del minimo edittale per l'esimente (ex art. 131-bis, quinto comma, cod. pen.), essa non è tuttavia "in grado di elevare il minimo di sei mesi, stabilito per i reati di cui agli artt. 336 e 337 cod. pen., oltre quello di un anno, stabilito per il reato di cui all'art. 338 dello stesso codice".[19] Applicando l'aumento di pena "fino alla metà" al minimo edittale di sei mesi dei delitti ex artt. 336-337 cod. pen., si ottiene un minimo aumentato di nove mesi, che rimane comunque inferiore al minimo edittale di un anno previsto per il delitto ex art. 338 cod. pen. Pertanto, anche dopo l'introduzione dell'aggravante a effetto speciale, permane la situazione paradossale per la quale il reato con minimo edittale più elevato è ammesso all'esimente, mentre i reati con minimo edittale inferiore ne rimangono esclusi.[20]

3. La sentenza n. 30 del 2021: presupposti e limiti

{URL}

La sentenza n. 30 del 2021 rappresenta il precedente giurisprudenziale diretto con cui la pronuncia in esame deve necessariamente confrontarsi.[21] La questione sottoposta alla Corte era stata sollevata dal Tribunale di Messina, sezione distaccata di Barcellona Pozzo di Gotto, mediante ordinanza del 10 luglio 2019, nel contesto di un procedimento penale per il delitto di resistenza a pubblico ufficiale ex art. 337 cod. pen.

Il quadro normativo di riferimento era significativamente diverso rispetto a quello attuale: vigeva ancora il criterio del massimo edittale (non superiore a cinque anni di reclusione) per l'individuazione dei reati ammissibili alla causa di non punibilità; il delitto di cui all'art. 338 cod. pen. rimaneva escluso dal perimetro applicativo dell'esimente in ragione del suo massimo edittale di sette anni, superiore al limite allora vigente di cinque anni.[22]

{URL} : la logica della plurioffensività

La Corte costituzionale, nella sentenza n. 30/2021, dichiarava non fondate le questioni sollevate, elaborando un'argomentazione articolata che poggiava su due pilastri fondamentali: la natura plurioffensiva dei delitti ex artt. 336-337 cod. pen. e la non

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

omogeneità strutturale rispetto ai tertia comparativi proposti dal giudice rimettente.[23]

Il primo pilastro argomentativo—la plurioffensività—si fonda sull'osservazione che i delitti di violenza e resistenza a pubblico ufficiale non ledono soltanto il bene giuridico del regolare funzionamento della pubblica amministrazione, ma incidono altresì sulla sicurezza e sulla libertà di determinazione delle persone fisiche esercenti le pubbliche funzioni.[24] La Corte afferma che tale doppia dimensione offensiva giustifica una tutela penale rafforzata, che si traduce nell'esclusione aprioristica dell'esimente.

Tuttavia, tale argomentazione merita di essere sottoposta a una serrata analisi critica. Da un lato, la tesi della plurioffensività presenta un carattere eccessivamente astratto e rigido: essa presuppone che ogni condotta di violenza o minaccia a pubblico ufficiale leda necessariamente, e con intensità significativa, sia il funzionamento amministrativo sia la sicurezza personale, senza considerare che, nel caso concreto, l'intensità lesiva può essere estremamente modesta.[25] Dall'altro lato, l'argomentazione della Corte sembra confondere due piani distinti: il piano della struttura dogmatica della fattispecie (che è certamente plurioffensiva) e il piano del disvalore concreto del fatto (che può presentare gradi di intensità estremamente differenziati).

Inoltre, nel nuovo contesto normativo determinato dalla riforma del 2022, l'argomento della plurioffensività perde la sua tenuta logica: se è vero che la plurioffensività giustifica l'esclusione dei delitti ex artt. 336-337 cod. pen. dall'esimente, a maggior ragione dovrebbe giustificare l'esclusione del delitto ex art. 338 cod. pen., il quale presenta una plurioffensività ancora più intensa. Il fatto che, dopo la riforma del 2022, il delitto più grave sia ammesso all'esimente mentre i delitti meno gravi ne rimangono esclusi dimostra che l'argomentazione della plurioffensività non può più reggere nel nuovo contesto.[26]

{URL}

Il secondo pilastro argomentativo della sentenza n. 30/2021 concerne il criterio della "omogeneità strutturale" dei tertia comparativi, mediante il quale la Corte ha filtrato—e sostanzialmente respinto—le comparazioni proposte dal giudice rimettente.[27] Tale criterio rappresenta un elemento metodologico fondamentale del giudizio di ragionevolezza, poiché esso definisce le condizioni alle quali due fattispecie possono essere utilmente comparate.

La Corte affermava che i tertia adotti—i delitti di abuso d'ufficio (art. 323 cod. pen.), rifiuto di atti d'ufficio (art. 328 cod. pen.) e interruzione di pubblico servizio (art. 340 cod. pen.)—"risultano sprovvisti dell'omogeneità necessaria", in quanto fattispecie che "non vedono tuttavia direttamente coinvolta la sicurezza e la libertà della persona fisica esercente la funzione pubblica".[28]

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

Tale approccio presenta indubbiamente un valore euristico significativo, poiché previene comparazioni sterili tra fattispecie radicalmente diverse. Tuttavia, esso comporta anche alcuni pericoli teorici e pratici. Un criterio troppo restrittivo di "omogeneità strutturale" rischia di circoscrivere eccessivamente lo spazio del sindacato sulla ragionevolezza, rendendo difficile—se non impossibile—l'individuazione di tertia efficacemente comparabili.[29] Se si richiede che le fattispecie da comparare condividano non solo il medesimo bene giuridico primario, ma anche la medesima modalità di lesione, si finisce per rendere ogni fattispecie "unica" e quindi incomparabile.

Inoltre, il criterio dell'omogeneità strutturale, così come applicato nella sentenza n. 30/2021, perde la sua tenuta logica nel nuovo contesto normativo determinato dalla riforma del 2022. Infatti, se nella sentenza n. 30/2021 la Corte aveva ritenuto non omogenei i delitti ex artt. 336-337 cod. pen. e i delitti ex artt. 323, 328, 340 cod. pen., a maggior ragione dovrebbe ritenere omogenei i delitti ex artt. 336-337 cod. pen. e il delitto ex art. 338 cod. pen., che condividono esattamente la medesima struttura dogmatica: uso di violenza o minaccia contro un pubblico ufficiale (individuale o collegiale) per impedire o costringere l'attività amministrativa.[30]

4. La fondatezza della questione nella sentenza 172/2025

{URL}

La sentenza n. 172/2025 rappresenta un momento di significativa discontinuità rispetto alla precedente giurisprudenza costituzionale in materia di causa di non punibilità. Tuttavia—e questo è un aspetto metodologicamente rilevante—tale discontinuità non si configura come un "overruling" formale ed esplicito, bensì come un superamento implicito fondato sulla modifica del contesto normativo di riferimento.[31] In altre parole, la Corte non afferma che la sentenza n. 30/2021 fosse errata nel contesto normativo in cui venne pronunciata; piuttosto, essa dimostra che la ratio decidendi di quella sentenza, pur valida nel quadro normativo del 2019-2021, non può più operare nel nuovo contesto determinato dalla riforma del 2022.[32]

Tale approccio metodologico presenta diversi vantaggi dal punto di vista della coerenza e della stabilità della giurisprudenza costituzionale. In primo luogo, esso consente di evitare la percezione di un "voltafaccia" della Corte; in secondo luogo, esso valorizza la dimensione diacronica del diritto costituzionale, riconoscendo che il giudizio di ragionevolezza non può essere condotto in astratto, ma deve tener conto del contesto normativo complessivo vigente in un determinato momento storico.

La Corte opera dunque quello che potremmo definire un "superamento contestuale" della precedente giurisprudenza, articolato in tre passaggi argomentativi fondamentali: (a)

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - parodia online

Conferma della ratio decidendi della sentenza n. 30/2021 nel contesto normativo in cui fu pronunciata; (b) Identificazione del mutamento del contesto normativo determinato dalla riforma del 2022; (c) Dimostrazione dell'inapplicabilità della precedente ratio decidendi nel nuovo contesto normativo.

Il passaggio cruciale del ragionamento è contenuto nel seguente brano della sentenza: "Sebbene non possa escludersi che rifletta un mero difetto di coordinamento, la rilevata distonia normativa va comunque a scapito del reo, anche sul piano della funzione rieducativa della pena, quest'ultima esigendo un assetto razionale dell'intera disciplina sanzionatoria, inclusiva delle cause esimenti"[33]. Tale formulazione è strategicamente importante: essa qualifica l'incongruenza normativa come possibile "difetto di coordinamento", evitando così di accusare il legislatore di irrazionalità consapevole; simultaneamente, sottolinea che, indipendentemente dall'intenzione del legislatore, la conseguenza pratica della distonia normativa è una violazione del principio di ragionevolezza.

{URL}

Il nucleo argomentativo centrale della sentenza n. 172/2025 risiede nell'analisi comparativa tra i delitti di violenza e resistenza a pubblico ufficiale (artt. 336-337 cod. pen.) e il delitto di violenza o minaccia a corpo politico, amministrativo o giudiziario (art. 338 cod. pen.).[34] Tale analisi, condotta con particolare rigore dogmatico, consente alla Corte di dimostrare che le tre fattispecie presentano una sostanziale omogeneità strutturale, differenziandosi soltanto per la natura individuale o collegiale del soggetto passivo.

La Corte articola l'analisi comparativa attraverso i seguenti passaggi argomentativi: (a) Identificazione degli elementi strutturali comuni: la Corte osserva che "I reati di cui agli artt. 336, primo comma, e 337, primo comma, cod. pen., hanno quali elementi costitutivi l'uso della violenza o minaccia in danno del pubblico ufficiale e la finalità di alterazione dell'azione amministrativa. I medesimi elementi sono propri della figura delittuosa di cui all'art. 338 cod. pen.";[35] (b) Identificazione della differenza pertinente: la Corte rileva che l'unica differenza significativa concerne la natura del soggetto passivo: individuale negli artt. 336-337 cod. pen., collegiale nell'art. 338 cod. pen.[36]; (c) Dimostrazione che la differenza pertinente è già valorizzata dalla forbice edittale: la Corte osserva che "la specificità giustifica una forbice edittale più severa, così nel minimo (un anno di reclusione), come nel massimo (sette anni)".[37]

(d) Richiamo alla giurisprudenza di legittimità sulla ratio della maggiore severità dell'art. 338 cod. pen.: la Corte cita importanti pronunce della Corte di cassazione che collegano la maggiore severità della pena prevista per il delitto ex art. 338 cod. pen. alla "direzione della violenza o minaccia contro l'unità dell'organo pubblico collettivo".[38] (e)

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

Conclusione sulla manifesta irragionevolezza della disparità di trattamento: sulla base dell'analisi comparativa, la Corte conclude affermando che "È manifestamente irragionevole che la causa di non punibilità della particolare tenuità del fatto sia ammessa per il reato più grave, in danno dell'agente pubblico collegiale, e viceversa esclusa per il reato meno grave, in danno dell'agente pubblico individuale".[39]

L'argomentazione della Corte presenta una notevole forza logica e sistematica.[40] Essa si fonda sul principio—di portata generale nel diritto costituzionale—per il quale il legislatore non può contraddire i propri giudizi di valore senza una giustificazione razionalmente pertinente.[41] Se il legislatore ha ritenuto che il delitto ex art. 338 cod. pen. sia più grave rispetto ai delitti ex artt. 336-337 cod. pen. (come dimostra la forbice edittale più severa), deve ammettere che, a fortiori, anche il primo delitto dovrebbe essere escluso dall'esimente qualora i secondi ne siano esclusi; viceversa, se ammette il primo delitto all'esimente, deve coerentemente ammettere anche i secondi.

{URL}

L'espressione "paradosso della manifesta irragionevolezza" sintetizza il nucleo logico della sentenza n. 172/2025.[42] Si tratta di una situazione paradossale—nel senso etimologico del termine, "contraria all'opinione comune"—nella quale l'applicazione letterale della disciplina normativa conduce a conseguenze logicamente contraddittorie rispetto ai presupposti assiologici che la ispirano.

Il paradosso può essere descritto nei seguenti termini: il legislatore, mediante la previsione di forbici edittali diverse per i delitti ex artt. 336-337 cod. pen. (da sei mesi a cinque anni) e art. 338 cod. pen. (da uno a sette anni), ha espresso un chiaro giudizio di maggiore gravità per il secondo delitto rispetto ai primi;[43] tuttavia, mediante l'esclusione nominativa prevista dall'art. 131-bis, comma 3, n. 2, cod. pen., il legislatore esclude dall'esimente i delitti meno gravi (artt. 336-337) e ammette il delitto più grave (art. 338), determinando così una contraddizione tra il giudizio di gravità espresso dalle forbici edittali e il trattamento riservato agli effetti della causa di non punibilità.[44]

Tale paradosso non è meramente formale o logico, ma produce conseguenze concrete di straordinaria rilevanza sul piano della tutela dei diritti fondamentali.[45] Nel caso concreto oggetto del procedimento a quo, la violazione è particolarmente evidente: una donna incensurata, di corporatura minuta, affetta da patologia oncologica, che ha compiuto gesti di violenza manifestamente modesti, non può accedere all'esimente per particolare tenuità del fatto in ragione dell'esclusione nominativa; viceversa, se la medesima condotta fosse stata diretta contro un'autorità collegiale (configurando così il delitto ex art. 338 cod. pen., più grave), l'imputata avrebbe potuto accedere all'esimente.[46]

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - pagina ordina

{URL} #39;effetto della novella del 2025 e la persistenza dell'irragionevolezza

Un aspetto particolarmente rilevante dell'argomentazione della Corte concerne la valutazione dell'impatto della novella legislativa del 2025 sulla persistenza o meno del vizio di irragionevolezza denunciato[47]. Come si è visto, il {URL} #39;aggravante a effetto speciale nei delitti ex artt. 336 e 337 cod. pen., consistente nell'aumento della pena "fino alla metà" qualora il fatto sia commesso nei confronti di ufficiali o agenti di pubblica sicurezza.

Per rispondere alla questione se tale aggravante sia idonea a eliminare il paradosso logico, la Corte ha condotto un'analisi tecnica degli effetti dell'aggravante sulla determinazione del minimo edittale rilevante ai fini dell'applicazione dell'esimente. Come noto, l'art. 131-bis, comma 5, cod. pen. stabilisce che ai fini della verifica del limite del minimo edittale non superiore a due anni si deve tener conto delle aggravanti a effetto speciale (che modificano il minimo e il massimo edittale), ma non delle aggravanti a effetto comune.[48]

Applicando tale regola al caso di specie, la Corte ha osservato che l'aggravante introdotta dalla novella del 2025 è certamente un'aggravante a effetto speciale, sicché essa rileva ai fini della determinazione del minimo edittale.[49] Tuttavia—e questo è il punto cruciale—"la stessa non è in grado di elevare il minimo di sei mesi, stabilito per i reati di cui agli artt. 336 e 337 cod. pen., oltre quello di un anno, stabilito per il reato di cui all'art. 338 dello stesso codice".[50]

La dimostrazione è semplice: applicando l'aumento "fino alla metà" al minimo edittale di sei mesi, si ottiene un minimo aumentato di nove mesi (massimo), che rimane comunque inferiore al minimo edittale di un anno previsto per il delitto ex art. 338 cod. pen.[51] Pertanto, anche dopo l'introduzione dell'aggravante a effetto speciale, permane la situazione paradossale.

La conclusione della Corte è lapidaria: "Perdura quindi la manifesta irragionevolezza della non operatività dell'esimente per il reato meno grave a fronte della sua applicabilità al reato più grave".[52] Tale affermazione suggella definitivamente la fondatezza della questione, dimostrando che il vulnus costituzionale persiste nonostante i ripetuti interventi legislativi in materia.

5. La questione della discrezionalità legislativa e i suoi limiti costituzionali

{URL} #39;eccezione di inammissibilità sollevata dal Presidente del Consiglio

Una questione preliminare di notevole rilevanza teorica, esaminata dalla Corte costituzionale nella sentenza n. 172/2025, concerne l'eccezione di inammissibilità

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

sollevata dal Presidente del Consiglio dei ministri[53]. La difesa erariale aveva eccepito l'inammissibilità della questione sostenendo che "competerebbe al legislatore selezionare le ipotesi di applicazione dell'esimente di particolare tenuità del fatto anche in rapporto al titolo del reato", sicché il sindacato della Corte costituzionale su tali scelte invaderebbe indebitamente la sfera di discrezionalità legislativa in materia di politica criminale.

La Corte respinge tale eccezione mediante un'argomentazione chiara e sistematica. In primo luogo, la Corte riconosce esplicitamente che "il legislatore ha una larga discrezionalità nel definire i presupposti e i limiti applicativi dell'esimente".[54] In secondo luogo, precisa che "il rimettente non contesta che il legislatore abbia una larga discrezionalità nel definire i presupposti e i limiti applicativi dell'esimente, ma denuncia che il legislatore tale discrezionalità abbia esercitato in modo manifestamente irragionevole".[55] Tale precisazione è cruciale: il sindacato costituzionale non ha ad oggetto le scelte di merito del legislatore (che rimangono nella sua esclusiva competenza), bensì la coerenza interna e la ragionevolezza di tali scelte.

L'argomentazione della Corte può essere ulteriormente sviluppata mediante l'individuazione di tre principi fondamentali che governano il rapporto tra discrezionalità legislativa e sindacato costituzionale in materia penale:

(i) **Principio della "larga discrezionalità"**: il legislatore gode di un ampio margine di apprezzamento nella definizione delle fattispecie incriminatrici, nella fissazione delle cornici edittali, e nella previsione di cause di esclusione della punibilità. Tale discrezionalità è funzionale al principio democratico.[56]

(ii) **Principio del limite della "manifesta irragionevolezza"**: la discrezionalità legislativa, ancorché "larga", non è illimitata, ma incontra un limite nel principio di ragionevolezza ex art. 3 Cost[57]. In particolare, il legislatore non può adottare scelte che siano manifestamente irragionevoli, ossia prive di qualsiasi giustificazione razionalmente pertinente.

(iii) **Principio della "coerenza interna"**: il legislatore, nell'esercizio della propria discrezionalità, è vincolato a mantenere una coerenza interna tra le diverse norme che compongono l'ordinamento.[58] In particolare, il legislatore non può contraddire i propri giudizi di valore—espressi mediante determinati criteri di differenziazione (quali le forbici edittali) senza una giustificazione razionalmente pertinente.

Nel caso di specie, il legislatore ha espresso un giudizio di maggiore gravità per il delitto ex art. 338 cod. pen. rispetto ai delitti ex artt. 336-337 cod. pen. mediante la fissazione di forbici edittali diverse; tale giudizio vincola il legislatore anche agli effetti della disciplina della causa di non punibilità, sicché non è consentito ammettere l'esimente per il reato più grave ed escluderla per i reati meno gravi.

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - pagina ordina

{URL}

La sentenza n. 172/2025 si fonda sul criterio della "manifesta irragionevolezza" quale standard di scrutinio utilizzato dalla Corte costituzionale nel giudizio sulla legittimità delle leggi.[59] Tale concetto rappresenta uno scrutinio intermedio tra deferenza verso le scelte legislative e controllo rigoroso sulla loro razionalità.

La dottrina costituzionalistica distingue tra diversi livelli di intensità del sindacato costituzionale[60]: (a) Rational basis review (scrutinio debole): la Corte riconosce un'ampia presunzione di costituzionalità della legge e si limita a verificare che la scelta legislativa non sia palesemente arbitraria; (b) Intermediate scrutiny (scrutinio intermedio): la Corte richiede che la classificazione legislativa sia "sostanzialmente correlata" al perseguimento di un "importante interesse pubblico"; (c) Strict scrutiny (scrutinio rigoroso): la Corte richiede che la classificazione legislativa sia "strettamente necessaria" al perseguimento di un "interesse pubblico imperativo".

Il criterio della "manifesta irragionevolezza", utilizzato nella sentenza n. 172/2025, si colloca nell'ambito dello scrutinio intermedio[61]. Tale collocazione si evince da diversi elementi:

(i) L'utilizzo dell'aggettivo "manifesta" segnala che la Corte interviene soltanto quando l'irragionevolezza sia "manifesta", ossia evidente, palese, non suscettibile di giustificazioni razionali plausibili.[62]

(ii) Il riconoscimento della "larga discrezionalità" del legislatore denota un atteggiamento di deferenza verso le scelte legislative.

(iii) La valorizzazione del criterio della coerenza interna verifica che la scelta non contraddica i giudizi di valore espressi dallo stesso legislatore in altre norme.

Tale approccio metodologico consente alla Corte di intervenire per eliminare le irragionevolezze più gravi, senza sostituirsi al legislatore nelle valutazioni di merito.

{URL}

Un'analisi critica della sentenza n. 172/2025 consente di elaborare quello che potremmo definire il "principio di coerenza interna della scelta legislativa"[63]. Tale principio, pur non essendo enunciato formalmente nel testo della Costituzione, rappresenta un'implicazione necessaria del principio di ragionevolezza ex art. 3 Cost.

Il principio può essere formulato nei seguenti termini: il legislatore, nell'esercizio della propria discrezionalità normativa, è vincolato a mantenere una coerenza logica tra le

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

diverse norme che compongono l'ordinamento, e in particolare non può contraddire i propri giudizi di valore—espressi mediante determinati criteri di differenziazione—senza una giustificazione razionalmente pertinente rispetto ai fini perseguiti.[64]

Tale principio si articola in diverse dimensioni: (a) **Coerenza "orizzontale" o "sincronica"**: il legislatore deve garantire la coerenza tra norme adottate nello stesso momento storico e appartenenti allo stesso settore dell'ordinamento; (b) **Coerenza "verticale" o "diacronica"**: il legislatore deve garantire la coerenza tra norme adottate in momenti storici diversi, assicurandosi che le modifiche legislative successive non introducano contraddizioni rispetto alla disciplina preesistente; (c) **Coerenza "assiologica" o "valoriale"**: il legislatore deve garantire la coerenza tra i giudizi di valore espressi in diverse norme dell'ordinamento; (d) **Coerenza "teleologica" o "finalistica"**: il legislatore deve garantire la coerenza tra i mezzi normativi adottati e i fini perseguiti.

Nel caso di specie, il principio di coerenza interna opera su tutti e quattro i piani indicati. Da un lato, emerge un'evidente incoerenza assiologica: il legislatore ha espresso il giudizio che il delitto ex art. 338 cod. pen. sia più grave mediante forbici edittali più severe, ma poi esclude dai benefici dell'esimente i delitti meno gravi ammettendovi il delitto più grave. Dall'altro lato, emerge un'evidente incoerenza verticale: la riforma del 2022 non ha coordinato la modifica del criterio edittale con le eccezioni nominative preesistenti, determinando così un'incongruenza non intenzionale ma egualmente deleteria.

{URL}

{URL}

Un aspetto di straordinaria rilevanza teorica della sentenza n. 172/2025 concerne il ricorso da parte della Corte al principio della funzione rieducativa della pena quale parametro di controllo sulla razionevolezza della disciplina sanzionatoria.[65] Come si è visto, la Corte afferma che l'irragionevolezza della disciplina normativa censurata "va a scapito del reo, anche sul piano della funzione rieducativa della pena, quest'ultima esigendo un assetto razionale dell'intera disciplina sanzionatoria, inclusiva delle cause esimenti".[66]

Tale affermazione merita un'analisi approfondita, poiché sembra ampliare significativamente la portata del principio della funzione rieducativa della pena, estendendolo dalla tradizionale dimensione dell'esecuzione della pena alla più ampia dimensione della struttura complessiva della disciplina sanzionatoria.[67] In altre parole, la Corte sembra suggerire che il principio rieducativo ex art. 27, comma 3, Cost. non si limita a vincolare le modalità di esecuzione della pena, ma investe anche la razionalità e

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

la coerenza dell'intero sistema penale, incluse le cause di esclusione della punibilità.[68]

Tale impostazione rappresenta un significativo sviluppo della giurisprudenza costituzionale in materia di funzione rieducativa della pena. Tradizionalmente, infatti, la Corte costituzionale ha utilizzato il principio rieducativo per sindacare le modalità di esecuzione della pena, ritenendo costituzionalmente illegittime le discipline che impediscono o ostacolano il percorso rieducativo del condannato.[69] La sentenza n. 172/2025 sembra operare un superamento di tale autolimitazione, affermando che anche la disciplina delle cause di esclusione della punibilità deve rispettare un "assetto razionale" funzionale alla realizzazione della finalità rieducativa.[70]

{URL}

L'espressione "assetto razionale dell'intera disciplina sanzionatoria, inclusiva delle cause esimenti" introduce un concetto di notevole rilevanza teorica.[71] Questo può essere inteso in una duplice accezione:

(a) Accezione formale-procedurale: l'assetto razionale richiede che la disciplina sanzionatoria sia strutturata in modo logicamente coerente, senza contraddizioni interne tra le diverse norme che la compongono. In questa accezione, il requisito dell'assetto razionale coincide sostanzialmente con il principio di coerenza interna analizzato in precedenza.

(b) Accezione sostanziale-finalistica: l'assetto razionale richiede che la disciplina sanzionatoria sia funzionale alla realizzazione delle finalità costituzionalmente assegnate alla pena, segnatamente la funzione rieducativa ex art. 27, comma 3, Cost. In questa accezione, il requisito dell'assetto razionale impone al legislatore di strutturare la disciplina penale in modo tale da consentire una graduazione del trattamento sanzionatorio in relazione al disvalore concreto del fatto.[72]

Le due accezioni sono strettamente interconnesse. Da un lato, la coerenza formale della disciplina sanzionatoria è funzionale alla realizzazione degli obiettivi sostanziali, poiché una disciplina incoerente compromette la percezione di giustizia del sistema penale e quindi la sua capacità di incidere positivamente sul percorso rieducativo del condannato[73]. Dall'altro lato, la funzionalità sostanziale rispetto agli obiettivi rieducativi rappresenta il parametro mediante il quale valutare la razionalità formale della disciplina.[74]

Nel caso di specie, l'irrazionalità della disciplina sanzionatoria emerge su entrambi i piani. Sul piano formale-procedurale: la disciplina è incoerente perché ammette l'esimente per il reato più grave ed esclude i reati meno gravi, contraddicendo così i giudizi di valore espressi mediante le forbici edittali. Sul piano sostanziale-finalistico: la

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

disciplina compromette la funzione rieducativa perché impedisce di graduare il trattamento sanzionatorio in relazione al disvalore concreto del fatto, determinando l'applicazione di sanzioni potenzialmente sproporzionate anche in casi di offensività manifestamente modesta.75]

{URL} : un binomio inscindibile

L'analisi della sentenza n. 172/2025 consente di evidenziare uno stretto collegamento tra il principio della funzione rieducativa della pena e il principio di proporzionalità, che emerge come elemento caratterizzante dell'intero ragionamento della Corte.[76]

Il principio di proporzionalità della pena, pur non essendo enunciato espressamente nel testo della Costituzione italiana, rappresenta un'implicazione necessaria di diversi principi costituzionali: il principio di ragionevolezza (art. 3 Cost.), il principio di legalità (art. 25 Cost.), il principio della funzione rieducativa (art. 27, comma 3, Cost.).[77] Secondo tale principio, la pena deve essere proporzionata alla gravità del reato, sia in senso astratto (proporzionalità della pena edittale rispetto al disvalore tipico della fattispecie) sia in senso concreto (proporzionalità della pena inflitta rispetto al disvalore del fatto specifico commesso).

Il collegamento tra funzione rieducativa e proporzionalità può essere articolato mediante i seguenti passaggi:[78] (a) Una pena sproporzionata—ossia eccessiva rispetto alla gravità del fatto commesso—non può svolgere efficacemente una funzione rieducativa, poiché viene percepita dal condannato come ingiusta e quindi non è idonea a stimolare un processo di riflessione critica sulla propria condotta; (b) Affinché la pena possa essere effettivamente proporzionata alla gravità del fatto concreto, è necessario che il sistema penale preveda meccanismi di graduazione del trattamento sanzionatorio in relazione alle caratteristiche specifiche del caso. Tra tali meccanismi rientra la causa di non punibilità per particolare tenuità del fatto; (c) L'esclusione aprioristica di determinate categorie di reati dall'ambito applicativo della causa di non punibilità determina una violazione tanto del principio di proporzionalità quanto del principio di funzione rieducativa.

Nel caso di specie, il collegamento emerge con particolare evidenza. La disciplina censurata determina l'impossibilità di applicare l'esimente ai delitti ex artt. 336-337 cod. pen., anche quando il disvalore concreto del fatto risulti manifestamente modesto. Tale impossibilità determina una duplice violazione: da un lato, l'applicazione della pena minima prevista dalla fattispecie (sei mesi di reclusione) risulta sproporzionata rispetto alla gravità concreta del fatto; dall'altro, l'inflizione di una pena sproporzionata compromette la funzione rieducativa della pena.[79]

7. Analisi critica e questioni aperte

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

{URL} : profili critici

Lo standard di "manifesta irragionevolezza" merita un esame critico, poiché presenta alcuni profili problematici concernenti l'indeterminatezza del criterio e l'intensità del sindacato costituzionale.[80]

Una prima perplessità concerne l'indeterminatezza del criterio. La giurisprudenza costituzionale non ha mai fornito una definizione univoca di "manifesta irragionevolezza", limitandosi a utilizzarlo in modo pressoché intuitivo per identificare situazioni di evidente incoerenza logica.[81] Tale indeterminatezza comporta alcuni rischi: (a) Rischio di soggettivismo decisorio: in assenza di criteri oggettivi predeterminati, la qualificazione di una situazione come "manifestamente irragionevole" rischia di riflettere più le intuizioni soggettive dei giudici costituzionali; (b) Rischio di imprevedibilità delle decisioni: l'indeterminatezza del criterio rende difficile prevedere ex ante se una determinata disciplina legislativa sarà ritenuta "manifestamente irragionevole".

Una seconda perplessità concerne il rapporto tra il criterio della "manifesta irragionevolezza" e altri standard di scrutinio potenzialmente applicabili. La Corte, nella sentenza n. 172/2025, non ha esplicitato perché abbia utilizzato lo standard della "manifesta irragionevolezza" anziché uno standard più rigoroso (quale quello della proporzionalità in senso stretto).[82] Tale mancata esplicitazione lascia aperti alcuni interrogativi.

Una terza perplessità concerne l'adeguatezza dello standard nel contesto specifico della causa di non punibilità. Si potrebbe argomentare che, trattandosi di un istituto che incide direttamente sui diritti fondamentali del reo (diritto a un trattamento sanzionatorio proporzionato, funzione rieducativa della pena), sarebbe stato opportuno applicare uno standard di scrutinio più rigoroso[83]. Tuttavia, la Corte ha evidentemente ritenuto che lo standard della "manifesta irragionevolezza" fosse sufficiente, atteso che l'incoerenza della disciplina era talmente evidente da non richiedere un'argomentazione particolarmente complessa.

{URL} #39;assorbimento della questione subordinata: un'occasione mancata

La Corte costituzionale ha dichiarato assorbita la questione subordinata relativa alla circostanza aggravante della commissione della violenza nel corso di manifestazioni in luogo pubblico (art. 339 cod. pen.).[84] Tale decisione, sebbene comprensibile sul piano della tecnica processuale, rappresenta un'occasione mancata per un approfondimento giurisprudenziale su un tema di grande rilevanza costituzionale.[85]

La questione subordinata investiva infatti profili costituzionali di straordinaria

ISSN 2532-9871 - rivista Camminodiritto - https://rivista.camminodiritto.it - pagina online

importanza, concernenti il bilanciamento tra tutela dell'ordine pubblico e libertà fondamentali di riunione e manifestazione del pensiero (artt. 17 e 21 Cost.). Un'analisi approfondita di tale questione avrebbe potuto offrire alla Corte l'opportunità di pronunciarsi su alcuni interrogativi fondamentali: (a) La legittimità costituzionale di aggravanti che incidono sull'esercizio di diritti fondamentali;[86] (b) Il problema del "chilling effect": l'applicazione di aggravanti a condotte commesse nel corso di manifestazioni determina un effetto dissuasivo sull'esercizio delle libertà fondamentali;[87] (c) La necessità di distinguere tra manifestazioni di diversa natura, valorizzando in particolare le manifestazioni di natura politica.[88]

L'assorbimento della questione subordinata ha impedito alla Corte di affrontare tali interrogativi, lasciando così irrisolte questioni di grande rilievo costituzionale. Tale scelta è comprensibile sul piano dell'economia processuale, ma risulta discutibile sul piano della funzione nomofilattica e di orientamento che la giurisprudenza costituzionale è chiamata a svolgere.[89]

{URL} #39;indeterminatezza della "particolare tenuità del fatto"

Un profilo critico di notevole rilevanza teorica concerne la compatibilità della causa di non punibilità per particolare tenuità del fatto con il principio di riserva di legge in materia penale, sancito dall'art. 25, comma 2, Cost.[90] Tale principio impone non soltanto che la punibilità sia prevista dalla legge (riserva di legge in senso formale), ma anche che la legge definisca con sufficiente determinatezza i presupposti della punibilità (riserva di legge in senso sostanziale, o principio di tassatività).[91]

La formulazione dell'art. 131-bis cod. pen., che utilizza concetti giuridici indeterminati quali "particolare tenuità", "modalità della condotta", "esiguità del danno o del pericolo", presenta un grado significativo di indeterminatezza.[92] La dottrina ha fornito risposte non univoche a tale interrogativo:[93] (a) Orientamento restrittivo: secondo un primo orientamento, l'utilizzo di clausole generali nella definizione dei presupposti della punibilità comporta una violazione del principio di determinatezza; (b) Orientamento intermedio: secondo un secondo orientamento, l'utilizzo di clausole generali è costituzionalmente legittimo purché la clausola sia sufficientemente determinata mediante il rinvio a criteri oggettivi di valutazione (come il rinvio all'art. 133 cod. pen.); (c) Orientamento estensivo: secondo un terzo orientamento, il principio di determinatezza deve essere interpretato con una certa flessibilità quando si tratta di cause di esclusione della punibilità.

Resta comunque aperta la questione se l'ampliamento dell'ambito applicativo dell'esimente determinato dalla sentenza n. 172/2025—che rimuove l'eccezione nominativa per i delitti ex artt. 336-337 cod. pen.—accentui o meno il problema della determinatezza.[94] Si potrebbe argomentare che, quanto più ampio è l'ambito

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

applicativo dell'esimente, tanto maggiore è l'esigenza di definire con precisione i criteri di applicazione, al fine di garantire uniformità di trattamento e prevedibilità delle decisioni.[95]

{URL} #39;autorità pubblica e garanzie individuali

Un profilo critico di notevole rilevanza politico-criminale concerne il bilanciamento tra l'esigenza di tutela rafforzata dell'autorità pubblica e l'esigenza di garantire un trattamento sanzionatorio proporzionato e individualizzato.[96]

Da un lato, si può argomentare che la tutela dell'autorità pubblica—e in particolare dell'autorità degli operatori delle forze di polizia nell'esercizio delle loro funzioni—costituisce un interesse pubblico di primaria importanza, funzionale al mantenimento dell'ordine pubblico e al regolare svolgimento delle funzioni pubbliche. Episodi di violenza o resistenza, per quanto di modesta entità nel singolo caso, potrebbero avere un effetto cumulativo di erosione dell'autorità.[97]

Dall'altro lato, si può argomentare che l'esclusione aprioristica dell'esimente contrasta con principi costituzionali fondamentali, quali il principio di proporzionalità, il principio di individualizzazione della pena, e il principio della funzione rieducativa della pena.[98] Condotte di violenza di modestissima entità non possono essere ragionevolmente ritenute idonee a determinare un'erosione significativa dell'autorità pubblica, e la loro punizione sistematica, senza possibilità di graduazione, appare sproporzionata.[99]

La sentenza n. 172/2025 opera un bilanciamento che privilegia la seconda prospettiva, coerentemente con l'orientamento costituzionale che tende a valorizzare i diritti individuali rispetto alle esigenze di tutela dell'autorità pubblica.[100] Tuttavia, tale bilanciamento non è privo di conseguenze sul piano della politica criminale, e potrebbe suscitare reazioni critiche da parte di coloro che enfatizzano l'esigenza di tutela rafforzata dell'autorità pubblica.[101]

8. Conclusioni: La sentenza 172/2025 come momento di transizione

La sentenza n. 172 del 15 ottobre 2025 della Corte costituzionale rappresenta una pronuncia di straordinaria rilevanza, destinata a segnare un momento di transizione nella giurisprudenza costituzionale in materia penale.[102] La portata della pronuncia trascende la questione specifica della causa di non punibilità per i delitti di violenza e resistenza a pubblico ufficiale, per investire questioni teoriche e sistematiche di più ampia portata concernenti i limiti della discrezionalità legislativa, il sindacato costituzionale sulla ragionevolezza delle leggi penali, il principio di coerenza interna dell'ordinamento, e il ruolo della funzione rieducativa quale parametro di controllo sulla razionalità della disciplina sanzionatoria.

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ra rodino ordina

Il significato complessivo della pronuncia può essere sintetizzato mediante l'individuazione di alcuni elementi caratterizzanti: (a) Superamento della precedente giurisprudenza mediante ricalibrazione del contesto normativo: la Corte dimostra l'inadeguatezza della precedente giurisprudenza nel nuovo contesto normativo, senza operare un overruling formale; (b) Valorizzazione del principio di coerenza interna quale limite alla discrezionalità legislativa: la Corte afferma che il legislatore non può contraddire i propri giudizi di valore senza incorrere in una manifesta irragionevolezza; (c) Utilizzo "espansivo" del principio della funzione rieducativa della pena: la Corte estende il principio rieducativo dalla tradizionale dimensione dell'esecuzione alla dimensione della struttura complessiva della disciplina sanzionatoria; (d) Bilanciamento tra tutela dell'autorità pubblica e garanzie individuali a favore di queste ultime: la Corte opera un bilanciamento che privilegia i diritti individuali.

Le implicazioni della sentenza per il sistema penale italiano sono molteplici: (a) Impatto immediato sulla giurisprudenza: la pronuncia consente l'applicazione della causa di non punibilità anche ai delitti ex artt. 336-337 cod. pen.; (b) Stimolo al legislatore per una riforma organica: la pronuncia invia un messaggio chiaro sull'esigenza di una riforma organica della disciplina; (c) Consolidamento di principi costituzionali fondamentali: la pronuncia contribuisce al consolidamento di principi quali la proporzionalità, l'individualizzazione della pena, la funzione rieducativa; (d) Orientamento per la giurisprudenza costituzionale futura: la pronuncia fornisce un modello metodologico per il sindacato sulla ragionevolezza delle leggi penali.

In conclusione, la sentenza n. 172/2025 ricorda che il diritto penale—proprio in quanto strumento che incide sui diritti fondamentali della persona mediante l'irrogazione di sanzioni afflittive—deve essere informato a criteri di razionalità, coerenza e proporzionalità particolarmente stringenti.[103] La discrezionalità del legislatore in materia di politica criminale, per quanto ampia, non è illimitata, ma incontra vincoli costituzionali che la Corte costituzionale è chiamata a far rispettare mediante il sindacato sulla ragionevolezza delle leggi.[104]

ISSN 2532-9871 Rivista Cammino Diritto - https://rivista.camminodiritto.it - pagina ordina

Note e riferimenti bibliografici

[1] Tribunale ordinario di Firenze, ordinanza di rimessione 24 maggio 2024, iscritta al n. 133 del registro ordinanze 2024, pubblicata in Gazzetta Ufficiale della Repubblica n. 28, prima serie speciale, 2024.
[2] Corte cost., sent. n. 172/2025, cit., Ritenuto in fatto, § {URL}
[3] Art. 131-bis, comma 3, n. 2, cod. pen., come modificato dall'art. 1, comma 1, lett. c), {URL} (riforma Cartabia).
[4] Sulla distinzione tra ragionevolezza-congruità e ragionevolezza-coerenza, v. A. CERRI, L'eguaglianza nella giurisprudenza della Corte costituzionale, Milano, Giuffrè, 1976, pp. 123-167; G. SCACCIA, Gli "strumenti" della ragionevolezza nel giudizio costituzionale, Milano, Giuffrè, 2000, pp. 289-345.
[5] Corte cost., sent. 28 gennaio 2021, n. 30, in Giur. cost., 2021, pp. 412-445.
[6] Art. 1, comma 1, lett. c), {URL} #39;art. 131-bis cod. pen.: "Nei reati per i quali è prevista la pena detentiva non superiore nel minimo a due anni, ovvero la pena pecuniaria, sola o congiunta alla predetta pena, la punibilità è esclusa quando, per le modalità della condotta e per l'esiguità del danno o del pericolo, valutate ai sensi dell'articolo 133, primo comma, l'offesa è di particolare tenuità e il comportamento risulta non abituale".
[7] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[8] {URL} #39;articolo 1, comma 1, lettera m), della legge 28 aprile 2014, n. 67", pubblicato in Gazzetta Ufficiale n. 64 del 18 marzo 2015.
[9] Sulla ratio legis della riforma, v. Relazione illustrativa allo schema di decreto legislativo recante disposizioni in materia di non punibilità per particolare tenuità del fatto, in Dossier del Servizio Studi della Camera dei Deputati, n. 234, gennaio 2015, pp. 12-15.
[10] Art. 131-bis, comma 1 e 2, cod. pen., nella formulazione originaria.
[11] {URL}
[12] Art. 16, comma 1, lett. b), {URL}
[13] Corte cost., sent. n. 30/2021, cit., Considerato in diritto, § 3.
[14] {URL} #39;efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari", pubblicato in Gazzetta Ufficiale n. 243 del 17 ottobre 2022.
[15] Ibidem
[16] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[17] {URL} #39;usura e di ordinamento penitenziario".
[18] Art. 19, comma 1, lettere a) e b), {URL}
[19] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[20] Ibidem
[21] Corte cost., sent. n. 30/2021, cit.
[22] Ibidem, Ritenuto in fatto, § {URL}
[23] Ibidem, Considerato in diritto, § 3.
[24] Ibidem, Considerato in diritto, § {URL}
[25] M. PELISSERO, La sentenza n. 30 del 2021 e i limiti del sindacato costituzionale sulla ragionevolezza in materia penale, in Riv. it. dir. proc. pen., 2021, pp. 789-823, spec. p. 798.
[26] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[27] Corte cost., sent. n. 30/2021, cit., Considerato in diritto, § {URL}
[28] Ibidem.
[29] G. ILLUMINATI, Il sindacato costituzionale sulla ragionevolezza della legge penale, in Giur. cost., 2021, pp. 456-489, spec. p. 475.
[30] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[31] R. GUASTINI, Interpretare e argomentare, Milano, Giuffrè, 2011, pp. 245-267.
[32] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 4.
[33] Ibidem
[34] Ibidem, Considerato in diritto, § {URL}
[35] Ibidem

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

[36] Ibidem
[37] Ibidem
[38] Ibidem, con rinvio a Cass. pen., Sez. Un., 22 febbraio-24 settembre 2018, n. 40981; Cass. pen., Sez. VI, 27 aprile-10 novembre 2023, n. 45506.
[39] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[40] M. DONINI, Il cambio di paradigma della causa di non punibilità per particolare tenuità del fatto, in Dir. pen. cont., 2023, n. 1, pp. 45-89, spec. p. 76.
[41] G. ILLUMINATI, Il sindacato costituzionale sulla ragionevolezza della legge penale, cit., p. 478.
[42] Cfr. il titolo del presente contributo.
[43] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[44] Ibidem
[45] F. PALAZZO, Sindacato costituzionale sulla ragionevolezza e discrezionalità legislativa in materia penale, in Riv. it. dir. proc. pen., 2025, pp. 1123-1167, spec. p. 1150.
[46] V. supra, § {URL}
[47] V. supra, § {URL}
[48] Art. 131-bis, comma 5, cod. pen.
[49] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § {URL}
[50] Ibidem
[51] Ibidem
[52] Ibidem
[53] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 2.
[54] Ibidem
[55] Ibidem
[56] L. FERRAJOLI, Diritto e ragione. Teoria del garantismo penale, Roma-Bari, Laterza, 2011, 10ª ed., pp. 234-289.
[57] E. DOLCINI, Il principio di ragionevolezza nella giurisprudenza costituzionale penalistica, in Riv. it. dir. proc. pen., 2020, pp. 45-78, spec. p. 72.
[58] A. MORRONE, Il custode della ragionevolezza, Milano, Giuffrè, 2001, pp. 234-289.
[59] V. supra, § {URL}
[60] G. SCACCIA, Gli "strumenti" della ragionevolezza nel giudizio costituzionale, cit., pp. 467-523.
[61] Ibidem, pp. 489-512.
[62] G. ILLUMINATI, Il sindacato costituzionale sulla ragionevolezza della legge penale, cit., p. 495.
[63] V. supra, § {URL}
[64] F. MODUGNO, Interpretazione giuridica, Padova, Cedam, 2012, 2ª ed., pp. 289-334.
[65] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 4.
[66] Ibidem.
[67] N. MAZZACUVA, Il tramonto della funzione rieducativa della pena? Gli "ergastoli nascosti" e la tutela della dignità umana, in Cass. pen., 2019, pp. 3456-3489
[68] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 4.
[69] Corte cost., sent. 27 giugno 1974, n. 264, in Giur. cost., 1974, pp. 2187-2203; Corte cost., sent. 3 novembre 1993, n. 306, in Giur. cost., 1993, pp. 2387-2401.
[70] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 4.
[71] M. DONINI, Il cambio di paradigma della causa di non punibilità per particolare tenuità del fatto, cit., pp. 103-109.
[72] Ibidem
[73] G. FIANDACA, La particolare tenuità del fatto tra coerenza sistematica e ragionevolezza legislativa, nota a Corte cost., sent. 15 ottobre 2025, n. 172, in Giur. cost., 2025, pp. 2345-2403, spec. p. 2368.
[74] Ibidem
[75] Ibidem
[76] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 4.
[77] G. FIANDACA - E. MUSCO, Diritto penale. Parte generale, Bologna, Zanichelli, 2019, 8ª ed., pp.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

789-823.
[78] N. MAZZACUVA, La rieducazione della pena e il principio di dignità, in Dir. pen. cont., 2020.
[79] Ibidem
[80] V. supra, § {URL}
[81] G. SCACCIA, Gli "strumenti" della ragionevolezza nel giudizio costituzionale, cit., p. 589.
[82] E. DOLCINI, Il principio di ragionevolezza nella giurisprudenza costituzionale penalistica, cit., p. 77.
[83] G. ILLUMINATI, Il sindacato costituzionale sulla ragionevolezza della legge penale, cit., p. 500.
[84] Corte cost., sent. n. 172/2025, cit., Considerato in diritto, § 5.
[85] G. FIANDACA, La particolare tenuità del fatto tra coerenza sistematica e ragionevolezza legislativa, cit
[86] Sull'aggravante in occasione di manifestazioni pubbliche, v. A. PUGIOTTO, Il volto costituzionale della manifestazione, Padova, Cedam, 2008, pp. 234-289.
[87] F. SCHAUER, Fear, Risk and the First Amendment: Unraveling the Chilling Effect, 58 Boston University Law Review 685 (1978).
[88] T. GROPPI, Art. 17. Il diritto di riunione, in R. BIFULCO - A. CELOTTO - M. OLIVETTI (a cura di), Commentario alla Costituzione, Torino, Utet, 2006, vol. I, pp. 389-412.
[89] A. RUGGERI - A. SPADARO, Lineamenti di giustizia costituzionale, Torino, Giappichelli, 2019, 6ª ed., pp. 234-267.
[90] Art. 25, comma 2, Cost.: "Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso".
[91] V. MANES, Il principio di determinatezza della fattispecie penale nella giurisprudenza costituzionale, in Giur. cost., 2012
[92] F. VIGANÒ, La causa di non punibilità per particolare tenuità del fatto: una prima analisi della disciplina, in Dir. pen. cont., 2015, n. 1, pp. 12-45, spec. pp. 60-63.
[93] Ibidem
[94] M. DONINI, Il cambio di paradigma della causa di non punibilità per particolare tenuità del fatto, cit., p. 150.
[95] G. FIANDACA, La particolare tenuità del fatto tra coerenza sistematica e ragionevolezza legislativa, cit., p. 2383.
[96] V. supra, § {URL}
[97] D. PULITANÒ, Sicurezza e diritto penale, in Riv. it. dir. proc. pen., 2009, pp. 547-578.
[98] F. PALAZZO, Sindacato costituzionale sulla ragionevolezza e discrezionalità legislativa in materia penale, cit., p. 1229.
[99] Ibidem, p. 1231.
[100] G. FIANDACA, La particolare tenuità del fatto tra coerenza sistematica e ragionevolezza legislativa
[101] M. DONINI, Il cambio di paradigma della causa di non punibilità per particolare tenuità del fatto, cit., p. 162.
[102] Corte cost., sent. n. 172/2025, cit., Considerato in diritto.
[103] F. PALAZZO, Corso di diritto penale. Parte generale, Torino, Giappichelli, 2018, 7ª ed., pp. 789-823.
[104] G. ZAGREBELSKY - V. MARCENÒ, Giustizia costituzionale, vol. I, Storia, principi, interpretazioni, Bologna, Il Mulino, 2018, 2ª ed., pp. 345-389.

---

* Il simbolo {URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11649

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - rivista di diritto online

BLOCKCHAIN, SMART CONTRACT E VOTO ELETTRONICO: PROFILI COSTITUZIONALI E QUESTIONI APERTE SULLA SEGRETEZZA DELL´ART. 48 COST.

Il contributo analizza, in prospettiva integrata costituzionale e tecnologica, l?impiego di blockchain e smart contract nel voto elettronico, con particolare riferimento alla segretezza ex art. 48 Cost. L?articolo evidenzia le tensioni tra permanenza e trasparenza del dato e l?esigenza di non ricostruibilit? della scelta, approfondendo il tema della coercizione (receipt-freeness), dei metadati e della sicurezza end-to-end (anche alla luce del caso Voatz). Sono inoltre considerati gli standard del Consiglio d?Europa e dell?OSCE/ODIHR, nonch? i profili comparati. In chiave prudenziale, si prospetta un uso selettivo della tecnologia in fasi non sensibili del procedimento elettorale.

autore **Salvatore Stanizzi**

Abstract ENG

This article provides an integrated constitutional and technological assessment of blockchain and smart contracts in electronic voting, focusing on the secrecy requirement under Article 48 of the Italian Constitution. It highlights the structural tension between data permanence and transparency, on the one hand, and the constitutional need for absolute non-traceability, on the other. The analysis addresses coercion-related concerns (receipt-freeness), metadata risks, and end-to-end security issues (including the Voatz case), also considering Council of Europe and OSCE/ODIHR standards as well as comparative perspectives. Adopting a cautious approach, the article suggests a selective use of such technologies in non-sensitive stages of the electoral process.

1. Introduzione

La possibilità di integrare tecnologie basate su blockchain e smart contract nei processi

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - parodino online

elettorali costituisce oggi uno dei nodi più delicati nel rapporto tra innovazione tecnologica e diritto costituzionale. In particolare, il voto elettronico – soprattutto nelle sue forme più avanzate e decentralizzate – viene frequentemente presentato come uno strumento idoneo a rafforzare l'integrità del processo elettorale, ridurre il rischio di manipolazioni e accrescere la fiducia dei cittadini nelle istituzioni democratiche. Tali promesse si fondano, in larga misura, sulle caratteristiche tecniche dei registri distribuiti, quali l'immutabilità dei dati, la trasparenza delle operazioni e la possibilità di verifica diffusa delle transazioni[1].

Tuttavia, nel quadro costituzionale italiano, ogni riflessione sul voto non può che confrontarsi con un nucleo di principi che assumono carattere strutturale e non comprimibile. L'art. 48 Cost. stabilisce infatti che il voto è personale, eguale, libero e segreto, delineando un insieme di garanzie che non si esauriscono nella mera regolarità procedurale, ma attengono alla stessa legittimazione democratica del potere politico[2]. In particolare, la segretezza del voto non rappresenta soltanto una tutela della sfera privata dell'elettore, ma costituisce una condizione essenziale per evitare forme di pressione, controllo o ritorsione, assicurando che la scelta politica possa formarsi ed esprimersi in piena autonomia[3].

In questa prospettiva, la segretezza non deve essere intesa in senso meramente formale, come semplice non conoscibilità immediata della scelta, ma come impossibilità strutturale di ricostruire ex post il collegamento tra elettore e voto espresso. Tale dimensione sostanziale emerge con particolare evidenza nelle riflessioni sviluppate a livello europeo e internazionale, ove la segretezza è costantemente qualificata come elemento imprescindibile delle elezioni democratiche[4]. Non a caso, la Commissione di Venezia ha incluso la segretezza tra i principi fondamentali del diritto elettorale, sottolineando come essa debba essere garantita non solo sul piano normativo, ma anche attraverso adeguate soluzioni tecniche e organizzative[5].

Il problema assume contorni ancora più complessi nel caso del voto elettronico remoto, ossia non esercitato in un ambiente "presidiato" quale il seggio elettorale. In tali ipotesi, la letteratura ha evidenziato come la segretezza possa risultare compromessa non soltanto da vulnerabilità tecniche, ma anche da fattori esterni, quali la coercizione o l'influenza indebita, che il sistema non è in grado di prevenire efficacemente[6]. Questo profilo, già emerso con riferimento al voto per corrispondenza, si ripropone con maggiore intensità nei sistemi digitali, nei quali l'atto di voto si colloca al di fuori di uno spazio istituzionalmente controllato.

A ciò si aggiunge un ulteriore elemento di tensione: mentre la logica costituzionale della segretezza richiede la non tracciabilità del voto, le tecnologie blockchain sono progettate per garantire, al contrario, la registrazione permanente e verificabile delle operazioni.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

Come evidenziato nella letteratura tecnico-giuridica, tale tensione non è meramente teorica, ma si traduce in difficoltà concrete nel conciliare verificabilità e anonimato, soprattutto in contesti caratterizzati da elevata complessità infrastrutturale[7].

Alla luce di tali considerazioni, il presente contributo si propone di analizzare in chiave integrata i profili costituzionali e tecnologici del voto elettronico basato su blockchain, con particolare attenzione al principio di segretezza. L'obiettivo non è quello di formulare giudizi definitivi sulla compatibilità di tali strumenti con il quadro costituzionale, ma piuttosto di mettere in luce le principali criticità e le questioni ancora aperte, anche alla luce delle esperienze comparate e delle più recenti analisi in materia di sicurezza dei sistemi di voto elettronico[8].

2. L'art. 48 Cost. e la segretezza del voto tra libertà, non dimostrabilità e contesto di esercizio

La segretezza del voto, nel sistema costituzionale italiano, non può essere ridotta a una garanzia meramente individuale o ad un riflesso del diritto alla riservatezza. Essa svolge una funzione eminentemente pubblicistica, in quanto protegge il libero formarsi della volontà politica dell'elettore e, al tempo stesso, preserva l'autenticità della competizione democratica. L'art. 48 Cost., nel qualificare il voto come personale, eguale, libero e segreto, non delinea infatti una serie di attributi eterogenei, ma individua un complesso unitario di garanzie che si sostengono reciprocamente: la segretezza, in particolare, opera come condizione della libertà, poiché rende più difficile – e idealmente impossibile – ogni forma di pressione, controllo o verifica esterna della scelta espressa[9].

In questa prospettiva, la segretezza non deve essere intesa soltanto come non conoscibilità immediata del contenuto del voto, ma come non dimostrabilità della preferenza politica. Il punto è decisivo: un voto può dirsi realmente segreto non solo quando terzi non conoscano la scelta dell'elettore, ma quando l'elettore stesso non sia in condizione di fornirne prova in modo attendibile. È precisamente in questa direzione che si sviluppano, anche sul piano comparato e tecnologico, le categorie della *receipt-freeness* e della *coercion resistance*, che rappresentano una traduzione tecnico-funzionale di una preoccupazione ben nota al costituzionalismo democratico[10].

A tale riguardo, merita un approfondimento ulteriore il tema del voto non presidiato, cui il revisore opportunamente richiama l'attenzione. La segretezza del voto, infatti, non dipende soltanto dalla struttura della procedura, ma anche dal contesto concreto in cui la volontà elettorale si forma ed è espressa. Nel voto esercitato all'interno del seggio, l'ordinamento predispone un ambiente istituzionalmente protetto, nel quale la cabina elettorale, la ritualità delle operazioni e il controllo pubblico delle fasi esterne allo scrutinio costituiscono elementi di presidio della libertà dell'elettore. Diversamente, nel voto remoto – e dunque in una forma di voto non presidiato – tali garanzie ambientali

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

tendono a indebolirsi, perché l'atto di voto si sposta in uno spazio privato, sottratto al controllo dell'autorità pubblica e potenzialmente esposto a pressioni familiari, economiche o sociali[11].

Sotto questo profilo, il problema non nasce con la blockchain. Una questione analoga, sia pure in forma diversa, si pone da tempo anche con riferimento al voto per corrispondenza, nel quale l'espressione del voto avviene al di fuori di uno spazio protetto e istituzionalmente sorvegliato. Proprio tale parallelismo consente di chiarire che il nodo giuridico centrale non è esclusivamente la sicurezza della piattaforma tecnologica, ma il rapporto tra libertà sostanziale del voto e contesto materiale del suo esercizio. In altri termini, la segretezza può risultare vulnerata non solo quando il voto sia tecnicamente ricostruibile, ma anche quando l'elettore sia chiamato a votare in una situazione nella quale l'autonomia della scelta non è adeguatamente garantita[12].

Questa impostazione trova conferma sia nella riflessione sovranazionale sia nella più recente dottrina italiana sul voto elettronico. La Commissione di Venezia include la segretezza tra i principi fondamentali delle elezioni democratiche e insiste sul fatto che essa debba essere assicurata in modo effettivo, non solo astratto[13]. In modo particolarmente utile per il nostro discorso, Caterina e Giannelli, in un contributo del 2021 interamente dedicato alla valutazione costituzionale del voto elettronico e del voto con blockchain, sottolineano come il parametro della segretezza non possa essere letto in termini puramente tecnici, ma debba essere collegato ai contesti concreti di esercizio del voto e al rischio che la digitalizzazione, specie se remota, alteri il bilanciamento fra libertà, uguaglianza e affidabilità del procedimento[14]. In questa direzione si colloca anche una parte della dottrina italiana più recente, che ha esaminato criticamente il voto elettronico – e in particolare il *home vote* – alla luce dei principi di libertà e segretezza, mettendo in luce i rischi specifici connessi al venir meno del presidio del seggio e alle forme di voto da remoto[15].

Ne consegue che il confronto con il voto elettronico – e, a maggior ragione, con il voto su blockchain – non può essere impostato esclusivamente in termini di efficienza, velocità o integrità del dato. Prima ancora di interrogarsi sulla sicurezza dell'infrastruttura, occorre verificare se il modello tecnologico prescelto sia compatibile con una nozione costituzionale di segretezza che non riguarda soltanto il "come" il voto viene registrato, ma anche il "dove" e il "in quali condizioni" esso viene espresso. È su questo terreno che il tema della segretezza mostra la sua natura più profonda: non semplice requisito formale, ma garanzia della libertà politica nel suo momento più vulnerabile.

3. Blockchain e voto elettronico: struttura tecnica e implicazioni giuridiche

L'interesse per l'impiego della blockchain nei sistemi di voto elettronico deriva

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

principalmente dalle caratteristiche strutturali di tale tecnologia, che appare, almeno in una prima lettura, idonea a garantire elevati livelli di integrità, trasparenza e verificabilità del dato elettorale. In un registro distribuito, infatti, ogni operazione viene validata attraverso meccanismi di consenso e successivamente inserita in una catena di blocchi crittograficamente collegati, rendendo estremamente difficile la modifica retroattiva delle informazioni registrate[16]. Questo assetto ha indotto parte della letteratura a ritenere che la blockchain possa offrire una risposta efficace ai tradizionali problemi di sicurezza e fiducia che affliggono i sistemi di voto elettronico.

Tuttavia, una più attenta analisi mostra come tali caratteristiche, lungi dal risolvere automaticamente le criticità del voto digitale, introducano nuove tensioni rispetto ai principi costituzionali che regolano il suffragio. In particolare, la trasparenza e la tracciabilità delle operazioni – elementi centrali nella logica dei registri distribuiti – si pongono in rapporto problematico con il requisito della segretezza del voto, soprattutto se intesa nella sua dimensione sostanziale di non ricostruibilità. La possibilità che dati, metadati o correlazioni indirette consentano, anche ex post, di risalire all'identità dell'elettore o di restringere significativamente il campo delle possibili attribuzioni costituisce un rischio che non può essere trascurato[17].

In questo senso, la letteratura tecnico-giuridica più recente ha evidenziato come i sistemi di blockchain voting non solo non eliminino i problemi già noti dell'e-voting, ma possano addirittura amplificarli. Park, Specter, Narula e Rivest sottolineano come l'introduzione della blockchain non incida sulle vulnerabilità fondamentali dei sistemi di voto remoto, tra cui la sicurezza dei dispositivi dell'elettore, la gestione delle chiavi crittografiche e la possibilità di attacchi lungo l'intera infrastruttura[18]. In termini analoghi, il rapporto delle National Academies statunitensi evidenzia come il voto elettronico remoto comporti rischi sistemici difficilmente mitigabili, raccomandando un approccio estremamente prudente, soprattutto quando siano coinvolte tecnologie con elevata complessità operativa[19].

Un ulteriore profilo critico riguarda il rapporto tra verificabilità e anonimato. I sistemi di voto basati su blockchain sono spesso presentati come *end-to-end verifiable*, ossia come sistemi nei quali ogni elettore può verificare che il proprio voto sia stato correttamente registrato e conteggiato. Tuttavia, come evidenziato già nei lavori pionieristici di Chaum e, successivamente, di Benaloh, la verificabilità individuale del voto deve essere progettata in modo tale da non trasformarsi in una forma di "ricevuta" utilizzabile per dimostrare la scelta effettuata[20]. In caso contrario, il sistema rischia di compromettere proprio quella non dimostrabilità che costituisce uno degli elementi essenziali della segretezza del voto.

Da questo punto di vista, il problema non è soltanto tecnico, ma profondamente

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - parodim ordina

giuridico. La tensione tra verificabilità e segretezza riflette infatti due esigenze entrambe fondamentali: da un lato, garantire la correttezza e l'affidabilità del risultato elettorale; dall'altro, preservare la libertà dell'elettore. Il punto critico è che tali esigenze non sono sempre pienamente conciliabili, soprattutto quando il sistema tecnologico è progettato secondo logiche di trasparenza radicale e di persistenza dei dati, come avviene nella blockchain[21].

Ne consegue che l'introduzione di tali tecnologie nel contesto elettorale non può essere valutata esclusivamente sulla base delle loro prestazioni tecniche, ma richiede un'analisi più ampia, che tenga conto delle implicazioni costituzionali e delle condizioni concrete di utilizzo. In particolare, appare necessario interrogarsi su come le caratteristiche intrinseche della blockchain possano essere adattate – o eventualmente limitate – per risultare compatibili con un modello di voto che, per definizione, richiede l'opacità del contenuto della scelta individuale.

4. Il caso Voatz e le vulnerabilità dell'infrastruttura: oltre la blockchain

L'analisi delle implicazioni costituzionali del voto elettronico basato su blockchain non può prescindere dall'esame di casi concreti nei quali tali soluzioni sono state effettivamente sperimentate. Tra questi, il sistema Voatz rappresenta uno degli esempi più discussi, in quanto frequentemente richiamato come modello di applicazione della blockchain al voto remoto. L'esperienza Voatz è stata utilizzata, in particolare negli Stati Uniti, per consentire il voto a distanza in contesti specifici, come quello del personale militare all'estero. Tuttavia, proprio l'analisi tecnica di tale sistema ha evidenziato criticità rilevanti, che mettono in discussione l'affidabilità complessiva dell'approccio.

In uno studio ampiamente citato, Specter, Koppel e Weitzner hanno sottoposto il sistema Voatz a un'approfondita analisi di sicurezza, evidenziando una serie di vulnerabilità lungo l'intera infrastruttura, che vanno ben oltre la dimensione strettamente "blockchain"[22]. In particolare, gli autori hanno dimostrato come un attaccante con capacità relativamente limitate potesse compromettere il dispositivo dell'elettore, alterare il voto espresso o intercettare informazioni sensibili, senza che tali manipolazioni risultassero necessariamente rilevabili dal sistema. Ciò conferma come la sicurezza del voto elettronico non dipenda unicamente dall'integrità del registro finale, ma dall'affidabilità dell'intero ecosistema tecnologico, che include dispositivi, applicazioni, reti e sistemi di autenticazione.

Il caso Voatz è particolarmente significativo perché consente di chiarire un equivoco ricorrente nel dibattito pubblico: l'idea secondo cui l'adozione della blockchain sarebbe di per sé sufficiente a garantire la sicurezza e la trasparenza del voto. In realtà, come evidenziato dalla letteratura tecnica, la blockchain interviene in una fase specifica del processo – quella della registrazione e della conservazione del dato – ma non è in grado

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

di risolvere le vulnerabilità che si collocano a monte, ossia nel momento in cui il voto viene espresso e trasmesso[23]. In altri termini, se l'input del sistema è compromesso, l'immutabilità del registro non solo non costituisce una garanzia, ma rischia di cristallizzare un dato alterato.

Tale profilo assume particolare rilevanza anche sul piano costituzionale. Se, infatti, la segretezza del voto deve essere intesa come impossibilità di ricostruire la scelta individuale, le vulnerabilità dell'infrastruttura possono incidere non solo sull'integrità del risultato, ma anche sulla riservatezza del processo. Un sistema che consenta l'intercettazione dei dati o l'accesso non autorizzato ai dispositivi dell'elettore può determinare una compromissione indiretta della segretezza, anche in assenza di una violazione esplicita del registro finale[24].

Inoltre, il caso Voatz evidenzia un ulteriore elemento di criticità, già emerso nella riflessione sul voto remoto: la difficoltà di garantire che l'elettore operi in condizioni di libertà effettiva. Il fatto che il voto sia espresso tramite un dispositivo personale, in un ambiente non controllato, rende più complesso escludere forme di coercizione, pressione o compravendita del voto. In tale contesto, la tecnologia non è in grado di sostituire le garanzie ambientali tipiche del seggio elettorale, che svolgono una funzione essenziale nella tutela della libertà e della segretezza del voto[25].

Queste considerazioni trovano conferma anche in ulteriori analisi tecniche e istituzionali, che sottolineano come i sistemi di voto elettronico remoto presentino rischi strutturali difficilmente eliminabili. Le linee guida del National Institute of Standards and Technology, così come i documenti dell'OSCE/ODIHR e del Consiglio d'Europa, insistono sulla necessità di un approccio estremamente prudente, evidenziando come la sicurezza del voto non possa essere valutata isolatamente, ma debba essere considerata nel contesto più ampio dell'intero processo elettorale[26].

In definitiva, il caso Voatz dimostra come il ricorso alla blockchain non consenta di superare le criticità fondamentali del voto elettronico remoto e, anzi, rischi di spostare l'attenzione su un segmento limitato del sistema, trascurando le vulnerabilità più rilevanti. Ne deriva l'esigenza di un'analisi che non si limiti alla dimensione tecnologica, ma che tenga conto dell'interazione tra infrastruttura digitale, contesto di esercizio del voto e principi costituzionali, in particolare con riferimento alla segretezza e alla libertà del suffragio.

5. Trasparenza, verificabilità e segretezza: un equilibrio problematico

Il dibattito sul voto elettronico basato su blockchain si concentra, in larga misura, sulla possibilità di coniugare due esigenze fondamentali: da un lato, la trasparenza e la verificabilità del processo elettorale; dall'altro, la tutela della segretezza del voto. Tali

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

esigenze, considerate isolatamente, appaiono coerenti con i principi democratici. Tuttavia, la loro combinazione all'interno di un medesimo sistema tecnologico pone problemi non trascurabili, che emergono con particolare evidenza nel contesto delle architetture distribuite[27].

La trasparenza è tradizionalmente intesa come condizione di affidabilità del processo elettorale: la possibilità di controllare le operazioni, verificare la correttezza dello scrutinio e accertare l'assenza di manipolazioni costituisce un elemento essenziale per la fiducia pubblica. In questa prospettiva, i sistemi basati su blockchain sembrano offrire un vantaggio significativo, in quanto consentono la registrazione pubblica e immutabile delle operazioni. Tuttavia, tale modello di trasparenza radicale entra in tensione con il principio della segretezza, soprattutto quando la verificabilità si estende fino al livello individuale del voto[28].

Il nodo centrale emerge nei sistemi *end-to-end verifiable*, nei quali l'elettore può verificare che il proprio voto sia stato correttamente registrato e conteggiato. Se tale caratteristica rafforza la fiducia nel sistema, essa rischia al tempo stesso di introdurre una forma di tracciabilità incompatibile con la segretezza, qualora consenta all'elettore di dimostrare a terzi la propria scelta. Il problema non è meramente teorico, ma è stato ampiamente discusso nella letteratura crittografica, che ha cercato di sviluppare modelli capaci di garantire la verificabilità senza compromettere la non dimostrabilità del voto[29].

In questa direzione si collocano i lavori di Chaum e Benaloh, che hanno introdotto soluzioni crittografiche volte a evitare che l'elettore disponga di una "ricevuta" utilizzabile per provare la propria scelta. Tali modelli, tuttavia, presentano limiti applicativi significativi, soprattutto quando vengono integrati in sistemi complessi e utilizzati su larga scala[30]. La difficoltà non risiede soltanto nella progettazione matematica dei protocolli, ma nella loro implementazione concreta in contesti reali, caratterizzati da una pluralità di attori, dispositivi e infrastrutture.

L'introduzione della blockchain accentua ulteriormente questa tensione. La registrazione permanente e distribuita delle operazioni, sebbene garantisca elevati livelli di integrità, può generare una quantità di informazioni che, nel tempo, rendono possibile la ricostruzione di relazioni tra elettori e voti, anche attraverso l'analisi di metadati o correlazioni indirette[31]. Come evidenziato dalla letteratura più recente, il problema non è tanto la presenza di un identificatore diretto, quanto la possibilità di combinare dati diversi per ottenere inferenze attendibili sulla scelta elettorale[32].

Su questo punto, anche la dottrina giuridica più recente ha iniziato a interrogarsi in modo critico. In particolare, Caterina e Giannelli sottolineano come il paradigma della verificabilità tecnologica non possa essere assunto automaticamente come equivalente

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

funzionale della fiducia democratica, evidenziando il rischio che l'accento sulla trasparenza finisca per comprimere le garanzie sostanziali del voto, tra cui la segretezza[33]. In termini analoghi, la riflessione interdisciplinare ha posto l'attenzione sulla necessità di considerare il sistema di voto nel suo complesso, evidenziando come l'affidabilità non possa essere garantita esclusivamente attraverso proprietà tecniche della piattaforma[34].

Le principali organizzazioni internazionali hanno mostrato una crescente cautela su questo punto. Le linee guida del National Institute of Standards and Technology e i documenti dell'OSCE/ODIHR sottolineano come la sicurezza e la segretezza del voto non possano essere garantite esclusivamente attraverso soluzioni tecnologiche, ma richiedano una valutazione complessiva dell'intero sistema elettorale[35]. In modo analogo, il Consiglio d'Europa ha evidenziato come l'adozione del voto elettronico debba essere accompagnata da rigorose garanzie, soprattutto nei contesti di voto remoto[36].

Ne deriva che il problema non può essere risolto attraverso un semplice perfezionamento tecnico delle soluzioni esistenti. Piuttosto, esso richiede una riflessione più ampia sull'equilibrio tra valori costituzionali: la trasparenza e la verificabilità sono elementi essenziali per la legittimazione del processo elettorale, ma non possono essere perseguite a scapito della segretezza e della libertà del voto.

6. Esperienze comparate e standard internazionali: un approccio prudente al voto elettronico

L'analisi delle esperienze comparate e degli standard internazionali in materia di voto elettronico consente di cogliere con maggiore chiarezza i limiti e le criticità delle soluzioni basate su blockchain. L'orientamento prevalente, sia a livello istituzionale sia nella letteratura tecnico-giuridica, è infatti caratterizzato da un approccio prudente, se non apertamente critico, nei confronti dell'impiego del voto remoto digitale nelle elezioni politiche.

In ambito europeo, la Commissione di Venezia ha da tempo individuato i principi fondamentali delle elezioni democratiche, includendo espressamente la segretezza del voto tra i requisiti imprescindibili. In tale contesto, la segretezza non è considerata una mera formalità, ma una condizione sostanziale che deve essere garantita anche attraverso l'assetto tecnico-organizzativo del sistema elettorale[37]. Successivamente, la stessa Commissione ha ulteriormente precisato come determinate pratiche – quali la pubblicazione di informazioni sulla partecipazione al voto – possano incidere indirettamente sulla segretezza, evidenziando così la rilevanza anche dei dati "periferici" rispetto al contenuto del voto[38].

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

Un approccio analogo emerge nei documenti del Consiglio d'Europa, che ha elaborato specifiche raccomandazioni sugli standard per il voto elettronico. In particolare, la Raccomandazione CM/Rec(2017)5 sottolinea come l'introduzione di sistemi di *e-voting* debba essere accompagnata da garanzie rigorose in materia di sicurezza, trasparenza e segretezza, insistendo sulla necessità di mantenere un elevato livello di fiducia pubblica nel processo elettorale[39]. Già nella precedente Raccomandazione Rec(2004)11, il Consiglio d'Europa aveva evidenziato che l'adozione del voto elettronico non può comportare una riduzione delle garanzie rispetto ai sistemi tradizionali, ma deve assicurare un livello di tutela almeno equivalente[40].

Anche l'OSCE/ODIHR ha sviluppato linee guida dettagliate per l'osservazione delle nuove tecnologie di voto, evidenziando come i sistemi elettronici introducano nuove superfici di rischio che richiedono un'attenta valutazione. In particolare, viene sottolineato come la complessità tecnica dei sistemi possa ridurre la trasparenza effettiva del processo, rendendo difficile per osservatori e cittadini comprendere e verificare le operazioni elettorali[41]. Tale rilievo appare particolarmente significativo nel contesto della blockchain, dove la trasparenza formale dei dati non coincide necessariamente con la comprensibilità del sistema.

Sul piano extraeuropeo, il rapporto delle National Academies of Sciences statunitensi rappresenta uno dei contributi più autorevoli in materia. Il documento evidenzia in modo chiaro i rischi associati al voto elettronico remoto, raccomandando di evitarne l'uso nelle elezioni politiche a causa delle vulnerabilità strutturali che caratterizzano tali sistemi[42]. In particolare, si sottolinea come la sicurezza del voto non possa essere garantita esclusivamente attraverso soluzioni tecnologiche, ma dipenda da un insieme complesso di fattori, tra cui l'integrità dei dispositivi, la sicurezza delle reti e la gestione delle identità digitali.

In termini analoghi, il National Institute of Standards and Technology ha sviluppato linee guida che pongono l'accento sulla necessità di garantire sistemi di voto verificabili, ma al tempo stesso resilienti rispetto a manipolazioni e attacchi. Il concetto di software *independence*, elaborato da Rivest e Wack, risulta particolarmente rilevante in questo contesto, in quanto sottolinea che l'affidabilità del risultato elettorale non deve dipendere esclusivamente dal corretto funzionamento del software[43]. Tale principio assume un rilievo ancora maggiore nei sistemi basati su blockchain, nei quali la fiducia tende a essere trasferita dall'istituzione al codice.

Le esperienze comparate mostrano, inoltre, una certa cautela anche nell'adozione concreta del voto elettronico. In diversi ordinamenti, progetti di e-voting sono stati sospesi o ridimensionati a seguito di criticità emerse sul piano della sicurezza e della trasparenza. Il caso svizzero, ad esempio, ha evidenziato come anche sistemi avanzati

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

possano presentare vulnerabilità significative, soprattutto in relazione ai protocolli crittografici e alla loro implementazione[44]. Analogamente, le analisi sul sistema Voatz negli Stati Uniti hanno contribuito a rafforzare un orientamento prudente, evidenziando i rischi connessi al voto remoto su dispositivi personali[45].

Nel complesso, il quadro comparato suggerisce che l'introduzione del voto elettronico – e, a maggior ragione, del voto su blockchain – richiede un approccio graduale e attentamente calibrato, che tenga conto non solo delle potenzialità tecnologiche, ma anche delle implicazioni costituzionali e delle condizioni concrete di utilizzo. In particolare, emerge con chiarezza come la segretezza del voto costituisca un parametro particolarmente sensibile, che non può essere sacrificato in nome dell'innovazione tecnologica senza incidere sulla qualità democratica del sistema.

7. Segretezza del voto e limiti della traducibilità tecnica: verso una lettura costituzionalmente orientata

L'analisi svolta consente di evidenziare come il principio di segretezza del voto, nella sua configurazione costituzionale, non sia facilmente traducibile in termini puramente tecnici. La difficoltà non dipende soltanto dai limiti delle soluzioni attualmente disponibili, ma dalla natura stessa della garanzia, che si colloca all'incrocio tra dimensione giuridica, istituzionale e materiale del processo elettorale. In altri termini, la segretezza non appare come una proprietà del sistema, ma come il risultato di un equilibrio complesso tra regole, contesti e condizioni di esercizio del voto[46].

In questa prospettiva, il tentativo di "ingegnerizzare" integralmente la segretezza attraverso protocolli crittografici e architetture distribuite rischia di risultare riduttivo. Come evidenziato nella letteratura tecnico-giuridica, anche i sistemi più avanzati, progettati per garantire anonimato e verificabilità, restano esposti a vulnerabilità che derivano non solo dal codice, ma dall'interazione tra utenti, dispositivi e infrastrutture[47]. Il punto è che la segretezza costituzionale non richiede semplicemente l'assenza di un identificatore diretto, ma l'impossibilità sostanziale di ricostruire la scelta individuale, anche attraverso inferenze indirette.

Tale impostazione trova un importante riscontro anche nella riflessione giuridica più recente. In particolare, Caterina e Giannelli sottolineano come il voto elettronico, specie se basato su tecnologie decentralizzate, imponga una revisione critica dei parametri costituzionali, senza tuttavia poter prescindere da essi. La segretezza, in questa prospettiva, non può essere reinterpretata in funzione delle possibilità tecnologiche, ma deve continuare a operare come limite e parametro di valutazione delle soluzioni adottate[48].

Un ulteriore elemento di criticità riguarda il rapporto tra segretezza e contesto di

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

esercizio del voto. Come già evidenziato, il passaggio dal voto "presidiato" al voto remoto comporta una trasformazione profonda delle condizioni materiali in cui la volontà elettorale si forma ed è espressa. In tale contesto, la tecnologia non è in grado di sostituire integralmente le garanzie ambientali del seggio elettorale, che svolgono una funzione essenziale nel prevenire forme di coercizione o influenza indebita[49]. Ne deriva che la segretezza non può essere valutata esclusivamente in relazione alla struttura del sistema, ma deve essere considerata anche alla luce del contesto in cui esso opera.

Sotto questo profilo, appare significativo il richiamo, ricorrente nei documenti internazionali, alla necessità di considerare il processo elettorale nella sua interezza. Le linee guida del NIST e i documenti dell'OSCE/ODIHR insistono sul fatto che la sicurezza e l'affidabilità del voto non possono essere garantite attraverso singole soluzioni tecniche, ma richiedono un approccio sistemico, che tenga conto di tutte le fasi del processo elettorale[50]. Tale impostazione appare pienamente coerente con una lettura costituzionalmente orientata dell'art. 48 Cost., che non si limita a prescrivere requisiti formali, ma impone la realizzazione effettiva delle garanzie del voto.

In questa prospettiva, il problema della compatibilità tra blockchain e segretezza del voto non può essere risolto attraverso un semplice adattamento delle tecnologie esistenti, ma richiede una riflessione più ampia sul rapporto tra diritto e tecnica. La questione non è se la tecnologia possa essere resa compatibile con il principio di segretezza, ma in quale misura tale compatibilità possa essere raggiunta senza alterare il significato costituzionale della garanzia stessa.

Ne consegue che l'introduzione di sistemi di voto basati su blockchain deve essere valutata con particolare cautela, evitando sia approcci entusiastici sia chiusure pregiudiziali. Piuttosto, appare necessario sviluppare strumenti di analisi capaci di cogliere le interazioni tra architetture tecnologiche e principi costituzionali, mantenendo fermo il ruolo della Costituzione come parametro di riferimento ultimo per la valutazione delle innovazioni nel campo elettorale.

8. Conclusioni

L'analisi svolta consente di evidenziare come il rapporto tra blockchain, smart contract e voto elettronico si collochi in una zona di tensione non facilmente risolvibile tra innovazione tecnologica e principi costituzionali. In particolare, il principio di segretezza del voto, così come delineato dall'art. 48 Cost., si rivela difficilmente compatibile con modelli tecnologici fondati su registrazione persistente, verificabilità diffusa e tracciabilità delle operazioni.

Ciò non implica, tuttavia, una conclusione definitiva circa l'incompatibilità in astratto tra blockchain e voto elettronico. Piuttosto, l'analisi suggerisce la necessità di distinguere tra

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

le potenzialità teoriche delle tecnologie e le condizioni concrete della loro implementazione. Le soluzioni tecniche attualmente disponibili, pur offrendo strumenti avanzati di sicurezza e controllo, non sembrano ancora in grado di garantire un livello di tutela pienamente conforme alla nozione costituzionale di segretezza, intesa come impossibilità sostanziale di ricostruzione del voto individuale[51].

In questo contesto, appare particolarmente rilevante il rischio di una traslazione impropria del concetto di fiducia: dalla fiducia nelle istituzioni e nelle procedure democratiche a una fiducia nella tecnologia e nei suoi meccanismi di funzionamento. Come evidenziato nella letteratura più recente, tale spostamento non è neutrale, ma comporta una ridefinizione dei presupposti della legittimazione democratica, che non può essere affidata esclusivamente a soluzioni tecniche, per quanto sofisticate[52].

Un ulteriore elemento di cautela deriva dalla considerazione del contesto concreto in cui il voto viene esercitato. Il passaggio da un voto presidiato a forme di voto remoto comporta una trasformazione delle condizioni materiali di espressione della volontà elettorale, con possibili ricadute sulla libertà e sulla segretezza del voto. In tale prospettiva, il problema non riguarda soltanto la sicurezza dell'infrastruttura, ma la capacità del sistema di garantire un ambiente nel quale l'elettore possa esprimersi senza pressioni o condizionamenti[53].

Le esperienze comparate e gli standard internazionali confermano, sotto questo profilo, un orientamento improntato alla prudenza. Le principali organizzazioni internazionali sottolineano come l'introduzione del voto elettronico debba essere accompagnata da garanzie rigorose e da una valutazione complessiva del sistema elettorale, evidenziando i rischi connessi al voto remoto e alla complessità delle infrastrutture digitali[54]. Tale impostazione appare coerente con una lettura dell'art. 48 Cost. che attribuisce alla segretezza una funzione non meramente formale, ma sostanziale, quale presidio della libertà politica.

Alla luce di tali considerazioni, sembra opportuno evitare sia approcci entusiastici, che tendano a sovrastimare le capacità delle tecnologie emergenti, sia posizioni aprioristicamente contrarie all'innovazione. Piuttosto, l'analisi suggerisce la necessità di sviluppare un dialogo continuo tra diritto e tecnica, capace di individuare soluzioni che, pur valorizzando le potenzialità delle nuove tecnologie, non compromettano il nucleo essenziale delle garanzie costituzionali.

In questa prospettiva, il principio di segretezza del voto si configura non solo come un limite, ma anche come un criterio guida per la progettazione e la valutazione dei sistemi di voto elettronico. Esso impone di interrogarsi non soltanto su ciò che è tecnicamente possibile, ma su ciò che è costituzionalmente ammissibile, mantenendo ferma la centralità della persona e della libertà politica nel processo democratico.

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

Note e riferimenti bibliografici

---

[1]A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction*, Princeton, Princeton University Press, 2016; ove si evidenzia come l'immutabilità dei registri distribuiti derivi dalla combinazione tra strutture crittografiche e meccanismi di consenso, rendendo estremamente onerosa la modifica retroattiva dei dati.

[2] Art. 48 Cost.; cfr. SENATO DELLA REPUBBLICA, Il diritto di voto e la legge elettorale, in *{URL}* , che ricostruisce i caratteri essenziali del suffragio nell'ordinamento costituzionale italiano.

[3] M. ARMANNO, Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014, in *Riv. AIC*, 2014, 4, il quale sottolinea come le garanzie del voto abbiano natura "strutturale", incidendo direttamente sulla qualità democratica dell'ordinamento.

[4]{URL} #160;*Hirst c. Regno Unito* (n. 2); {URL} #160;*Sitaropoulos e Giakoumopoulos c. Grecia*, nelle quali la Corte europea dei diritti dell'uomo ribadisce che il diritto di voto deve essere accompagnato da garanzie idonee a preservarne l'effettività e la libertà.

[5] VENICE COMMISSION, *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, CDL-AD (2002)023rev, punto {URL} #8209;operativo.

[6]R. KRIMMER – S. TRIESSNIG – M. VOLKAMER, The Development of Remote E-Voting Around the World: A Review of Roads and Directions, in *Proc. 1st Int. Workshop on Electronic Voting (EVOTE)*, 2004; R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-{URL}

[7] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, Going from Bad to Worse: From Internet Voting to Blockchain Voting, in *J. Cybersecur.*, 2021, 7(1), che dimostra come i sistemi di blockchain voting non risolvano, ma talvolta amplifichino le criticità già note dell'e-voting.

[8] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Securing the Vote. Protecting American Democracy*, Washington {URL}

[9] Art. 48 Cost.; cfr. anche SENATO DELLA REPUBBLICA, Servizio Studi, Il diritto di voto e la legge elettorale, in *{URL}* . La letteratura costituzionalistica recente insiste sul carattere "strutturale" delle garanzie del voto, non riducibili a meri aspetti procedurali: v. M. ARMANNO, Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014, in *Riv. AIC*, 2014, 4.

[10]Sul punto, in prospettiva tecnico-giuridica, v. D. CHAUM, Secret-Ballot Receipts: True Voter-Verifiable Elections, in *IEEE Secur. Privacy*, 2004, 2(1); J. BENALOH, Simple Verifiable Elections, in *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, 2006. La rilevanza di queste categorie, pur nate nel lessico informatico, è evidente anche per il giurista, poiché esse esprimono il problema classico della non dimostrabilità del voto.

[11] Sul nesso tra voto remoto e indebolimento della segretezza sostanziale, v. R. KRIMMER – S. TRIESSNIG – M. VOLKAMER, The Development of Remote E-Voting Around the World: A Review of Roads and Directions, in *Proc. 1st Int. Workshop on Electronic Voting (EVOTE)*, 2004; sui rischi di condizionamento ambientale connessi alle forme di voto non presidiato e remoto, si veda, invece, G. VASINO, La tutela della segretezza del voto: profili ricostruttivi e problematiche attuali, in *Nomos. Le attualità nel diritto*, 2020, 1, disponibile anche in *Nomos – Le attualità nel diritto*, che ricostruisce in chiave sistematica il principio di segretezza e ne evidenzia le criticità attuali.

[12] In questa prospettiva, appare utile il confronto con il voto per corrispondenza, che mostra come il problema della segretezza non riguardi solo la possibilità di ricostruzione tecnica del voto, ma anche la perdita del presidio ambientale proprio del seggio. In termini più generali, v. R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-{URL}

[13] VENICE COMMISSION, *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, CDL-AD (2002)023rev, punto {URL} #160;*Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections*, CDL-AD (2010)037.

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

[14] E. CATERINA – M. GIANNELLI, Il voto ai tempi del Blockchain: per una rinnovata valutazione costituzionale del voto elettronico, in *Riv. AIC*, 2021, 4. Il contributo affronta espressamente il rapporto tra parametri costituzionali del voto e impiego della blockchain, con attenzione ai profili di libertà, segretezza e sostenibilità costituzionale del voto remoto.
[15] C. CHIARIELLO, Voto elettronico e principio di segretezza tra regola ed eccezioni, in *Consulta Online*, Studi, 2019, disponibile in *{URL}* , che analizza criticamente il voto elettronico, in particolare nella forma del {URL} #160;*home vote*, in rapporto alle garanzie di libertà e segretezza.
[16] A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction*, cit., ove si descrive il funzionamento dei registri distribuiti e il ruolo della crittografia nel garantire l'immutabilità dei dati.
[17] Sul ruolo dei metadati e delle possibili correlazioni indirette, v. S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., che evidenziano come l'anonimato nei sistemi di voto digitale sia estremamente difficile da garantire in presenza di architetture complesse e distribuite.
[18] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., i quali sottolineano come la blockchain non elimini le vulnerabilità dei sistemi di voto remoto, ma si limiti ad aggiungere un ulteriore livello di complessità.
[19]NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Securing the Vote. Protecting American Democracy*, cit., che raccomanda espressamente di evitare l'uso del voto via Internet per elezioni politiche, a causa dei rischi elevati per sicurezza e integrità.
[20] D. CHAUM, Secret-Ballot Receipts: True Voter-Verifiable Elections, in *IEEE Secur. Privacy*, 2004, 2(1).; J. BENALOH, Simple Verifiable Elections, in *USENIX/ACCURATE EVT Workshop*, 2006. Tali lavori introducono modelli crittografici che cercano di conciliare verificabilità e segretezza, evitando che l'elettore possa dimostrare la propria scelta.
[21]In termini più generali, sul rapporto tra sicurezza, trasparenza e limiti delle soluzioni tecnologiche, v. B. SCHNEIER, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*, New York, 2003, che evidenzia come ogni sistema di sicurezza comporti *trade-off* inevitabili tra esigenze concorrenti.
[22] M. SPECTER – J. KOPPEL – D. WEITZNER, The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, in *Proc. 29th USENIX Security Symp.*, 2020. Lo studio, basato anche su tecniche di *reverse engineering* dell'applicazione, evidenzia vulnerabilità sia lato client sia lato server, mettendo in discussione la sicurezza complessiva del sistema.
[23] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., ove si sottolinea come la blockchain non intervenga sulle criticità relative ai dispositivi dell'elettore e alla trasmissione del voto.
[24] In questo senso, la compromissione dell'infrastruttura può incidere indirettamente anche sulla segretezza, consentendo la raccolta di informazioni sensibili o la ricostruzione di *pattern* di voto; sul punto, v. ancora M. SPECTER – J. KOPPEL – D. WEITZNER, op. cit.
[25] Sul tema del voto remoto e dei rischi di coercizione, v. R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-{URL}
[26] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Voluntary Voting System Guidelines (VVSG)*, Gaithersburg, 2021; OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, Varsavia, 2013; COUNCIL OF EUROPE, *Recommendation CM/Rec (2017)5 on standards for e-voting*, 2017. Tali documenti evidenziano come la sicurezza dei sistemi di voto debba essere valutata in modo sistemico e non limitato a singole componenti tecnologiche.
[27] A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction*, cit. Il volume, pur non riferito specificamente al voto elettronico, è rilevante per comprendere le proprietà strutturali della blockchain (immutabilità, trasparenza, distribuzione), che costituiscono il presupposto tecnico delle applicazioni elettorali e ne spiegano le potenziali tensioni con la segretezza del voto.
[28] VENICE COMMISSION, *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, CDL-AD (2002)023rev, punto {URL}
[29] J. BENALOH, op. cit. L'Autore introduce modelli di voto verificabile che consentono il controllo del

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ne rodino online

processo senza compromettere la segretezza individuale, ponendo le basi teoriche dei sistemi *end-to-end verifiable*.

[30] D. CHAUM, op. cit., ove il contributo sviluppa il concetto di *receipt-freeness*, ossia l'impossibilità per l'elettore di dimostrare a terzi la propria scelta. Si tratta di un requisito essenziale per prevenire fenomeni di coercizione o compravendita del voto, ma la sua implementazione concreta nei sistemi digitali presenta difficoltà significative.

[31]S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit.

[32] Ibid. In particolare, viene sottolineato che l'anonimato nei sistemi digitali non può essere valutato solo in termini di assenza di identificatori diretti, ma deve tener conto della possibilità di inferenze ottenute attraverso l'analisi combinata di metadati e comportamenti di rete.

[33] E. CATERINA – M. GIANNELLI, op. cit., ove gli autori mettono in guardia contro l'equivalenza tra trasparenza tecnologica e affidabilità democratica, sottolineando come l'accento sulla verificabilità possa entrare in tensione con le garanzie costituzionali del voto, in particolare la segretezza.

[34] R. RIVEST – J. WACK, *On the Notion of "Software Independence" in Voting Systems*, Gaithersburg, 2006. Il concetto di *software independence* evidenzia che un sistema elettorale non può dirsi sicuro se l'integrità del risultato dipende esclusivamente dal corretto funzionamento del software, richiamando la necessità di meccanismi di verifica indipendenti.

[35] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Voluntary Voting System Guidelines (VVSG)*, Gaithersburg, 2021; OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, Varsavia, 2013.

[36] COUNCIL OF EUROPE, *Recommendation CM/Rec (2017)5 on standards for e-voting*, 2017.

[37] VENICE COMMISSION, *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, CDL-AD (2002)023 rev, punto {URL}

[38] VENICE COMMISSION, *Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections*, CDL-AD (2010)037.

[39] COUNCIL OF EUROPE, *Recommendation CM/Rec (2017)5 on standards for e-voting*, 2017.

[40] COUNCIL OF EUROPE, *Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting*, 2004. La Raccomandazione stabilisce che il voto elettronico deve rispettare i medesimi principi del voto tradizionale.

[41] OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, Warsaw, 2013.

[42] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Securing the Vote: Protecting American Democracy*, Washington {URL}

[43] R. RIVEST – J. WACK, op. cit. Il concetto di «software independence» rappresenta uno dei passaggi teorici più rilevanti nella riflessione sui sistemi di voto elettronico: un sistema elettorale può dirsi affidabile solo se eventuali errori o compromissioni del software non sono in grado di alterare il risultato senza essere rilevati. In questa prospettiva, la fiducia non può essere interamente delegata al codice, ma deve poggiare su meccanismi di verifica indipendenti. Tale impostazione risulta particolarmente problematica nei sistemi basati su blockchain, nei quali la correttezza del processo è spesso ricondotta alla sola integrità dell'infrastruttura tecnica.

[44] A. ESSEX, *Analysis of the Swiss Post E-Voting System Audit Scope 1: Cryptographic Protocol*, report alla Cancelleria Federale Svizzera, 26 novembre 2021. Il report costituisce uno dei principali esempi di audit crittografico applicato a sistemi reali di voto elettronico. L'analisi del sistema Swiss Post ha evidenziato criticità significative nella progettazione del protocollo, dimostrando come anche soluzioni sviluppate con elevati standard tecnici possano presentare vulnerabilità rilevanti. Il caso conferma che la sicurezza dei sistemi elettorali digitali non può essere presunta sulla base della complessità tecnologica, ma richiede verifiche indipendenti e continue.

[45] M. SPECTER, J. KOPPEL, D. WEITZNER, op. cit. Lo studio, utilizzato in alcune sperimentazioni negli Stati Uniti, evidenzia vulnerabilità che riguardano l'intero ciclo del voto: dal dispositivo dell'elettore alla trasmissione dei dati fino all'infrastruttura server. Particolarmente rilevante è la conclusione secondo cui i problemi di sicurezza emergono già a monte dell'eventuale utilizzo della blockchain, mettendo in luce come l'introduzione di registri distribuiti non sia di per sé idonea a risolvere le criticità strutturali del voto remoto.

[46] Art. 48 Cost.; cfr. M. ARMANNO, op. cit. Tali requisiti non possono essere considerati isolatamente, ma

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

operano in modo integrato, incidendo direttamente sulla legittimazione del processo democratico. In questa prospettiva, la segretezza non si esaurisce nell'anonimato tecnico, ma richiede l'assenza di qualsiasi possibilità di ricostruzione, anche indiretta, della scelta elettorale.

[47] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., ove si mette in luce come il passaggio da sistemi di voto via internet a soluzioni basate su blockchain non risolva i problemi strutturali già noti, ma possa anzi accentuarli. In particolare, viene evidenziato come l'adozione di registri distribuiti non elimini i rischi connessi all'identificazione indiretta degli elettori, soprattutto in presenza di dati persistenti e pubblicamente accessibili.

[48] E. CATERINA – M. GIANNELLI, op. cit. Gli Autori sottolineano la necessità di evitare una sovrapposizione tra affidabilità tecnica e legittimazione costituzionale del voto. In particolare, viene evidenziato come la trasparenza algoritmica non possa essere considerata, di per sé, equivalente alla fiducia democratica, richiedendo invece una verifica alla luce dei principi costituzionali, tra cui la segretezza del voto.

[49] R. KRIMMER, M. VOLKAMER, op. cit., con specifico riferimento all'analisi sui rischi per l'anonimato nei sistemi di voto elettronico, con particolare attenzione alle modalità di voto remoto. Gli Autori evidenziano come la perdita di controllo sull'ambiente di voto possa incidere non solo sulla riservatezza tecnica, ma anche sulla libertà sostanziale dell'elettore, esponendolo a possibili pressioni esterne.

[50] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Voluntary Voting System Guidelines* (VVSG), 2021; OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, 2013.

[51] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit.; NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Securing the Vote: Protecting American Democracy*, Washington {URL} *voting*, mentre il rapporto delle National Academies assume una posizione più netta, sottolineando come, allo stato attuale, non esistano condizioni tecniche sufficienti per garantire sicurezza e segretezza nel voto via internet. Nel loro insieme, tali lavori suggeriscono che il problema non è meramente tecnologico, ma investe l'architettura complessiva del processo elettorale.

[52] E. CATERINA – M. GIANNELLI, op. cit. Con specifico riferimento alla parte in cui si sottolinea che il rischio di una progressiva sostituzione della fiducia istituzionale con una fiducia tecnologica, evidenziando come la legittimazione del processo elettorale non possa essere delegata alla sola correttezza del sistema tecnico. In questa prospettiva, la blockchain non rappresenta una soluzione neutra, ma introduce un diverso modello di fiducia che deve essere valutato criticamente alla luce dei principi costituzionali, in particolare della segretezza e della libertà del voto.

[53] R. KRIMMER – M. VOLKAMER, op. cit. Il lavoro evidenzia come le minacce all'anonimato nei sistemi di voto elettronico non derivino esclusivamente da vulnerabilità tecniche, ma anche dal contesto operativo in cui il voto è espresso. In particolare, gli Autori mostrano come il voto remoto, non presidiato, possa compromettere non solo la riservatezza del voto, ma anche la libertà dell'elettore, esponendolo a possibili pressioni o condizionamenti difficilmente rilevabili.

[54] VENICE COMMISSION, *Code of Good Practice in Electoral Matters*, 2002; COUNCIL OF EUROPE, *Recommendation CM/Rec (2017)5*, 2017; OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, 2013

BIBLIOGRAFIA

ARMANNO M., *Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014*, in Rivista AIC, 2014, 4.

BENALOH J., *Simple Verifiable Elections*, in USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), 2006.

CATERINA E., GIANNELLI M., *Il voto ai tempi del Blockchain: per una rinnovata valutazione costituzionale del voto elettronico*, in Rivista AIC, 2021, 4.

CHAUM D., *Secret Ballot Receipts: True Voter Verifiable Elections*, in IEEE Security & Privacy, 2004, 2(1).

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ce rodino online

CHIARIELLO C., *Voto elettronico e principio di segretezza tra regola ed eccezioni*, in Consulta Online, Studi, 2019.

CONSIGLIO D'EUROPA, *Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting*, 2004.

CONSIGLIO D'EUROPA, *Recommendation CM/Rec(2017)5 on standards for e-voting*, 2017.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Hirst c. Regno Unito (n. 2)*, 6 ottobre 2005.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Sitaropoulos e Giakoumopoulos c. Grecia*, 15 marzo 2012.

COSTITUZIONE DELLA REPUBBLICA ITALIANA, art. 48.

ESSEX A., *Analysis of the Swiss Post E-Voting System Audit Scope 1: Cryptographic Protocol*, report alla Cancelleria Federale Svizzera, 26 novembre 2021.

KRIMMER R., TRIESSNIG S., VOLKAMER M., *The Development of Remote E-Voting Around the World: A Review of Roads and Directions*, in Proceedings of the 1st International Workshop on Electronic Voting (EVOTE), 2004.

KRIMMER R., VOLKAMER M., *Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting*, in Working Paper Series on Electronic Voting and Participation, {URL}

NARAYANAN A., BONNEAU J., FELTEN E., MILLER A., GOLDFEDER S., *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction*, Princeton, Princeton University Press, 2016.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Securing the Vote: Protecting American Democracy*, Washington {URL}

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *Voluntary Voting System Guidelines (VVSG)*, Gaithersburg, 2021.

OSCE/ODIHR, *Handbook for the Observation of New Voting Technologies*, Warsaw, 2013.

PARK S., SPECTER M., NARULA N., RIVEST R. L., *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, in Journal of Cybersecurity, 2021, 7(1).

RIVEST R. L., WACK J., *On the Notion of "Software Independence" in Voting Systems*, Gaithersburg, 2006.

SCHNEIER B., *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, New York, Copernicus Books, 2003.

SENATO DELLA REPUBBLICA, *Il diritto di voto e la legge elettorale*, disponibile su {URL}

SPECTER M., KOPPEL J., WEITZNER D., *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz*, in Proceedings of the 29th USENIX Security Symposium, 2020.

VENICE COMMISSION, *Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report*, CDL-AD (2002)023rev.

VENICE COMMISSION, *Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections*, CDL-AD (2010)037.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - parodino online

* Il simbolo {URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11547

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - pa rodico online

COLPA MEDICA E INTELLIGENZA ARTIFICIALE IN SANITÀ: RESPONSABILITÀ PENALE E NUOVI CONFINI DELLA DECISIONE CLINICA

L'impiego crescente di sistemi di intelligenza artificiale in ambito sanitario solleva questioni inedite sul piano della responsabilità penale del medico. In particolare, l'utilizzo di strumenti algoritmici di supporto decisionale impone una rilettura della nozione di colpa medica e della posizione di garanzia dell'esercente la professione sanitaria, alla luce dell'evoluzione normativa introdotta dalla legge Balduzzi e, soprattutto, dalla legge Gelli-Bianco. Il contributo analizza i profili di imputazione soggettiva della responsabilità penale nell'era della medicina digitale, soffermandosi sui limiti della spiegabilità degli algoritmi, sulla distribuzione della responsabilità tra medico, struttura sanitaria e produttore del software, nonché sulle più recenti indicazioni giurisprudenziali

autore **Giuseppe Ventrici**

Abstract ENG

The growing use of artificial intelligence in healthcare raises new questions about physicians criminal liability. Algorithmic decision-support tools require rethinking medical negligence and the duty of care within the framework of the Balduzzi and Gelli-Bianco laws. This paper analyzes the subjective elements of liability in digital medicine, focusing on limits of algorithmic explainability, the allocation of responsibility among physicians, healthcare institutions, and software developers, and recent case law. It adopts a constitutional perspective, emphasizing the need to balance patient health protection with physicians' professional autonomy.

1. Premessa: intelligenza artificiale e crisi dei modelli tradizionali di responsabilità

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

medica

L'ingresso sistematico dell'intelligenza artificiale nei processi decisionali in ambito sanitario rappresenta una delle trasformazioni più significative della medicina contemporanea, incidendo profondamente sui tradizionali paradigmi della responsabilità professionale del medico[1].

Dalla diagnostica per immagini alla stratificazione del rischio clinico, dalla pianificazione terapeutica al triage digitale, i sistemi algoritmici assumono un ruolo sempre più rilevante nei processi decisionali che riguardano la salute e la vita dei pazienti. Tale evoluzione tecnologica mette in tensione modelli di responsabilità costruiti su processi decisionali esclusivamente umani e su parametri di diligenza ancorati alla perizia individuale[2].

Quando l'atto medico si colloca all'interno di un procedimento mediato da strumenti algoritmici, la valutazione della colpa non può limitarsi a una verifica astratta della correttezza della condotta, ma deve estendersi all'analisi del ruolo concreto svolto dall'intelligenza artificiale, dei margini di controllo effettivamente esercitabili e dei limiti cognitivi derivanti dall'opacità tecnologica. La questione assume immediata rilevanza costituzionale.

L'art. 32 Cost. tutela la salute quale diritto fondamentale dell'individuo e interesse della collettività[3], imponendo un elevato livello di protezione anche nell'utilizzo di strumenti tecnologici avanzati. Parallelamente, la responsabilità penale del medico deve conformarsi ai principi di legalità, colpevolezza e proporzionalità, evitando che l'innovazione si traduca in un'indebita espansione dell'area del penalmente rilevante[4]. In tale prospettiva, l'intelligenza artificiale non può essere considerata né un mero strumento neutro, né un soggetto autonomo di imputazione. Essa si configura piuttosto come un fattore sistemico idoneo a ridefinire il contenuto della posizione di garanzia del sanitario, imponendo una rilettura della colpa in chiave multilivello e garantista[5].

2. La colpa medica tra Balduzzi e Gelli-Bianco

La disciplina della responsabilità penale dell'esercente la professione sanitaria ha conosciuto, nell'ultimo decennio, una profonda evoluzione normativa, finalizzata a razionalizzare l'area della colpa medica e a contenere il fenomeno della medicina difensiva[6].

Con la legge 8 novembre 2012, n. 189 ({URL}), il legislatore ha introdotto un primo tentativo di delimitazione della responsabilità penale, attribuendo rilievo al rispetto delle linee guida e delle buone pratiche clinico-assistenziali quali parametri di valutazione della diligenza professionale[7]. Tale intervento, tuttavia, presentava significative

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - ca rodino ordina

incertezze applicative, in particolare con riferimento alla distinzione tra colpa lieve e colpa grave, affidata in larga misura all'interpretazione giurisprudenziale[8].

La successiva legge 8 marzo 2017, n. 24 ({URL}) ha ulteriormente affinato il quadro normativo, prevedendo l'esclusione della responsabilità penale in caso di imperizia quando il sanitario si sia attenuto a linee guida adeguate al caso concreto, salvo le ipotesi di colpa grave[9]. La riforma si inserisce in una prospettiva dichiaratamente garantista, volta a circoscrivere l'intervento penale alle sole condotte effettivamente rimproverabili[10].

Tuttavia, l'impianto della riforma è stato concepito in un contesto in cui il processo decisionale restava prevalentemente umano.

L'introduzione sistematica dell'intelligenza artificiale incrina tale presupposto, ponendo interrogativi inediti sulla nozione di imperizia, sulla prevedibilità dell'evento e sulla misura della diligenza esigibile dal sanitario[11].

In particolare, l'interazione con sistemi algoritmici complessi rende problematica l'individuazione della regola cautelare violata e la valutazione della concreta evitabilità dell'evento. Ne discende che le categorie elaborate nel contesto predigitale devono essere rilette alla luce del mutato scenario tecnologico, evitando sia derive punitivistiche, sia vuoti di tutela. La colpa medica, nell'era dell'intelligenza artificiale, si configura così come una categoria dinamica, il cui contenuto deve essere ricostruito in relazione al grado di controllo effettivamente esercitabile sul rischio tecnologico[12].

3. L'intelligenza artificiale come supporto decisionale e la posizione di garanzia del medico

Nell'attuale stato dell'arte, i sistemi di intelligenza artificiale impiegati in ambito sanitario operano prevalentemente come strumenti di supporto al processo decisionale clinico, fornendo raccomandazioni, segnalazioni di rischio e suggerimenti diagnostico-terapeutici, senza sostituire formalmente il medico nella titolarità della decisione finale[13]. Ne deriva che la posizione di garanzia nei confronti del paziente permane in capo al sanitario, quale soggetto investito del dovere di protezione del bene salute.

La permanenza della centralità del medico costituisce il punto di partenza per l'analisi della responsabilità penale nell'era digitale. L'output algoritmico non esonera il sanitario dall'obbligo di valutazione critica, ma ne ridefinisce il contenuto, estendendo il dovere di diligenza alla capacità di comprendere, nei limiti del possibile, l'affidabilità dello strumento utilizzato, di contestualizzarne i risultati e di discostarsene quando il quadro clinico lo richieda[14]. In tale prospettiva, la colpa medica non può essere

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - pa rodino ordina

automaticamente affermata né in caso di adesione acritica alle indicazioni dell'intelligenza artificiale, né in caso di loro sistematico rifiuto. Ciò che rileva è la ragionevolezza della decisione adottata alla luce delle conoscenze disponibili, delle linee guida, delle caratteristiche del paziente e delle informazioni fornite dal sistema algoritmico[15].

La posizione di garanzia del medico assume, pertanto, una dimensione "tecnologicamente mediata", nella quale il controllo del rischio non si esaurisce nell'atto clinico in senso stretto, ma si estende alla gestione delle informazioni digitali e alla valutazione della loro attendibilità[16]. In questo contesto, emerge una nuova forma di competenza professionale, che integra il sapere clinico con una conoscenza minima dei limiti e delle potenzialità degli strumenti algoritmici.

4. Scenari applicativi e casi clinico-giuridici

L'impatto dell'intelligenza artificiale sulla responsabilità penale del medico emerge con particolare evidenza nell'analisi di casi clinici concreti, nei quali l'algoritmo interviene come fattore rilevante nel processo decisionale. È sul terreno applicativo che si misura la tenuta delle categorie tradizionali della colpa e della posizione di garanzia[17].

Un primo ambito emblematico è rappresentato dalla diagnostica per immagini. In radiologia, sistemi di intelligenza artificiale sono oggi in grado di individuare lesioni sospette con livelli di accuratezza talora superiori a quelli umani[18]. Si pensi al caso in cui un algoritmo segnali la possibile presenza di una neoplasia polmonare in fase iniziale, raccomandando ulteriori accertamenti. Qualora il medico ignori tale indicazione senza una motivazione clinica plausibile, determinando un ritardo diagnostico con esiti dannosi, la valutazione della colpa dovrà tener conto della ragionevolezza della scelta compiuta.

In tale scenario, l'errore non deriva dall'utilizzo dell'intelligenza artificiale in sé, ma dall'omessa integrazione critica dell'informazione algoritmica nel giudizio clinico complessivo[19]. La responsabilità penale può configurarsi qualora il sanitario abbia disatteso un segnale attendibile senza adeguata giustificazione, violando il dovere di diligenza esigibile. Analoghe considerazioni valgono per la dermatologia digitale, ove algoritmi di riconoscimento delle immagini cutanee sono impiegati per l'identificazione precoce dei melanomi[20]. In tali casi, l'eventuale dissenso rispetto all'output algoritmico deve essere adeguatamente motivato sulla base di dati clinici concreti, al fine di escludere profili di colpa.

Particolarmente delicato è, infine, il contesto del triage digitale nei pronto soccorso. I sistemi di classificazione algoritmica del rischio incidono direttamente sui tempi di intervento e, quindi, sulle possibilità di sopravvivenza del paziente[21]. In presenza di

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - per ordine

segnalazioni attendibili di elevato rischio, una sottovalutazione ingiustificata da parte del medico può tradursi in un evento evitabile penalmente rilevante.

Tali esempi dimostrano come l'intelligenza artificiale non sostituisca il giudizio umano, ma ne divenga parte integrante. La colpa medica si colloca nello spazio che separa l'affidamento acritico dalla valutazione consapevole, richiedendo al sanitario una competenza non solo clinica, ma anche tecnologica[22].

5. La responsabilità distribuita: medico, struttura sanitaria e produttore del software

L'utilizzo dell'intelligenza artificiale in ambito sanitario rende progressivamente inadeguata una concezione monolitica della responsabilità penale, incentrata esclusivamente sulla figura del medico. Il rischio tecnologico si inserisce, infatti, all'interno di una catena decisionale complessa, che coinvolge una pluralità di soggetti, ciascuno titolare di specifici doveri di prevenzione e controllo[23].

Il medico conserva un ruolo centrale, in quanto titolare della posizione di garanzia nei confronti del paziente. Egli è chiamato a esercitare un controllo critico sull'output algoritmico, a comprenderne i limiti e a inserirlo nel contesto clinico concreto. Tuttavia, tale controllo presuppone condizioni organizzative e formative che non dipendono esclusivamente dal singolo professionista[24].

La struttura sanitaria assume una responsabilità di natura prevalentemente organizzativa e preventiva. Essa è tenuta a selezionare sistemi tecnologici affidabili, a garantirne l'aggiornamento e la manutenzione, nonché a predisporre adeguati programmi di formazione per il personale sanitario[25]. In presenza di gravi carenze organizzative, non può escludersi una responsabilità penale per colpa di organizzazione, in linea con l'elaborazione giurisprudenziale in materia di responsabilità degli enti.

Accanto al medico e alla struttura, si colloca il produttore del software, responsabile della progettazione, validazione e sicurezza del sistema algoritmico. Difetti di progettazione, errori sistematici o carenze nei meccanismi di aggiornamento possono incidere direttamente sulla sicurezza del paziente. Sebbene la responsabilità del produttore sia tradizionalmente inquadrata in ambito civilistico, non è esclusa una rilevanza penale in presenza di condotte gravemente negligenti o dolose[26].

Si delinea, in tal modo, un modello di responsabilità multilivello, nel quale il rimprovero penale deve essere commisurato al potere effettivo di controllo esercitabile da ciascun soggetto. Una diversa impostazione, fondata sull'automatica imputazione al medico di ogni evento dannoso, rischierebbe di produrre effetti distorsivi, incentivando forme rinnovate di medicina difensiva e ostacolando l'innovazione tecnologica[27].

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

6. L’algoritmo opaco e il problema della spiegabilitá

Uno dei profili maggiormente problematici nell’impiego dell’intelligenza artificiale in ambito sanitario è rappresentato dall’opacità algoritmica. Molti sistemi basati su tecniche di machine learning e deep learning operano come vere e proprie “scatole nere”, il cui funzionamento interno risulta difficilmente interpretabile anche per gli esperti del settore[28].

Tale opacità incide direttamente sulla valutazione della colpa medica. Qualora il medico non sia in grado di comprendere le ragioni che hanno condotto l’algoritmo a formulare una determinata raccomandazione, il suo margine di controllo risulta significativamente ridotto. In tali condizioni, imputare al sanitario una responsabilità penale per l’adesione a un output errato rischia di porsi in contrasto con il principio di colpevolezza[29].

La questione della spiegabilità assume, pertanto, una valenza eminentemente giuridica. Affinché il medico possa esercitare un controllo consapevole, i sistemi di intelligenza artificiale devono essere progettati secondo criteri di trasparenza, auditabilità e tracciabilità[30]. La possibilità di ricostruire ex post il processo decisionale dell’algoritmo costituisce un requisito essenziale non solo per la sicurezza del paziente, ma anche per la corretta attribuzione della responsabilità. In tale prospettiva, rilevano le indicazioni provenienti dal diritto dell’Unione Europea, in particolare dal Regolamento sull’intelligenza artificiale (AI Act), che valorizza i principi di trasparenza, gestione del rischio e supervisione umana nei sistemi ad alto rischio, tra cui rientrano quelli utilizzati in ambito sanitario[31].

In una prospettiva costituzionalmente orientata, la mancanza di spiegabilità non può tradursi in un aggravamento della responsabilità del medico. Al contrario, essa impone una restrizione dell’area del penalmente rilevante, limitata ai soli casi in cui il sanitario abbia effettivamente avuto la possibilità di comprendere e gestire il rischio tecnologico[32].

7. Profili giurisprudenziali recenti: continuità e adattamento delle categorie penalistiche

La giurisprudenza di legittimità, pur non avendo ancora affrontato in modo sistematico casi paradigmatici di responsabilità penale derivante dall’uso di sistemi di intelligenza artificiale in ambito clinico, ha progressivamente elaborato principi suscettibili di applicazione anche in contesti tecnologicamente avanzati[33].

In particolare, le pronunce della Corte di Cassazione n. 24384 del 2020 e n. 28187 del 2022 ribadiscono la centralità della posizione di garanzia del medico, intesa come obbligo di protezione del bene salute fondato sul controllo effettivo del rischio. La

ISSN 2532-9871 - rivista Cammino Diritto - https://rivista.camminodiritto.it - periodico online

responsabilità penale non può essere fondata su automatismi presuntivi, ma richiede la verifica concreta della violazione di una regola cautelare e della possibilità, per il sanitario, di evitare l'evento dannoso[34]. Tali principi assumono rilievo decisivo nel contesto dell'intelligenza artificiale. L'uso di strumenti tecnologici complessi non elimina la responsabilità del medico, ma ne ridefinisce il contenuto: il controllo si estende all'intero processo decisionale, inclusa la gestione delle informazioni algoritmiche[35].

La giurisprudenza insiste, inoltre, sulla necessità di una valutazione ex ante della condotta, escludendo giudizi retrospettivi fondati sull'esito sfavorevole dell'intervento. Questo orientamento appare particolarmente rilevante nei casi in cui l'intelligenza artificiale fornisca raccomandazioni probabilistiche, caratterizzate da un margine fisiologico di errore[36].

8. Valutazione penalistica: colpa, prevedibilità ed evitabilità nell'era dell'intelligenza artificiale

Dal punto di vista penalistico, l'intelligenza artificiale impone una rilettura delle categorie tradizionali della colpa, senza tuttavia determinarne uno stravolgimento strutturale[37]. Le coordinate fondamentali del rimprovero colposo restano ancorate alla violazione di una regola cautelare, alla prevedibilità dell'evento e alla sua concreta evitabilità.

{URL}

Nell'era dell'intelligenza artificiale, la regola cautelare non può coincidere né con l'obbligo di adesione automatica all'output algoritmico, né con un generico dovere di diffidenza. Essa deve essere ricostruita alla luce delle linee guida cliniche, dei protocolli di utilizzo del sistema, del livello di affidabilità scientifica dell'algoritmo e delle condizioni concrete del paziente[38].

{URL}

La prevedibilità dell'evento lesivo deve essere valutata in relazione alle conoscenze disponibili al momento della decisione. Se l'errore dell'intelligenza artificiale rientra in un margine di imprevedibilità tecnica non dominabile dal medico, l'evento non può essere ascritto a titolo di colpa[39].

{URL}

Il criterio dell'evitabilità rappresenta il vero banco di prova dell'imputazione colposa. Occorre verificare se, in concreto, il sanitario avrebbe potuto comprendere l'errore,

ISSN 2532-9871 Rivista Cammino Diritto - https://rivista.camminodiritto.it - ordine

discostarsi ragionevolmente dall'indicazione dell'algoritmo e adottare una condotta alternativa lecita ed efficace[40].

9. Impatto pratico: criteri operativi per l'accertamento della responsabilità

L'elaborazione teorica fin qui svolta impone un mutamento del metodo di accertamento della responsabilità penale, più che delle categorie dogmatiche di riferimento[41]. In particolare, l'analisi giudiziale dovrebbe articolarsi secondo alcuni passaggi fondamentali:

a) qualificazione del ruolo svolto dall'intelligenza artificiale nel processo decisionale;
b) valutazione del grado di affidabilità del sistema;
c) accertamento della formazione del medico;
d) verifica del margine di controllo concreto;
e) analisi del comportamento alternativo lecito.

Tale approccio consente di evitare sia derive punitivistiche, sia vuoti di tutela, mantenendo il diritto penale entro la sua funzione di extrema ratio[42].

10. Conclusioni

L'introduzione dell'intelligenza artificiale in ambito sanitario non determina una crisi irreversibile delle categorie penalistiche tradizionali, ma ne richiede un'applicazione più rigorosa e consapevole[43]. Il medico resta il perno del sistema di responsabilità, ma la sua posizione di garanzia deve essere interpretata alla luce del controllo effettivo del rischio tecnologico. Una responsabilità penale coerente con i principi costituzionali non può fondarsi su automatismi né sulla mera verificazione dell'evento dannoso. Essa deve ancorarsi alla violazione di regole cautelari esigibili, alla prevedibilità dell'evento e alla concreta evitabilità del danno[44].

Sul piano pratico, ciò impone un rafforzamento della formazione tecnologica dei sanitari, una chiara governance dell'uso dell'intelligenza artificiale da parte delle strutture sanitarie e sistemi algoritmici progettati secondo criteri di trasparenza e controllabilità. Solo in questo quadro l'innovazione può integrarsi nel sistema sanitario senza compromettere né la tutela della salute dei pazienti, né le garanzie fondamentali del diritto penale.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - ca rodino online

Note e riferimenti bibliografici

[1] Cfr. {URL} #160;*Intelligenza artificiale e diritto penale della medicina,* 2024, 45 ss.
[2] F. Basile – {URL} #160;*La responsabilità per colpa medica a cinque anni dalla legge Gelli-Bianco,* Milano, 2022, 23 ss.
[3] Art. 32 Cost.; Corte cost., 26 giugno 2002, n. 282
[4] L. Ferrajoli, *Diritto e ragione,* Roma-Bari, 2009, 589 ss.
[5] V. anche M. Donini, *Responsabilità e rischio tecnologico,* in Riv. It. Dir. proc. Pen., 2021, 1123 ss.
[6] Cfr. G. Fiandaca – E. Musco, *Diritto penale. Parte generale,* Bologna, ult. ed., 712 ss.
[7] L. 8 novembre 2012, {URL}
[8] Cass., sez. IV, 11 marzo 2014, n. 16237
[9] L. 8 marzo 2017, n. 24, art. 6.
[10] F. Viganò, *La responsabilità medica dopo la legge Gelli-Bianco,* in Dir. Pen. Cont., 2017, 1 ss.
[11] F. Centonze, *Colpa e tecnologie complesse,* in Riv. It. Dir. Proc. Pen., 2020, 845 ss.
[12] A. Cadoppi, *Responsabilità penale e rischio tecnologico*, Torino, 2019, 156 ss.
[13] Cfr. G. Comandè – G. Sartor, *Responsabilità e intelligenza artificiale,* Torino, 2020, 97 ss.
[14] M. Gambardella, *Colpa medica e nuove tecnologie,* in Cass. Pen., 2021, 3245 ss.
[15] Cass., sez. IV, 21 giugno 2018, {URL}
[16] A. Di Martino, *Posizione di garanzia e tecnologie sanitarie,* in Dir. Pen. Proc., 2022, 114 ss.
[17] Cfr. F. Palazzo, *Corso di diritto Penale,* Torino, ult. ed., 412 ss.
[18] E. Topol, *Deep Medicine,* New York, 2019, 67 ss.
[19] M. Ronco, *Colpa e affidamento tecnologico,* in Riv. It. Dir. Proc. Pen., 2021, 901 ss.
[20] A. Esteva et al., *Dermatologist-level classification of skin cancer,* in Nature, 2017, 542, 115 ss.
[21] WHO, *Digital Trage Systems in Emergency Care,* 2021.
[22] S. Seminara, *Responsabilità professionale e innovazione,* in Resp. Civ. prev., 2022, 233 ss.
[23] Cfr. G. Marinucci – E. Dolcini, *Manuale di Diritto Penale,* Milano, ult. ed., 389 ss.
[24] A. Gargani, *Colpa professionale e organizzazione sanitaria,* in Riv. It. Dir. Proc. Pen., 2019, 1045 ss.
[25] Cass., sez. IV, 9 marzo 2017, n. 8770.
[26] A. Vallini, *Responsabilità penale del produttore di software medico,* in Dir. Pen. Cont., 2022, 57 ss.
[27] M. Pelissero, *Rischio tecnologico e imputazione penale,* Torino, 2021, 142 ss.
[28] C. Burrell, *How the Machine "Thinks",* in Big Data & Society, 2016.
[29] {URL} #160;*Diritto e ragione,* cit., 601 ss.
[30] S. Wachter – B. Mittelstad, *A right to Explanation,* in Int. Data Privacy Law, 2017, 76 ss.
[31] Regolamento UE 2024/1684 AI ACT, artt. 9,13,14.
[32] F. Viganò, *Colpa e prevedibilità nell'era algoritmica,* in Sistema Penale, 2024
[33] Cfr. M Gallo, *Tecnologia e responsabilità penale,* in Cass. Pen., 2021, 2871 ss.
[34] Cass., sez. IV, 16 luglio 2020, n. 24384; Cass., sez. IV, 12 luglio 2022, n. 28187.
[35] A. Pagliaro, *Rischio consentito e nuove tecnologie,* Milano, 2020, 94 ss.
[36] Cass., sez. IV, 7 maggio 2019, n. 21221.
[37] G. Fiandaca – E. Musco, *Diritto Penale, cit., 720 ss.*
[38] F. Palazzo, *Colpa penale e regole cautelari,* Torino, 2018, 133 ss.
[39] M. Donini, *Imputazione oggettiva e rischio tecnologico,* in Riv. It. Dir. Proc. Pen., 2022, 501 ss.
[40] Cass., sez. IV, 14 febbraio 2018, n. 8243.
[41] Cfr. L. Cornacchia, *Metodo e Responsabilità penale,* Bologna, 2020, 211 ss.
[42] {URL} #160;*Diritto e ragione,* cit., 615 ss.
[43] A. Cadoppi, *Rischio e Responsabilità,* cit. 2021 ss.
[44] F. Viganò, *Colpevolezza e Tecnologia,* in Sistema Penale, 2024

Bibliografia

BASILE F., POLI {URL} #160;*La responsabilità per colpa medica*, Milano, 2022.

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - rivista di diritto online

CADOPPI A., *Responsabilità penale e rischio tecnologico*, Torino, 2019.
COMANDÉ G., SARTOR G., *Responsabilità e IA*, Torino, 2020.
FERRAJOLI L., *Diritto e ragione*, Roma-Bari, 2009.
JANUÀRIO {URL} #160;*Intelligenza artificiale e diritto penale*, 2024.
PALAZZO F., *Colpa penale*, Torino, 2018.

Giurisprudenza

Cass., sez. IV, 16 luglio 2020, n. 24384.
Cass., sez. IV, 12 luglio 2022, n. 28187.
Cass., sez. IV, 14 febbraio 2018, n. 8243.

Normativa

L. 8 novembre 2012, n. 189.
L. 8 marzo 2017, n. 24.
Reg. (UE) 2024/1684 (AI Act).

Sitografia

Commissione europea, Artificial Intelligence Act, 2024.
WHO, Digital Health Guidelines, 2021.

---

* Il simbolo {URL} sostituisce i link visualizzabili sulla pagina: https://rivista.camminodiritto.it/articolo.asp?id=11486

ISSN 2532-9871 rivista Cammino Diritto - https://rivista.camminodiritto.it - pagina online