L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SUI SISTEMI DI VOTO ELETTRONICO NELL'EPOCA DELLE CRISI GLOBALI

Federica Bertoni

ILS
INFORMATION, LAW & SOCIETY

Milano University Press

Federica Bertoni

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SUI SISTEMI DI VOTO ELETTRONICO NELL'EPOCA DELLE CRISI GLOBALI

Milano University Press

L'impatto dell'intelligenza artificiale sui sistemi di voto elettronico nell'epoca delle crisi globali / Federica Bertoni. Milano: Milano University Press, 2026. (Information, Law & Society, 3)

ISBN 979-12-5510-380-6 (print)
ISBN 979-12-5510-384-4 (PDF)
ISBN 979-12-5510-387-5 (EPUB)
DOI 10.54103/infolawsoc.280

Pubblicato da:
Milano University Press
Via Festa del Perdono 7 – 20122 Milano
Sito web: https://milanoup.unimi.it
e-mail: redazione.milanoup@unimi.it

L'edizione cartacea del volume può essere ordinata in tutte le librerie fisiche e online ed è distribuita da Ledizioni (www.ledizioni.it)

Indice

PARTE VI
CONCLUSIONI E RACCOMANDAZIONI PER IL FUTURO

Premessa

La scintilla che ha dato avvio a questo lavoro si è accesa poco prima delle elezioni presidenziali statunitensi del 2016. In quel periodo iniziai a occuparmi degli scenari di attacco ai sistemi di voto elettronico e degli aspetti di Digital Forensics sottesi. Ben presto mi resi conto della portata del problema. L'analisi dei possibili vettori d'attacco e i primi approfondimenti sulle vulnerabilità delle macchine per il voto elettronico, discussi anche in prestigiose conferenze internazionali come Black Hat e DEF CON, confermarono infatti quanto fossero concreti quei rischi. Ricordo, ad esempio, che alla DEF CON di Las Vegas del 2017 un team di esperti riuscì a compromettere diverse urne elettroniche nel giro di pochissimo tempo: fu sufficiente circa un'ora e mezza perché venisse violato il primo dispositivo e poco più per gli altri[1]. La conferenza Black Hat, tenutasi l'anno successivo, ospitò a sua volta un intervento dedicato all'analisi forense delle macchine di voto WinVote, già ritirate dallo Stato della Virginia dopo il 2015, a causa delle loro falle e che furono descritte come «le peggiori mai realizzate», in termini di sicurezza[2].

Eventi come questi dimostrarono chiaramente che i sistemi di voto dovevano essere al più presto considerati e protetti come *infrastrutture critiche*, mentre all'epoca il tema era pressoché assente dal dibattito pubblico. Non a caso, poco dopo le elezioni del 2016 anche le autorità statunitensi riconobbero l'importanza strategica di tali sistemi, arrivando a designare formalmente le piattaforme elettorali come "infrastrutture critiche" nazionali[3].

Ero quindi sempre più convinta che servisse un cambio di paradigma nel modo di considerare la sicurezza elettorale e ho cercato di promuovere questa visione in diversi contesti. Già intorno al 2015 ebbi modo di "lanciare il sasso" e d'iniziare a discutere brevemente di queste tematiche, in un intervento durante un Security Summit, quando il voto elettronico era un argomento ancora trascurato e dunque forse un po' pionieristico, soprattutto per l'Italia e in contesti congressuali a forte impronta commerciale, dove tali tematiche faticavano ancora a trovare spazio. Poco dopo ebbi l'opportunità di tenere una lezione

1 Everyeye Tech. (2017). *Alla Defcon le macchine per il voto americane sono state craccate in 90 minuti*. Disponibile su: https://tech.everyeye.it/notizie/alla-defcon-seggi-elettronici-statunitensi-sono-stati-craccati-in-90-minuti-300364.html *(consultato il 9 luglio 2025)*.

2 Black Hat. (2018). *A History of Voting Machine Vulnerabilities & Persistent Hacks*. Disponibile su: https://www.blackhat.com/latestintel/06052018-history-voting-machine-vulnerabilities.html *(consultato il 9 luglio 2025)*.

3 U.S. Department of Homeland Security. (2017). *Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*. Disponibile su: https://www.dhs.gov/archive/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical *(consultato il 9 luglio 2025)*.

di un'intera giornata in un master in cybersecurity presso il parco scientifico Kilometro Rosso di Bergamo: anche in quell'occasione illustrai ai partecipanti la mia convinzione che i sistemi di e-voting andassero annoverati fra le infrastrutture critiche, evidenziandone i rischi emergenti e le possibili contromisure.

La costante attività di ricerca indipendente e il confronto su questi argomenti hanno arricchito enormemente il mio percorso professionale. Una cosa è certa: tutti i dibattiti a cui ho potuto partecipare all'epoca mi hanno permesso di crescere e di affinare tutte le idee sviluppate e confluite in queste pagine. Desidero quindi ringraziare di cuore tutti coloro che, in un modo o nell'altro, hanno finito per contribuire alla realizzazione di questo lavoro.

L'auspicio è che l'opera possa stimolare riflessioni, suscitare domande e offrire spunti utili per affrontare le sfide che le tecnologie dell'intelligenza artificiale pongono oggi alla nostra democrazia.

È con questo spirito che consegno il mio lavoro ai lettori, nella speranza che possano trovarvi non solo informazioni e analisi, ma anche una reale fonte di ispirazione per guardare al futuro con maggiore consapevolezza e, soprattutto, con **etica** e responsabilità.

Ringraziamenti

Al Professor Giovanni Ziccardi

A lui devo una delle opportunità più significative dell'intero mio percorso professionale: essere accolta, sin dal primo incontro, con rara apertura, fiducia e autentica stima nel cuore pulsante del suo straordinario Information Society Law Center. Nonostante un iter formativo che, negli anni universitari, si sia progressivamente discostato dalle traiettorie accademiche e forensi più convenzionali, come il dottorato o la pratica forense, mi è stata concessa, con generosità non comune, la possibilità di partecipare attivamente alla vita di un centro di ricerca d'eccellenza, contribuendo a corsi, iniziative editoriali e, soprattutto, alla realizzazione di questa opera. Desidero ringraziarlo in modo particolare per la pazienza discreta e la costanza lucida con cui ha saputo accompagnarmi, senza mai forzare, anche nei momenti di inevitabile discontinuità dettati dalle esigenze dell'attività professionale. Lo ha fatto con quella sua inconfondibile combinazione di garbo e determinazione, che nei momenti decisivi è capace di indicare, senza rumore, l'essenziale. È anche grazie a lui se ho imparato – professionalmente e umanamente – che i "cerchi" vanno chiusi, e che il rigore non esclude la misura, né l'autenticità. Al Professor Ziccardi rivolgo la mia più profonda stima, un sentimento di viva e sincera riconoscenza e un affetto che nasce dal riconoscere, nel suo modo d'insegnare e guidare, qualcosa di genuinamente umano e perciò tanto più raro quanto prezioso.

Grazie.

Ai miei genitori

A voi desidero dedicare queste pagine, che custodiscono non solo un lavoro di ricerca, ma il compimento di un cammino nato molto prima di ogni traguardo accademico. Vi siete congedati troppo presto per poter assistere con i vostri occhi a ciò che oggi è divenuto realtà: che la Cybersecurity e la Digital Forensics non erano una semplice infatuazione adolescenziale, ma il nucleo vivo di una vocazione autentica, radicata con forza e consapevolezza sin dagli anni del liceo. Quando, a quindici anni, immaginavo scenari di attacchi informatici, investigazioni digitali e minacce alla sicurezza delle istituzioni, sentivo, in silenzio, che quella sarebbe stata la mia direzione. Avrei voluto mostrarvi il senso profondo di quella passione precoce, allora forse difficile da decifrare, e dimostrarvi che, nel tempo, ha trovato piena legittimazione nella scienza, nelle professioni, nelle istituzioni e nella quotidianità della nostra società interconnessa. Eppure, credo che abbiate sempre saputo, anche senza dichiararlo apertamente, intuivate che in quella scelta così atipica vi fosse qualcosa di necessario, qualcosa che non poteva essere ignorato. E che, forse, nel seguire una strada inconsueta con ostinazione e fiducia, in fondo ci avevo visto giusto. A voi, che mi avete dato molto più di quanto la vita vi abbia concesso di vedere.

Con amore e gratitudine,

Federica

Introduzione

L'intelligenza artificiale (I.A.) sta ridefinendo il nostro rapporto con la tecnologia e trasformando profondamente i contesti sociali, economici e politici in cui viviamo. Tra le molteplici applicazioni di questa disciplina, il suo utilizzo nei sistemi di voto elettronico rappresenta una delle sfide più significative e delicate del nostro tempo. Questo saggio si pone l'obiettivo di analizzare in modo sistematico e rigoroso il ruolo dell'I.A. nel contesto elettorale, con particolare attenzione alle implicazioni etiche, legali e tecnologiche che emergono in un'epoca caratterizzata da crisi globali senza precedenti (dall'emergenza sanitaria segnata dalla pandemia del 2020 alle guerre e alle emergenze climatiche).

Dal punto di vista metodologico, lo studio adotta un approccio di ricerca qualitativo e comparativo, basato sull'analisi teorica e sul confronto tra diversi casi ed esperienze rilevanti nel panorama internazionale. Tale cornice metodologica permette di esaminare il fenomeno integrando prospettive multidisciplinari, senza limitarsi a un singolo contesto nazionale o a un'unica disciplina.

I diversi scenari di crisi su scala mondiale degli ultimi anni hanno già inciso profondamente sui processi elettorali. La pandemia da Covid-19, ad esempio, ha aperto un vivace dibattito sull'estensione di modalità di voto alternative e sicure per garantire la partecipazione senza rischi sanitari[1]. Parallelamente, il 2024 è stato definito "l'anno elettorale più grande della storia" – con oltre metà della popolazione globale chiamata al voto – e la rapida diffusione dell'IA ha suscitato timori su come siffatte tecnologie potessero influenzare i processi elettorali in tutto il mondo[2]. I conflitti geopolitici odierni hanno alimentato il rischio di attacchi cibernetici ai sistemi di voto condotti mediante strumenti di IA, minacciando seriamente l'integrità dei processi democratici[3]. Allo stesso tempo, gli eventi climatici estremi sempre più frequenti rischiano d' interrompere le normali operazioni di voto: basti pensare che dopo l'uragano Sandy negli USA venne persino consentito il voto via e-mail o fax in via eccezionale[4]. Tutto ciò rende evidente la necessità di soluzioni di voto più resilienti e innovative per

1 International IDEA. (2020). *Elections and Covid-19: How special voting arrangements were expanded in 2020*. Disponibile su: https://www.idea.int/news/elections-and-covid-19-how-special-voting-arrangements-were-expanded-2020 *(consultato il 9 luglio 2025)*.

2 Ash Center for Democratic Governance and Innovation – Harvard Kennedy School. (2024). *The role of AI in the 2024 Elections*. Disponibile su: https://ash.harvard.edu/resources/the-role-of-ai-in-the-2024-elections/ *(consultato il 7 luglio 2025)*.

3 BitMat. (2024). *Guerra informatica: le elezioni globali, un bersaglio dei cyber attacchi*. Disponibile su: https://www.bitmat.it/sicurezza/guerra-informatica-le-elezioni-globali-un-bersaglio-dei-cyber-attacchi *(consultato l'8 luglio 2025)*.

4 RAND Corporation. (2024, gennaio). *Preparing for Climate Change Risks to the 2024 Elections*. Disponibile su: https://www.rand.org/pubs/commentary/2024/01/preparing-for-climate-change-risks-to-the-2024-elections.html *(consultato il 7 luglio 2025)*.

fronteggiare situazioni d'emergenza[5], di qualsiasi natura. Queste convergenti crisi globali rendono ancora più urgente se non addirittura imperante innovare i meccanismi del voto elettronico, affinché la democrazia possa funzionare efficacemente anche nei momenti di grave difficoltà collettiva.

Contesto e finalità dell'opera

L'adozione dell'IA nei sistemi di voto elettronico è una tematica complessa, che unisce aspetti tecnici e normativi a problematiche sociali e geopolitiche. Il lavoro nasce dall'urgenza di comprendere come queste tecnologie possano essere impiegate per migliorare i processi elettorali, garantendo al contempo sicurezza, trasparenza e inclusività. Tuttavia, è cruciale interrogarsi anche sui rischi connessi a tali innovazioni, tra cui l'abuso di dati personali, l'utilizzo di deepfake per la disinformazione e le vulnerabilità correlate agli attacchi cibernetici. Il presente saggio si propone dunque di:

- Fornire un'analisi critica delle tecnologie emergenti applicate al voto elettronico, evidenziandone benefici e limiti.
- Esplorare i quadri normativi esistenti e proporre strategie per colmare le lacune regolatorie in materia di IA e voto digitale.
- Offrire raccomandazioni per un uso etico e responsabile dell'IA nei processi democratici, con uno sguardo alle prospettive future di medio e lungo termine.

In altri termini, le domande chiave cui questa ricerca mira a rispondere sono le seguenti: in che modo le tecnologie di I.A. emergenti possono rafforzare la sicurezza, la trasparenza e l'inclusività del voto elettronico in un contesto di crisi globali? Quali sono le principali lacune dell'attuale regolamentazione relativa all'I.A. applicata alle elezioni, e come è possibile colmarle? Infine, quali linee guida e best practice possono essere sviluppate per garantire un impiego dell'I.A. conforme ai principi democratici, minimizzandone i rischi e massimizzandone i benefici per il futuro? Gli scopi dell'opera sono dunque molteplici: da un lato sensibilizzare il lettore sull'importanza d'integrare l'innovazione tecnologica nel rispetto dei principi democratici; dall'altro, fornire strumenti di analisi utili non solo alla comunità accademica ma anche a legislatori, amministratori elettorali e professionisti del settore, sì da contribuire in modo concreto al dibattito pubblico e alle politiche in materia.

5 S. James, Alistair Clark e Erik Asplund (a cura di). (2023). *Elections during Emergencies and Crises: Lessons for Electoral Integrity from the Covid-19 Pandemic. Stockholm: International Institute for Democracy and Electoral Assistance* (International IDEA), 724 pp. ISBN 978-91-7671-627-4 (PDF). DOI: 10.31752/idea.2023.24. Disponibile su: https://www.idea.int/publications/catalogue/elections-during-emergencies-and-crises (link consultato il 12 luglio 2025).

Limiti

Pur trattando un argomento di ampio respiro, il saggio si concentra su specifici aspetti ritenuti nevralgici, delineando con chiarezza i confini dell'analisi. In particolare, lo studio privilegia il piano qualitativo e teorico-comparativo, senza addentrarsi nei dettagli strettamente tecnici o algoritmici dei sistemi di voto elettronico. Le soluzioni tecnologiche (ad esempio i protocolli crittografici o le implementazioni software) sono discusse nei loro principi generali, ma non costituiscono oggetto di progettazione o sperimentazione diretta in questa sede. Inoltre, per ragioni di spazio, l'indagine si focalizza principalmente su esempi ed esperienze recenti particolarmente significative, come le elezioni svoltesi durante la pandemia da Covid-19 o in contesti di conflitto, senza pretesa di coprire in maniera esaustiva tutte le realtà geografiche. Tali scelte metodologiche e di campo assicurano una trattazione mirata e coerente, ma al tempo stesso rappresentano un limite che si auspica di colmare con future ricerche estese ad altri contesti e con approfondimenti interdisciplinari ulteriori.

Struttura del lavoro

L'opera è strutturata in sei parti principali, ciascuna delle quali affronta temi cruciali legati all'intersezione tra intelligenza artificiale e processo elettorale. Di seguito si offre una panoramica della struttura del lavoro e dei contenuti di ciascuna parte:

- Parte I – Fondamenti d'intelligenza artificiale (I.A.) e sue applicazioni nella Cybersecurity
  Questa prima parte introduce i concetti fondamentali dell'intelligenza artificiale, illustrandone l'evoluzione storica e i principali approcci metodologici. Viene poi analizzato l'impiego dell'IA nell'ambito della cybersecurity, con particolare attenzione alle sue applicazioni per il rilevamento delle minacce, la difesa predittiva e l'investigazione digitale, evidenziandone il ruolo crescente nella protezione dei sistemi informatici.
- Parte II – Voto elettronico e online
  La seconda parte è dedicata all'esame del voto elettronico e del voto online, ripercorrendo le principali implementazioni e sperimentazioni a livello internazionale. Si analizzano le implicazioni tecnologiche e democratiche di questi sistemi, evidenziando come le tecnologie digitali – tra cui l'intelligenza artificiale – stiano trasformando le modalità di espressione del voto, con effetti su accessibilità, trasparenza ed efficienza dei processi elettorali.
- Parte III – I.A. per la sicurezza e l'integrità elettorale
  In questa parte si approfondisce l'utilizzo dell'intelligenza artificiale a tutela della sicurezza e dell'integrità del voto. Il primo capitolo esplora le applicazioni dell'IA nella protezione del ciclo elettorale, nel rilevamento

delle interferenze e nella lotta alla disinformazione. Il secondo capitolo presenta casi di studio ed esperienze concrete in cui l'IA ha contribuito positivamente a garantire elezioni più sicure, trasparenti e resilienti, evidenziando buone pratiche e prospettive future.

– Parte IV – Rischi e profili di uso malevolo dell'IA nel voto elettronico.
  In queste pagine si affrontano le minacce connesse all'uso illecito o malevolo dell'intelligenza artificiale in ambito elettorale. In particolare, vengono analizzati fenomeni quali la disinformazione amplificata da deepfake, gli attacchi informatici avanzati alle infrastrutture di voto digitale e la manipolazione algoritmica dell'opinione pubblica. Questa parte del lavoro mette in guardia sugli impatti potenzialmente dannosi di un'I.A. non adeguatamente regolamentata, evidenziando la necessità di contromisure efficaci.
– Parte V – Scenari di crisi globali e impatto sul voto elettronico.
  In questa sezione si offrono alcune riflessioni su come situazioni di crisi sanitarie, belliche o climatiche, possano influire sullo svolgimento delle consultazioni elettorali. Vengono discussi casi ed esempi in cui eventi eccezionali (ad esempio, una pandemia o una guerra) hanno richiesto l'adozione di soluzioni alternative di voto, come il ricorso al voto online o postale, analizzando i risultati e le lezioni apprese. Si evidenzia come le crisi globali fungano da catalizzatore per l'innovazione nel settore elettorale, accelerando cambiamenti che in tempi normali avverrebbero più gradualmente.
– Parte VI – Conclusioni e raccomandazioni per il futuro.
  L'ultima parte sintetizza i risultati dell'analisi e traccia le conclusioni generali dello studio. Vengono proposte raccomandazioni pratiche per implementare l'IA nei processi di voto in modo responsabile, mitigando i rischi identificati e massimizzando le opportunità a beneficio della collettività. Infine, si delineano alcune prospettive future, indicando possibili direttrici di ricerca e sviluppo (sia tecnologico che normativo) affinché la combinazione tra IA e voto elettronico possa rafforzare la democrazia nell'epoca delle crisi globali.

PARTE I
FONDAMENTI D'INTELLIGENZA ARTIFICIALE (I.A.)

Capitolo 1
Principi d'intelligenza artificiale

1.1 Definizione e storia dell'intelligenza artificiale

L'Intelligenza Artificiale (IA) è un campo interdisciplinare che unisce informatica, matematica, neuroscienze e altre scienze con l'obiettivo di progettare sistemi capaci di svolgere compiti tipicamente umani. Tali attività comprendono il ragionamento, l'apprendimento dall'esperienza, la percezione sensoriale, la comprensione del linguaggio naturale e persino la capacità decisionale autonoma. Attraverso algoritmi avanzati, l'I.A. non si limita ad imitare questi processi, ma spesso li potenzia: grazie all'analisi rapidissima di enormi quantità di dati, i sistemi intelligenti riescono a individuare schemi e connessioni che sfuggirebbero all'occhio umano. In altre parole, l'IA può scoprire regolarità nei dati e trarre conclusioni con un'efficienza irraggiungibile per una mente umana, aprendo la strada ad applicazioni prima impensabili[1]

Il concetto di "macchina intelligente" ha radici teoriche profonde. Già nel 1950 il matematico Alan Turing si interrogò su come verificare l'intelligenza di un calcolatore, proponendo il celebre *Test di Turing* come criterio: se un osservatore non riesce a distinguere, dialogando al buio, un computer da un essere umano, allora il computer può essere considerato intelligente[2]. Questa idea pionieristica pose le basi filosofiche dell'IA, sollevando la domanda fondamentale su cosa significhi *pensare* per una macchina.

Come disciplina autonoma, l'IA nacque ufficialmente alla conferenza di Dartmouth del 1956, durante la quale John McCarthy (che proprio in quell'occasione coniò il termine *"Artificial Intelligence")* delineò insieme ad altri studiosi la visione di macchine in grado di risolvere problemi e riprodurre forme di ragionamento umano. Alla fine degli anni '50 vennero sviluppati i primi programmi simbolici: ad esempio, Allen Newell e Herbert Simon progettarono il *Logic Theorist* (1956), capace di dimostrare teoremi matematici, e il *General Problem Solver* (1957), un risolutore generale di problemi basato su tecniche euristiche.

---

1 S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*, Pearson Education, 2016. La definizione di IA come campo multidisciplinare è comune nella letteratura accademica e riflette la natura diversificata della ricerca in questo campo; I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, 2016. La capacità degli algoritmi di IA di rilevare pattern nascosti nei dati è uno degli elementi distintivi dell'IA moderna.

2 Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, 59(236), 433–460. Il Test di Turing è un concetto fondante nella storia dell'IA, ancora oggi utilizzato come riferimento fondamentale per valutare l'intelligenza delle macchine.

Questi prototipi dimostrarono concretamente che algoritmi informatici potevano emulare processi logici umani, suscitando grande entusiasmo nella comunità scientifica. Sempre nel 1958, il ricercatore Frank Rosenblatt introdusse il *Perceptron*, il primo modello di rete neurale artificiale ispirato al funzionamento dei neuroni biologici: esso era in grado di apprendere a riconoscere semplici pattern (come forme geometriche), ponendo le basi per lo sviluppo successivo delle reti neurali e dell'apprendimento automatico.

Tuttavia, le aspettative elevate dei primi anni '60 dovettero fare i conti con limiti tecnici significativi. Nel 1969 Marvin Minsky e Seymour Papert dimostrarono matematicamente che il Perceptron a singolo strato non poteva risolvere neppure semplici funzioni logiche (come l'operazione XOR), evidenziando la necessità di reti multistrato più complesse per superare tali ostacoli[3]. Questo risultato, insieme ad altre difficoltà dell'epoca, provocò un brusco rallentamento nella ricerca: fu il primo "inverno dell'IA", un periodo in cui finanziamenti e interesse verso l'intelligenza artificiale calarono drasticamente. Negli anni '70 l'attenzione si spostò verso i cosiddetti sistemi esperti – programmi progettati per riprodurre il processo decisionale di specialisti in domini ristretti (famosi i prototipi *MYCIN* in ambito medico e *DENDRAL* in ambito chimico). Pur avendo inizialmente successo in compiti specifici, questi sistemi basati su regole rigide soffrivano l'assenza di capacità di apprendimento adattivo, il che ne limitò la scalabilità e portò a un secondo "inverno dell'IA" tra fine anni '80 e inizio '90.

Una nuova fase di rapida evoluzione si è avuta a partire dalla metà degli anni '90, grazie ai progressi nel machine learning (apprendimento automatico) di impostazione statistica e all'aumento esponenziale della potenza di calcolo disponibile. Algoritmi come le *support vector machines* e reti neurali più avanzate, uniti alla disponibilità di moli crescenti di dati digitali, permisero di superare molte limitazioni precedenti. Un momento chiave di questa *rinascita* fu il 2012, quando una rete neurale profonda (*deep neural network*) denominata *AlexNet* (sviluppata da Hinton, Krizhevsky e altri) vinse la competizione ImageNet di riconoscimento visivo: la capacità di quella rete di classificare correttamente milioni di immagini segnò l'inizio della rivoluzione del deep learning e mostrò al mondo il potenziale delle tecniche neurali a più strati. Da allora l'IA ha vissuto un'accelerazione impressionante, con applicazioni prima fantascientifiche divenute realtà quotidiana (dalla visione artificiale agli assistenti vocali, fino alle auto a guida autonoma).

Negli ultimissimi anni, infine, si è imposta all'attenzione globale la cosiddetta IA generativa. Modelli avanzati come la serie GPT di OpenAI, in grado di produrre testi di sorprendente coerenza a partire da semplici istruzioni in linguaggio naturale, o come DALL-E (OpenAI) capace di creare immagini originali da

3 Minsky, M., & Papert, S. (1969). *Perceptrons: An Introduction to Computational Geometry*. MIT Press. L'opera evidenziò i limiti delle reti neurali a singolo strato, contribuendo al primo "inverno" dell'IA.

descrizioni testuali, hanno dimostrato che le macchine possono ora generare contenuti nuovi – testi, immagini, audio – e non solo analizzare dati esistenti. Strumenti come questi (a cui si aggiungono altri esempi, ad es. *MusicLM* di Google per generare brani musicali) aprono scenari applicativi inediti ma sollevano al contempo nuove questioni etiche e giuridiche. L'IA generativa può infatti essere utilizzata sia positivamente (si pensi alla creazione di contenuti personalizzati o al supporto creativo) sia in modi potenzialmente dannosi, ad esempio per produrre fake news o *deepfake* difficili da distinguere dal reale. Per questo le istituzioni stanno correndo ai ripari: governi e organismi sovranazionali stanno lavorando a linee guida e normative (come il Regolamento europeo AI Act) per assicurare che l'evoluzione dell'IA avvenga in modo trasparente, sicuro e rispettoso dei diritti fondamentali. La storia dell'IA, in sintesi, è caratterizzata da cicli di entusiasmo e momenti di crisi, ma mostra un chiaro trend di crescita nelle capacità delle macchine intelligenti – un progresso che rende sempre più urgente affrontarne responsabilmente le implicazioni sociali.

1.2 Principali tecniche e algoritmi dell'I.A.

Nell'ambito dell'intelligenza artificiale (IA) si distinguono diverse tecniche e paradigmi fondamentali che, nel loro insieme, ne hanno plasmato l'evoluzione. In primo luogo, il Machine Learning (ML) – o apprendimento automatico – costituisce un pilastro centrale dell'IA, fornendo ai sistemi la capacità di imparare automaticamente dai dati e dall'esperienza senza essere esplicitamente programmati per ogni compito specifico. Uno sviluppo di spicco all'interno del ML è rappresentato dal Deep Learning (DL), un sottoinsieme avanzato del machine learning e dell'IA basato su modelli di reti neurali artificiali multistrato capaci di estrarre rappresentazioni gerarchiche dai dati, dove i concetti di alto livello emergono a partire da quelli di basso livello. Parallelamente, ha assunto crescente rilievo l'Intelligenza Artificiale Spiegabile (XAI, eXplainable AI), un insieme di metodologie volto a rendere trasparenti e comprensibili agli esseri umani i meccanismi decisionali di modelli di ML tipicamente opachi, aumentando così la fiducia degli utenti nelle decisioni automatizzate e garantendo una maggiore conformità a requisiti normativi nei contesti applicativi critici. Un ulteriore ambito cruciale è l'Elaborazione del Linguaggio Naturale (NLP, Natural Language Processing), sottodisciplina dell'IA e dell'informatica che utilizza algoritmi di machine learning per consentire ai computer di comprendere, interpretare e generare il linguaggio umano in forma testuale o vocale, permettendo applicazioni che spaziano dalla traduzione automatica all'analisi semantica di documenti. Sul piano metodologico, gran parte degli algoritmi di IA comporta la risoluzione di problemi di ottimizzazione: in tal senso, tecniche matematiche per ottimizzare sono impiegate per tarare modelli e trovare soluzioni ottimali a problemi complessi; ad esempio, l'algoritmo della discesa del gradiente costituisce un

procedimento cardine per addestrare reti neurali e altri modelli di ML, minimizzando iterativamente una funzione di errore. Infine, la Visione Artificiale (o Computer Vision) rappresenta un altro pilastro dell'IA, concernendo l'insieme di tecniche che permettono ai sistemi informatici di vedere e interpretare informazioni visive. Questo campo dell'IA combina algoritmi avanzati (spesso basati su deep learning) per analizzare immagini e video ed estrarne conoscenza utile, replicando in parte la capacità umana di riconoscere oggetti, volti e pattern visivi con elevati livelli di accuratezza.

1.3 Applicazioni attuali dell'I.A.

Le applicazioni dell'Intelligenza Artificiale stanno trasformando in modo radicale e pervasivo una vasta gamma di settori, migliorando processi tradizionali grazie alla capacità dei sistemi IA di analizzare enormi quantità di dati in autonomia e con grande efficienza ed efficacia. Questa rivoluzione tecnologica si traduce in significativi avanzamenti in termini di produttività e qualità, permettendo alle organizzazioni di affrontare sfide complesse, con un approccio più flessibile e proattivo. L'adozione dell'IA consente infatti di trovare soluzioni innovative a problemi un tempo intrattabili, spesso in tempo reale, e apre la strada a nuovi modelli di servizio e di business. Al contempo, l'uso diffuso dell'IA in contesti critici solleva interrogativi circa l'impatto etico e normativo, richiedendo un attento bilanciamento tra innovazione e tutela dei valori fondamentali[4].

Si analizzano di seguito le principali applicazioni attuali dell'intelligenza artificiale.

a) Sanità.

In ambito sanitario l'IA sta avendo un impatto dirompente su prevenzione, diagnosi e cura. Sistemi di deep learning addestrati su immagini mediche (radiografie, risonanze, TAC) supportano i medici nell'individuare lesioni o anomalie con un'accuratezza spesso paragonabile a quella umana. Algoritmi predittivi analizzano le cartelle cliniche elettroniche e i dati genetici per identificare pazienti a rischio e suggerire trattamenti personalizzati, promuovendo un approccio di medicina preventivo-proattiva basata sui dati[5]. In ambito farmacologico, tecniche di AI accelerano la scoperta di nuovi farmaci simulando virtualmente milioni di molecole e selezionando le più promettenti. Tuttavia, l'utilizzo di dati clinici sensibili richiede

4 Russell, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach*. Pearson Education. Le applicazioni dell'IA si estendono in numerosi settori – dalla medicina alla finanza – sollevando al contempo importanti questioni di natura etica e normativa.

5 Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books. L'IA promette di migliorare diagnosi e cure mediche attraverso tecnologie avanzate, contribuendo a una sanità più efficiente e personalizzata.

l'adozione di standard etici e normativi molto elevati. Regolamenti come il GDPR dell'Unione Europea e specifiche normative nazionali impongono rigorose tutele sulla privacy dei pazienti e sulla sicurezza dei dati sanitari, influenzando direttamente la progettazione delle applicazioni di IA in questo settore[6]. Ciò assicura, ad esempio, che algoritmi per la diagnosi automatica siano sviluppati e utilizzati rispettando la riservatezza delle informazioni mediche e i diritti dei pazienti.

b) Finanza.

Il settore finanziario è stato tra i primi ad abbracciare su vasta scala le soluzioni di IA, con benefici tangibili in termini di efficienza e capacità predittiva. Algoritmi di machine learning vengono utilizzati per rilevare transazioni fraudolente in tempo reale, analizzando i pattern di spesa degli utenti e bloccando attività anomale ancor prima che possano causare danni significativi. Nella gestione del rischio, modelli IA valutano grandi moli di dati di mercato per prevedere fluttuazioni e default con maggiore accuratezza rispetto ai metodi tradizionali, supportando banche e assicurazioni nel prendere decisioni più informate. Anche il trading ha visto l'ascesa di sistemi algoritmici alimentati da IA, capaci di eseguire operazioni in microsecondi cogliendo opportunità altrimenti invisibili all'operatore umano. L'uso altamente diffuso dell'IA in finanza solleva però questioni di trasparenza e affidabilità: è essenziale infatti poter spiegare le decisioni automatiche che incidono su investimenti o concessione di credito, sia per motivi regolamentari sia per mantenere la fiducia degli utenti. Diverse normative di settore influenzano l'adozione di IA nei servizi finanziari: ad esempio, la Payment Services Directive 2 (PSD2) in Europa ha promosso standard più elevati di sicurezza e apertura nel banking digitale[7], mentre negli Stati Uniti il Dodd-Frank Wall Street Reform and Consumer Protection Act del 2010 impone requisiti di trasparenza e accountability alle istituzioni finanziarie, incoraggiando approcci prudenziali anche nell'uso di algoritmi intelligenti per la gestione del rischio[8].

---

6 Colapietro, C. (2019). *Il trattamento dei dati sanitari nell'era digitale: tra GDPR e intelligenza artificiale*. Giuffrè Editore. Le normative italiane si sono adeguate al GDPR, regolando in particolare l'uso dell'IA nel settore sanitario per garantire il rispetto della privacy dei pazienti.

7 European Union. (2015). *Direttiva (UE) 2015/2366* del Parlamento Europeo e del Consiglio, del 25 novembre 2015, sui servizi di pagamento nel mercato interno (PSD2). La PSD2 ha innalzato gli standard di sicurezza nei pagamenti digitali e promosso l'innovazione nei servizi finanziari europei.

8 *Dodd-Frank Wall Street Reform and Consumer Protection Act* (2010). Public Law 111-203, 124 Stat. 1376. La riforma Dodd-Frank ha introdotto maggiori requisiti di trasparenza e responsabilità nel settore finanziario statunitense, influenzando anche l'uso di algoritmi avanzati per la gestione del rischio.

c) Sicurezza informatica e Digital Forensics.

La Cybersecurity rappresenta uno dei campi in cui l'IA trova applicazioni tra le più importanti e immediatamente fruibili. Sistemi di monitoraggio basati su I.A. analizzano costantemente il traffico di rete e il comportamento degli endpoint (computer, dispositivi mobili, server) al fine di identificare in tempo reale tentativi d'intrusione o attività anomale indicative di una compromissione. Tecniche di apprendimento automatico permettono di rilevare malware sconosciuti, analizzandone il comportamento (anziché tramite firme già note), contribuendo a contrastare minacce avanzate come gli APT (Advanced Persistent Threats).

Nel campo della Digital Forensics, l'IA aiuta gli analisti a filtrare ed esaminare grandi volumi di dati alla ricerca di evidenze digitali: ad esempio, algoritmi possono estrarre automaticamente informazioni pertinenti da copie forensi di hard disk, recuperando elementi anche quando nascosti in mezzo a milioni di file, oppure ricostruire sequenze di eventi da log di sistema, accelerando indagini che richiederebbero mesi di lavoro manuale.

In Europa, la già citata Direttiva NIS 2 impone oggi agli operatori di servizi essenziali e a quelli di importanza critica l'adozione di standard ancora più elevati di sicurezza informatica. La NIS2 ha significativamente ampliato la platea dei soggetti obbligati, innalzato i livelli minimi di protezione e introdotto un sistema più stringente di vigilanza e sanzioni. Essa incentiva, tra l'altro, l'impiego di strumenti di intelligenza artificiale per la prevenzione, il monitoraggio e la risposta rapida agli incidenti, promuovendo l'integrazione di tecnologie predittive e adattive nella gestione del rischio cibernetico.

Un ulteriore tassello normativo di rilievo è il Regolamento eIDAS (Electronic Identification, Authentication and Trust Services), che garantisce validità legale ai documenti digitali e alle firme elettroniche: ciò implica che le prove raccolte attraverso procedure digitali, anche se supportate da algoritmi di IA, abbiano pieno riconoscimento giuridico e possano essere utilizzate nei procedimenti giudiziari, inclusi quelli di natura penale o contenziosa amministrativa[9]. A livello internazionale, la Convenzione di Budapest del Consiglio d'Europa fornisce un quadro normativo armonizzato per la raccolta, la conservazione e l'analisi delle prove digitali in ambito forense, facilitando la cooperazione transnazionale nelle indagini sui crimini informatici e nella cyber forensics[10].

---

9 European Union. (2014). *Regolamento (UE) n.910/2014* del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (Regolamento eIDAS). Il Regolamento eIDAS garantisce l'efficacia legale dei documenti e delle firme digitali, conferendo validità probatoria alle evidenze digitali anche nei procedimenti giuridici.

10 Council of Europe. (2001). *Convention on Cybercrime* (ETS No.185). Budapest. La Convenzione di Budapest definisce standard internazionali per contrastare i crimini informatici e facilita la

d) Voto elettronico.
Ecco che in un'epoca caratterizzata da crisi globali, come pandemie o conflitti, in grado d'impedire lo svolgimento tradizionale delle consultazioni elettorali, il voto elettronico sta emergendo come soluzione per garantire la continuità dei processi democratici. L'I.A. può quindi contribuire a migliorare la sicurezza e l'affidabilità dei sistemi di e-voting, ad esempio attraverso l'analisi dei log delle votazioni, per rilevare anomalie indicative di tentativi di broglio digitale, come pure per rafforzare i meccanismi di autenticazione degli elettori e prevenire accessi non autorizzati. Nell'Unione Europea, l'implementazione del voto elettronico è guidata dalle linee guida stabilite dal Codice di buona condotta elettorale della Commissione di Venezia, che definisce i principi fondamentali per garantire elezioni democratiche e trasparenti, incluso l'uso sicuro e verificabile delle tecnologie digitali nelle votazioni[11]. Sul piano internazionale, la Global Commission on the Stability of Cyberspace (GCSC) ha evidenziato l'urgenza di proteggere i processi elettorali digitali dalle minacce cibernetiche, invitando gli stati e le organizzazioni a adottare standard di sicurezza globali per salvaguardare l'integrità dei sistemi di voto elettronico[12].

1.4 Aspetti etici e normativi dell'I.A.

Lo sviluppo dell'IA è sempre stato accompagnato da un intenso dibattito etico e normativo. Ogni nuova ondata di progressi tecnologici in questo campo ha sollevato interrogativi su come garantire che l'I.A. venga utilizzata a beneficio della società nel rispetto dei principi etici condivisi[13]. Il contesto giuridico legato all'IA è altamente dinamico e si concentra in particolare sulla protezione dei dati personali e dei diritti degli individui. In Europa, il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nel 2018, ha stabilito un quadro stringente per il trattamento dei dati personali, con implicazioni dirette sulla progettazione e implementazione di sistemi di IA. Il GDPR richiede trasparenza,

---

cooperazione transnazionale nelle indagini digitali.

11 European Commission for Democracy through Law (Venice Commission). (2003). *Code of Good Practice in Electoral Matters*. Strasbourg: Council of Europe Publishing. Il Codice di buona condotta elettorale della Commissione di Venezia enuncia principi per assicurare elezioni democratiche e trasparenti, offrendo raccomandazioni anche sull'utilizzo sicuro di tecnologie elettroniche di voto.

12 Global Commission on the Stability of Cyberspace. (2020). *Advancing Cyber Stability: Final Report*. The Hague: GCSS. La GCSC sottolinea la necessità di proteggere i processi elettorali digitali dalle minacce cibernetiche e promuove l'adozione di standard globali di sicurezza per salvaguardare la democrazia nell'era digitale.

13 Floridi, L. (2021). *The Ethics of Artificial Intelligence*. Oxford University Press. Le questioni etiche sollevate dall'IA richiedono un approccio interdisciplinare: l'autore esamina come guidare lo sviluppo dell'IA in modo rispettoso dei principi morali e dei diritti umani fondamentali.

equità e responsabilità nella gestione dei dati, quali criteri fondamentali per tutelare i diritti dei cittadini nell'era digitale. Inoltre, introduce il concetto di privacy by design, imponendo che fin dalla fase di sviluppo gli algoritmi rispettino i principi di minimizzazione e sicurezza dei dati[14]. In linea con il GDPR, l'ordinamento italiano si è adeguato attraverso il D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018, recependo la normativa europea anche rispetto ai sistemi automatizzati, tra cui l'intelligenza artificiale. Inoltre, il Garante per la protezione dei dati personali ha pubblicato linee guida ad hoc sui profili di trasparenza algoritmica, profilazione e decisioni automatizzate, con particolare riguardo all'uso dell'IA in sanità e settore pubblico. Infine, sono state avviate iniziative normative e operative per favorire l'adozione responsabile dell'IA nelle pubbliche amministrazioni e nei servizi digitali[15]. Ciò è particolarmente rilevante in àmbiti ad alto rischio come quello sanitario, dove il trattamento di dati sensibili mediante I.A. deve rispettare rigorosi vincoli a garanzia della privacy e della sicurezza. Anche fuori dall'Europa l'attenzione del legislatore verso l'I.A. e i dati è crescente. Negli Stati Uniti, ad esempio, il California Consumer Privacy Act (CCPA) del 2018, ovvero una delle normative più avanzate in tema di privacy, conferisce ai cittadini californiani maggior controllo sui propri dati e impone alle aziende obblighi di trasparenza e responsabilità nel loro utilizzo[16]. Sebbene il CCPA non sia specifico sull'IA, la sua enfasi sulla protezione dei dati influenza anche le pratiche di sviluppo di sistemi I.A. orientati ai consumatori. In Brasile, la Lei Geral de Proteção de Dados (LGPD), entrata pienamente in vigore nel 2020, è l'omologo del GDPR europeo in uno dei più grandi paesi emergenti: anche questa legge disciplina in modo rigoroso il trattamento dei dati personali, con un impatto significativo sui progetti di I.A. che coinvolgono informazioni degli utenti[17]. Oltre alle leggi sulla privacy e sui dati, stanno nascendo normative specifiche per l'Intelligenza Artificiale. In Europa, l'AI Act è entrato in vigore il 1° agosto 2024 e dal 2 febbraio 2025 le prime norme – in particolare quelle

14 Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer. Il GDPR ha imposto un approccio rigoroso e trasparente alla gestione dei dati personali, influenzando profondamente la progettazione dei sistemi di IA soprattutto in termini di privacy e sicurezza.

15 Garante per la protezione dei dati personali (2022). *Linee guida su decisioni automatizzate e profilazione*. Documento di indirizzo del 14 luglio 2022, disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9782890 (consultato il 9 luglio 2025)

16 Determann, L. (2020). *California Privacy Law*. O'Reilly Media. Il CCPA rappresenta una delle normative più avanzate in materia di privacy dei dati dei consumatori e, pur non riferendosi esplicitamente all'IA, ne influenza lo sviluppo imponendo maggiore trasparenza e controllo nell'uso delle informazioni personali.

17 Monteiro, F. M. (2020). Lei Geral de Proteção de Dados Pessoais (LGPD): Uma análise crítica. *Revista de Direito da Proteção de Dados Pessoais e do Consumidor, 1*(1), 61–80. La LGPD brasiliana ricalca molti principi del GDPR, imponendo vincoli stringenti sul trattamento dei dati personali con effetti rilevanti anche sui progetti di IA a livello locale.

riguardanti pratiche inaccettabili e alfabetizzazione digitale – sono già applicate in UE[18]. Dal 2 agosto 2025 scattano le disposizioni relative ai modelli generali di IA (*GPAI*, quali GPT4, Gemini, LLaMA) – obblighi di trasparenza, analisi dei rischi e supervisione umana – mentre le norme su organismi notificati, governance e sanzioni saranno operative a partire da agosto 2025, con piena applicabilità delle regole per i sistemi ad alto rischio nel 2027. È previsto un Code of Practice volontario per i GPAI entro fine 2025 per facilitare la compliance[19]. Pur sotto pressione da parte di alcune aziende europee, la Commissione ha confermato che non sono previsti rinvii ufficiali, sebbene siano in discussione ipotesi di semplificazione normativa, soprattutto per le PMI[20]. In parallelo sono stati emanati importanti documenti etici non vincolanti, come le Linee guida per un'IA affidabile della Commissione Europea e i principi del Global Partnership on AI (GPAI), che promuovono best practice di sviluppo responsabile.

In conclusione, la governance etica e normativa dell'Intelligenza Artificiale, pur avendo compiuto passi decisivi con l'adozione dell'AI Act, in Europa resta un cantiere in evoluzione a livello globale. Mentre la tecnologia avanza rapidamente, istituzioni, legislatori e società civile lavorano per definire principi e regole in grado di massimizzare i benefici dell'IA riducendone i rischi. Il dialogo interdisciplinare tra tecnologi, giuristi, eticisti e policy maker è oggi più che mai essenziale per tracciare una rotta che concili innovazione, diritti fondamentali e responsabilità sociali.

18 European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final. Bruxelles. La proposta di AI Act costituisce un tentativo pionieristico di regolamentare l'IA in base ai rischi, introducendo requisiti di trasparenza e controllo umano per le applicazioni più delicate.

19 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, che stabilisce norme armonizzate sull'intelligenza artificiale (Artificial Intelligence Act), artt. 56–58. Il regolamento prevede l'elaborazione di un *Code of Practice* volontario per i modelli di intelligenza artificiale per finalità generali (GPAI), da svilupparsi con il coinvolgimento degli stakeholder e sotto il coordinamento della Commissione europea, con l'obiettivo di facilitare l'adeguamento progressivo agli obblighi normativi e supportare la compliance prima della piena applicazione delle disposizioni vincolanti.

20 Commissione europea, posizioni istituzionali espresse nel corso del processo di implementazione del Regolamento (UE) 2024/1689 (*Artificial Intelligence Act*). Pur in presenza di pressioni esercitate da parte di alcune imprese e associazioni industriali europee, la Commissione ha confermato l'assenza di rinvii ufficiali nell'entrata in applicazione del regolamento; al contempo, sono oggetto di valutazione ipotesi di semplificazione e misure di accompagnamento di natura non vincolante, con particolare attenzione alle esigenze delle piccole e medie imprese.

Capitolo 2
Intelligenza artificiale e Cybersecurity

2.1 Introduzione

Negli ultimi anni, l'evoluzione delle minacce informatiche, che si son fatte via via sempre più numerose, sofisticate e rapide, ha spinto verso l'adozione di strumenti di Intelligenza Artificiale (IA) a supporto della cybersecurity. I tradizionali approcci basati su regole statiche e intervento umano faticano infatti a tenere il passo con volumi di dati di log e segnali di attacco in costante crescita. In questo contesto, l'IA (in particolare il *machine learning* e le sue declinazioni quali il *deep learning*) offre la capacità di individuare pattern anomali e comportamenti malevoli all'interno di grandi moli di informazioni in tempo reale, migliorando la velocità e l'accuratezza delle difese informatiche[1]. Ad esempio, algoritmi di apprendimento automatico sono impiegati per analizzare il traffico di rete alla ricerca di intrusioni (IDS basati su ML), classificare file o processi per distinguere malware da software legittimo, riconoscere e-mail di *phishing* attraverso l'analisi del linguaggio, e molto altro. Queste applicazioni hanno dimostrato in diversi casi prestazioni superiori ai metodi tradizionali, grazie alla capacità dei modelli IA di *apprendere* caratteristiche sottili e non ovvie ai ricercatori umani[2].

L'adozione dell'IA in cybersecurity, dunque, rappresenta un cambio di paradigma: dall'approccio reattivo basato su firme statiche si passa a un approccio proattivo e adattivo, dove sistemi intelligenti apprendono continuamente dai dati per anticipare mosse degli attaccanti e rilevare anomalie prima che causino danni significativi.

2.2 Vantaggi e applicazioni dell'I.A. nella sicurezza informatica

L'integrazione dell'IA nei sistemi di difesa informatica comporta numerosi vantaggi. In primo luogo, i modelli IA eccellono nell'automazione di compiti ripetitivi e ad alta intensità di dati, alleggerendo il carico cognitivo degli analisti

1 Li, L. "Comprehensive Survey on Adversarial Examples in Cybersecurity: Impacts, Challenges, and Mitigation Strategies." *arXiv* preprint arXiv:2412.12217, 2024. Disponibile su: https://arxiv.org/abs/2412.12217 (link verificato l'8 luglio 2025).

2 Slavova, S. I. *Adoption of AI in Cybersecurity: Bridging the Gap Between Innovation and Application*. Master's Thesis, Delft University of Technology, 2024. Disponibile su: https://repository.tudelft.nl/record/uuid:68e7c879-2a84-490f-8a38-8459d626f93e (link verificato l'8 luglio 2025).

di sicurezza. Ad esempio, in un Security Operations Center (SOC) tipicamente giungono ogni giorno migliaia di allarmi: algoritmi di *machine learning* possono filtrare e correlare questi eventi, prioritizzando gli incidenti più critici e riducendo drasticamente i falsi allarmi che il team umano deve esaminare[3]. In secondo luogo, l'IA permette di rilevare minacce sconosciute (*zero-day*) attraverso l'individuazione di anomalie rispetto al comportamento atteso. In tal senso, modelli *unsupervised* o semi-supervised (come reti neurali autoencoders, clustering, ecc.) vengono addestrati sul normale traffico di rete o sul comportamento abituale di utenti e sistemi, segnalando eventuali deviazioni sospette che potrebbero indicare un'intrusione. Questo approccio, basato sul profilo comportamentale, arricchisce le difese oltre le tradizionali firme di attacco.

Un ulteriore campo di applicazione è l'analisi malware e threat intelligence: tecniche di *deep learning* (es. reti neurali convolutive o ricorrenti) sono utilizzate per classificare malware in famiglie, prevederne la pericolosità e persino generare indicatori di compromissione a partire da grandi database di codice malevolo già noto[4]. Ciò consente di automatizzare parte dell'analisi forense e di reagire più velocemente a nuove varianti di malware. Similmente, l'IA viene impiegata per identificare schemi ricorrenti nei tentativi di intrusione (ad esempio riconoscendo le sequenze di comandi o exploit tipiche di specifici gruppi APT) e per il *vulnerability management* (p.es. sistemi di *predictive analytics* che stimano quali vulnerabilità in un parco macchine sono più probabili bersagli di attacchi imminenti). In ambito di autenticazione e controllo degli accessi, algoritmi IA analizzano comportamenti anomali degli utenti (attraverso tecniche di *user behavior analytics*) identificando possibili compromissioni di account o uso malevolo di credenziali.

Dal punto di vista strategico, l'IA consente un cambio di passo, ovvero determina la transizione da una difesa statica a una difesa adattiva e in continua evoluzione. I modelli possono essere *addestrati continuamente* con dati aggiornati sulle nuove minacce emergenti, rendendo il sistema di sicurezza *dinamico*. Ad esempio, sistemi di *machine learning* all'interno di firewall o piattaforme di endpoint protection possono aggiornare i loro modelli in base ai nuovi attacchi rilevati in rete (approccio federato o centralizzato), migliorando progressivamente la capacità di riconoscere pattern malevoli. Questo apprendimento continuo contribuisce a colmare più rapidamente il *gap temporale* tra la comparsa di una nuova tecnica di attacco e l'implementazione di contromisure efficaci, aumentando la resilienza complessiva delle infrastrutture digitali.

---

3 Beg, O. A., Khan, A. A., Rehman, W. U., & Hassan, A. "A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids." *Energies*, vol. 16, no. 22, 2023, p. 7644. Disponibile su: https://www.mdpi.com/1996-1073/16/22/7644 (link verificato l'8 luglio 2025).

4 "Cybersecurity implications of using data with AI." *IT News (Indiana University)*, 30 settembre 2024. Disponibile su: https://news.iu.edu/it/live/news/37973-cybersecurity-implications-of-using-data-with-ai (link verificato l' 8 luglio 2025).

2.3 Casi di studio: approcci IA in contesti critici

Per illustrare in concreto l'impatto dell'IA applicata alla cybersecurity, di seguito si presentano due esempi emblematici in contesti critici, evidenziandone evoluzione e risultati.

Caso di studio 1. Finanza e attacchi phishing

Nel settore finanziario, bersaglio privilegiato di campagne di phishing e frodi informatiche, sono stati sviluppati sistemi basati su IA capaci di analizzare in tempo reale e-mail e transazioni sospette. Ad esempio, reti neurali addestrate su grandi insiemi di e-mail hanno permesso di raggiungere elevati tassi di riconoscimento di mail di phishing camuffate da comunicazioni bancarie, riducendo sensibilmente sia i falsi negativi (phishing non rilevato) sia i falsi positivi rispetto ai filtri tradizionali basati su parole chiave.

Parallelamente, algoritmi di *machine learning* vengono utilizzati nelle piattaforme antifrode per l'analisi delle transazioni finanziarie. Essi, cioè, sono in grado di apprendere i modelli di spesa legittimi dei clienti bloccando in automatico operazioni anomale, che potrebbero indicare un furto di credenziali o una compromissione (*account takeover*).

Tali soluzioni hanno mostrato efficacia nello sventare frodi in tempo reale, proteggendo conti correnti e carte di pagamento prima che il danno economico si materializzi. Inoltre, l'avvento di tecniche di *Natural Language Processing (NLP)* e di modelli linguistici avanzati ha aperto la strada ad assistenti virtuali di sicurezza (ad esempio chatbot intelligenti) che educano gli utenti nel riconoscere tentativi di phishing, aumentando la consapevolezza e la postura di sicurezza del personale non tecnico.

Caso di studio 2. Infrastrutture critiche e smart grid

Le infrastrutture elettriche e industriali rappresentano un ambito in cui l'IA sta giocando un ruolo crescente per prevenire attacchi cyber potenzialmente catastrofici. Basti pensare ai noti blackout in Ucraina nel 2015 e 2016, causati rispettivamente dai malware *BlackEnergy* e *Industroyer* che colpirono i sistemi SCADA della rete elettrica, lasciando al buio centinaia di migliaia di cittadini[5].

Simili incidenti hanno messo in luce la vulnerabilità dei sistemi di controllo industriale e la necessità di strumenti più avanzati per il monitoraggio di reti elettriche e impianti critici. In risposta, la comunità scientifica e gli operatori del settore hanno sviluppato soluzioni basate su IA per il rilevamento precoce di intrusioni nelle reti OT (*Operational Technology*). Ad esempio, sono stati

5 Balogh, Š., Mlynček, M., Vraňák, O., & Zajac, P. "Using Generative AI Models to Support Cybersecurity Analysts." *Electronics*, vol. 13, no. 23, 2024, p. 4718. Disponibile su: https://www.mdpi.com/2079-9292/13/23/4718 (link verificato il giorno 8 luglio 2025).

implementati sistemi di anomaly detection con reti neurali e modelli statistici nei centri di controllo elettrici che apprendono il normale profilo operativo (parametri elettrici, flussi di comunicazione tra sensori e attuatori, ecc.) e generano *allarmi immediati* non appena rilevano deviazioni anomale, potenzialmente indicative di un'attività ostile, come comandi malevoli inviati a interruttori di rete o falsi dati di telemetria immessi nei sistemi[6].

Studi recenti confermano l'efficacia di questi approcci: algoritmi di machine learning sono riusciti a individuare in simulazioni attacchi di *false data injection* o manomissione di logica industriale con un alto grado di precisione, permettendo di isolare le porzioni compromesse del sistema, prima che il guasto si propagasse[7]. Inoltre, l'IA non solo aiuta nel rilevamento, ma supporta la mitigazione e il ripristino: modelli predittivi possono stimare l'impatto di un attacco sul network elettrico e suggerire azioni correttive ottimali (ad es. riallocazione del carico su linee non affette), riducendo così il tempo di disservizio[8].

In sintesi, nel dominio delle infrastrutture critiche l'IA sta diventando un alleato fondamentale per incrementare la resilienza, poiché grazie alle capacità di apprendimento automatico, i sistemi di controllo diventano più consapevoli del proprio stato e più reattivi nel fronteggiare comportamenti anomali, contribuendo a evitare che gli attacchi cyber si traducano in gravi conseguenze fisiche o interruzioni di servizi essenziali.

2.4 Limiti e sfide dell'IA applicata alla cybersecurity

Sebbene le potenzialità dell'IA in ambito sicurezza siano notevoli, è fondamentale adottare uno sguardo critico ed evidenziare le limitazioni e i rischi connessi al suo utilizzo, per evitare valutazioni sbilanciate solo sugli aspetti positivi. In primo luogo, i sistemi basati su IA non sono infallibili e possono commettere errori di classificazione, ovvero falsi negativi (minacce reali non riconosciute) e falsi positivi (allarmi su eventi leciti). Si tratta di evenienze che continuano a verificarsi. Questi errori possono derivare da modelli addestrati su dati incompleti o non rappresentativi di tutte le casistiche. Se infatti un algoritmo d'intrusion detection è stato addestrato principalmente su attacchi di un certo

6 Xu, M., Fan, J., Huang, X., Zhou, C., Kang, J., Niyato, D., Mao, S., Han, Z., Shen, X., & Lam, K.-Y. "Forewarned is Forearmed: A Survey on Large Language Model-based Agents in Autonomous Cyberattacks." *arXiv* preprint arXiv:2505.12786, 2025. Disponibile su: https://arxiv.org/abs/2505.12786 (link verificato il 9 luglio 2025).

7 Mercer, S., & Watson, T. *Generative AI in Cybersecurity: Assessing Impact on Current and Future Malicious Software*. CETaS Briefing Paper, The Alan Turing Institute, 10 giugno 2024. Disponibile su: https://cetas.turing.ac.uk/publications/generative-ai-cybersecurity (link verificato il 9 luglio 2025).

8 Kshetri, N. "Transforming Cybersecurity with Agentic AI to Combat Emerging Cyber Threats." *Telecommunications Policy*, vol. 49, no. 6, 2025, p. 102976. Disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5159598 (link verificato il 9 luglio 2025).

tipo, potrebbe mancare di rilevare attacchi differenti e mai visti prima, oppure al contrario segnalare come malevoli attività lecite ma poco comuni.

Un problema correlato è quello dei bias algoritmici. I modelli IA possono cioè ereditare o amplificare pregiudizi presenti nei dati di addestramento, producendo decisioni distorte[9]. Ad esempio, se un dataset di sicurezza contiene principalmente esempi di attacchi provenienti da una certa regione geografica o eseguiti con determinate tecniche, il sistema potrebbe sovrastimare la pericolosità di eventi con quelle caratteristiche (*bias di conferma*) e sottostimare minacce atipiche che esulano dal profilo appreso. Ciò pone rischi sia di efficacia (vulnerabilità non rilevate), sia di equità e correttezza nelle azioni automatizzate intraprese dal sistema di sicurezza.

Un'altra criticità da considerare è la dipendenza dai dati, in quanto gli algoritmi di IA necessitano di grandi quantità di dati di qualità per addestrarsi. Nella cybersecurity spesso ottenere dati etichettati accuratamente è complesso (si pensi ai dataset di attacchi, che possono essere incompleti o classificati in modo ambiguo). Dati scarsi o rumorosi portano a modelli fragili, inclini all'overfitting o a decisioni errate quando sono messi di fronte a situazioni leggermente diverse da quelle viste in training. Inoltre, i sistemi di AI invecchiano man mano che le minacce evolvono. È dunque necessario un continuo *aggiornamento, un update* del modello (attraverso *re-training* periodico con nuovi dati) per evitare il concept drift, altrimenti l'efficacia del rilevamento cala col tempo.

Dal punto di vista operativo, una sfida cruciale è rappresentata dalla trasparenza e dalla spiegabilità delle decisioni prese dall'IA. Molti modelli avanzati (come le reti neurali profonde) sono delle "scatole nere" difficili da interpretare: in ambito sicurezza questo pone problemi nel momento in cui un sistema automatizzato dovesse, ad esempio, bloccare una transazione finanziaria o isolare un server critico. È fondamentale per gli analisti comprendere il perché di certe segnalazioni (ad es. quali caratteristiche hanno portato a classificare un file come malware) per poter validare l'allarme ed eventualmente intervenire. La mancanza di spiegabilità può minare la fiducia degli operatori verso l'IA e rallentarne l'adozione su vasta scala[10].

Per tali ragioni, si stanno sviluppando approcci di *Explainable AI (XAI)* per mitigare questo problema, ad esempio fornendo agli analisti descrizioni leggibili delle regole inferite dal modello o evidenziando le parti di input più rilevanti per la decisione. Si parla di feature importance.

---

9 Traynor, O. "Understanding DORA: What Financial Institutions Need to Know (2025)." *CybelAngel*, 17 marzo 2025. Disponibile su: https://cybelangel.com/dora-eu-financial-regulations-2025/ (link verificato il giorno 8 luglio 2025).

10 Chee, F. Y. "EU Sticks with Timeline for AI Rules." *Reuters*, 4 luglio 2025. Disponibile su: https://www.reuters.com/world/europe/artificial-intelligence-rules-go-ahead-no-pause-eu-commission-says-2025-07-04/ (link verificato il 9 luglio 2025).

Last but not least, va considerato che l'IA stessa può diventare bersaglio di attacchi da parte di attori malevoli. Una nuova classe di minacce, nota come *adversarial machine learning*, sfrutta infatti i punti deboli dei modelli di apprendimento automatico. Attraverso attacchi adversariali è possibile dunque manipolare gli input ai sistemi di AI per ingannarli. In pratica, gli attaccanti possono creare *esempi adversariali*, cioè dati appositamente alterati in modo quasi impercettibile, che tuttavia inducono il modello a compiere errori grossolani di classificazione[11]. Ad esempio, è stato dimostrato che aggiungendo un lieve "rumore" a un malware è possibile farlo passare inosservato a un classificatore automatizzato, o che inserendo specifiche sequenze di byte inutili in un file malevolo si può eludere un antivirus basato su rete neurale, senza compromettere la funzionalità del malware[12]. Analogamente, piccoli cambiamenti in pacchetti di rete o nelle chiamate API possono far sì che un IDS potenziato da IA non rilevi attività che altrimenti identificherebbe. Questi scenari evidenziano una sorta di "gara" tra difensori e attaccanti anche sul piano dell'IA, dal momento che ogni nuovo metodo di rilevamento basato su machine learning potrebbe stimolare la creazione di tecniche di evasione su misura per quel modello. La conseguenza è che l'efficacia di un sistema IA va valutata non solo in termini di metriche su dataset statici, ma anche rispetto alla robustezza agli attacchi adversariali nel mondo reale. La ricerca accademica sta esplorando contromisure come l'*adversarial training*, ovvero come fosse un vaccino, addestrando i modelli includendo esempi alterati per renderli più robusti, nonché algoritmi di difesa proattiva. Si tratta di un campo in continua e rapida evoluzione[13].

---

11 S. Biggio, F. Roli, *Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning*, Pattern Recognition, vol. 84, 2018, pp. 317–331; I. J. Goodfellow, J. Shlens, C. Szegedy, *Explaining and Harnessing Adversarial Examples*, International Conference on Learning Representations (ICLR), 2015. Gli attacchi adversarial consistono nella manipolazione intenzionale degli input mediante perturbazioni minime, spesso impercettibili all'occhio umano, ma sufficienti a indurre modelli di apprendimento automatico a produrre classificazioni errate o decisioni significativamente distorte, evidenziando vulnerabilità strutturali nei sistemi di IA.

12 H. S. Anderson, A. Kharkar, B. Filar, P. Roth, D. Evans, *Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning*, in Proceedings of the 2017 Workshop on Artificial Intelligence and Security (AISec), ACM, 2017; F. Pierazzi, F. Pendlebury, J. Cortellazzi, L. Cavallaro, *Intriguing Properties of Adversarial Malware Attacks*, IEEE Security & Privacy Workshops, 2018. È stato dimostrato che l'introduzione di perturbazioni minime, quali l'aggiunta di rumore controllato o di sequenze di byte semanticamente irrilevanti, consente di eludere modelli di classificazione automatizzata e sistemi antivirus basati su reti neurali, senza alterare il comportamento funzionale del malware, mettendo in luce limiti intrinseci dei meccanismi di rilevamento basati esclusivamente su apprendimento automatico.

13 I. J. Goodfellow, J. Shlens, C. Szegedy, *Explaining and Harnessing Adversarial Examples*, International Conference on Learning Representations (ICLR), 2015; A. Madry, A. Makelov, L. Schmidt, D. Tsipras, A. Vladu, *Towards Deep Learning Models Resistant to Adversarial Attacks*, International Conference on Learning Representations (ICLR), 2018. La letteratura ha evidenziato come le metriche di accuratezza calcolate su dataset statici non siano sufficienti a valutare l'affidabilità dei sistemi di intelligenza artificiale in contesti operativi reali, proponendo

Infine, considerazioni etiche e giuridiche sull'uso dell'IA non possono non essere contemplate in decisioni di sicurezza, come a dire che affidare a un algoritmo scelte che possono impattare sugli utenti (es. blocco di account, segnalazione alle autorità di comportamenti sospetti) richiede necessariamente garanzie sul rispetto dei diritti e delle libertà individuali. È importante assicurare che i sistemi di cyber-defence automatizzati operino con imparzialità e in conformità con le normative sulla protezione dei dati e non producano conseguenze discriminatorie o ingiuste a causa di errori algoritmici. In quest'ottica, un bilanciamento tra automazione e supervisione umana rimane essenziale, con l'IA che dovrebbe pur sempre agire come *forza moltiplicatrice* per potenziare gli analisti, ma non come sostituto incontrollabile. Un approccio graduale, che preveda validazione umana per gli interventi più critici e una continua verifica delle performance del modello, consente di sfruttare i benefici dell'IA mantenendo il controllo sui suoi output.

2.5 Evoluzioni recenti e tendenze emergenti

In questa sezione si evidenziano i più recenti sviluppi tecnologici e di scenario (aggiornati al 2025) e che stanno plasmando il ruolo dell'IA nella cybersecurity.

IA generativa e Large Language Model (LLM) per la difesa

Una delle novità più dirompenti dell'ultimo periodo è l'applicazione dei modelli linguistici di grandi dimensioni (*Large Language Models*, come GPT-4 e simili) alle operazioni di sicurezza informatica. Questi modelli, originariamente sviluppati per comprendere e generare linguaggio naturale, si sono rivelati utili come assistenti intelligenti per i team di cybersecurity. Ad esempio, recenti studi hanno mostrato che chatbot avanzati basati su LLM possono aiutare gli analisti in compiti come la *revisione di configurazioni*, l'analisi di *log* e persino l'individuazione di vulnerabilità in applicazioni, fornendo suggerimenti e riassunti automatici delle informazioni di sicurezza[14]. In un caso, un LLM è stato impiegato con

approcci di *adversarial training* e di difesa proattiva finalizzati a migliorare la robustezza dei modelli rispetto a perturbazioni intenzionali. Il settore è caratterizzato da un'elevata dinamicità, con un continuo confronto tra nuove tecniche di attacco e strategie di mitigazione.

14 M. Bommasani et al., *On the Opportunities and Risks of Foundation Models*, Stanford Center for Research on Foundation Models, 2022; E. Athiwaratkun, C. A. Chen, J. Kang et al., *Large Language Models for Cybersecurity: Opportunities, Challenges, and Limitations*, arXiv preprint, 2023; S. Pearce, A. Ahmad, B. Tan et al., *Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions*, IEEE Symposium on Security and Privacy, 2022. Studi recenti indicano che i modelli linguistici di grandi dimensioni (LLM), pur nati per compiti di comprensione e generazione del linguaggio naturale, possono supportare i team di cybersecurity in attività quali l'analisi di log, la revisione di configurazioni, la sintesi di informazioni di sicurezza e l'individuazione preliminare di vulnerabilità applicative, agendo come strumenti di assistenza e supporto decisionale piuttosto che come sostituti dell'analisi umana.

successo per esaminare il codice di applicazioni Android alla ricerca di potenziali vulnerabilità e per riassumere grandi file di registro di sistema evidenziando solo le anomalie più rilevanti per l'indagine.

L'adozione di LLM come *copiloti* negli strumenti di sicurezza (ad esempio integrati in piattaforme SIEM/SOAR) promette di aumentare l'efficienza operativa, velocizzando attività che richiederebbero ore e ore di lavoro umano, come ad esempio leggere migliaia di righe di log, consentendo di scalare le capacità del SOC, senza moltiplicare linearmente il personale.

Tuttavia, va anche riconosciuto che questi sistemi presentano criticità specifiche: i LLM attuali operano come *modelli a scatola nera* e soffrono di limiti nel contesto (finestra di testo limitata) e possibili *allucinazioni* o errori fattuali. Gli esperimenti condotti evidenziano che, se da un lato, un chatbot può fornire spiegazioni rapide su un potenziale *bug* di sicurezza, dall'altro può tralasciare dettagli cruciali o, peggio, restituire indicazioni sbagliate con eccessiva sicurezza[15]. Problemi pratici come la lunghezza massima del prompt (contesto) e i costi computazionali delle richieste avanzate ne limitano per ora l'uso su scala massiva nei SOC[16]. Si tratta comunque di un ambito in rapido progresso, poiché i produttori stanno già lavorando su versioni di LLM ottimizzate per i dati tecnici e sulle integrazioni con strumenti di sicurezza esistenti. Nel frattempo, è raccomandato usare questi assistenti come *supporto* e non come fonti di verità assoluta, mantenendo un esperto umano all'interno del ciclo decisionale per verificare i risultati prodotti.

Uso duale dell'IA generativa, ovvero difensori VS attaccanti

Parallelamente ai vantaggi per i "buoni", l'IA generativa sta aprendo nuove possibilità anche per gli attori malevoli, delineando così un potenziale dual use della tecnologia. Da un lato, i defender possono sfruttare modelli generativi

15 S. Pearce, A. Ahmad, B. Tan et al., *Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions*, IEEE Symposium on Security and Privacy, 2022; N. Carlini, M. Jagielski, A. Oprea et al., *Poisoning Web-Scale Training Datasets Is Practical*, IEEE Symposium on Security and Privacy, 2023; A. Ghassemi, S. Suresh, S. Reddy, *The False Promise of Explainable AI for Cybersecurity*, IEEE Security & Privacy, vol. 20, n. 6, 2022. La letteratura empirica evidenzia come sistemi conversazionali basati su modelli linguistici di grandi dimensioni possano fornire spiegazioni rapide e apparentemente plausibili su problemi di sicurezza, ma al contempo presentino rischi di incompletezza, errori fattuali o *overconfidence*, con potenziali implicazioni negative in contesti operativi sensibili se non adeguatamente supervisionati.

16 A. Athiwaratkun, C. A. Chen, J. Kang et al., *Large Language Models for Cybersecurity: Opportunities, Challenges, and Limitations*, arXiv preprint, 2023; OpenAI, *GPT-4 Technical Report*, 2023; ENISA, *Artificial Intelligence Cybersecurity Challenges*, 2023. Studi recenti evidenziano come vincoli tecnici quali la limitata finestra di contesto (*context window*), la latenza delle richieste complesse e i costi computazionali associati all'uso intensivo di modelli linguistici di grandi dimensioni rappresentino, allo stato attuale, fattori limitanti per un impiego sistematico e su larga scala nei contesti operativi dei Security Operations Center, in particolare per attività ad alta frequenza e in tempo reale.

per potenziare le difese (si pensi alla generazione di *dataset* sintetici di attacchi per addestrare meglio i rilevatori, o alla simulazione automatizzata di scenari di attacco per testare le contromisure). Dall'altro, però, gli aggressori informatici hanno iniziato a impiegare strumenti di IA generativa per aumentare la sofisticazione e l'efficacia dei propri attacchi. Un esempio concreto è l'uso di LLM per automazione dell'hacking. Al riguardo recentissime ricerche hanno dimostrato che modelli di ultima generazione possono autonomamente assistere in task offensivi complessi, dal trovare, ad esempio, exploit in codice, fino alla preparazione di campagne di *phishing* mirato, riducendo drasticamente la necessità di abilità specialistiche da parte dell'attaccante umano[17]. In pratica, strumenti come *PentestGPT* o agenti basati su GPT-4 consentono a un attore con competenze limitate di eseguire penetration test automatizzati contro un bersaglio. Alcuni prototipi hanno raggiunto accesso a sistemi vulnerabili nel giro di pochi minuti e con costi irrisori, laddove un attacco manuale avrebbe richiesto giorni di lavoro esperto[18]. Ciò ha portato gli esperti a coniare il termine *Cyber Threat Inflation* per indicare l'aumento di scala degli attacchi reso possibile dall'IA con i costi operativi per lanciare campagne malevole che calano, mentre la loro portata e frequenza aumenta esponenzialmente[19].

---

17 P. Lin, J. Moss, R. N. L. Chia et al., *Measuring and Mitigating the Risk of AI-Assisted Cyber Attacks*, arXiv preprint, 2024; M. Goldstein, A. K. Jones, *Generative AI and the Democratization of Cyber Offense*, Journal of Cybersecurity, vol. 10, n. 1, 2024; OpenAI, *Preparedness Framework and Red Teaming Insights*, 2023. Ricerche recenti indicano che modelli di intelligenza artificiale di ultima generazione sono in grado di supportare, in modo sempre più autonomo, attività offensive complesse quali l'analisi di codice vulnerabile, l'assistenza nella scoperta di exploit e la generazione di contenuti per campagne di phishing altamente mirate. Tali capacità, pur variabili in funzione dei controlli implementati e dei contesti di utilizzo, contribuiscono a ridurre significativamente la barriera di competenze tecniche tradizionalmente richieste agli attaccanti umani, sollevando rilevanti questioni di sicurezza e governance.

18 J. Deng, Z. Zhang, Y. Liu et al., *PentestGPT: An LLM-Driven Autonomous Penetration Testing Framework*, arXiv preprint, 2023; Y. Xie, J. Kang, E. Athiwaratkun et al., *Agent-Based Large Language Models for Cybersecurity Tasks*, arXiv preprint, 2024; OpenAI, *GPT-4 System Card*, 2023. La letteratura sperimentale e i prototipi di ricerca mostrano come strumenti di penetration testing assistiti o orchestrati da modelli linguistici di grandi dimensioni possano automatizzare fasi significative delle attività di assessment offensivo, riducendo tempi e costi rispetto agli approcci manuali tradizionali. Tali risultati, ottenuti in ambienti controllati e con finalità di ricerca o difensive, evidenziano una potenziale riduzione della barriera di competenze necessarie, con rilevanti implicazioni in termini di sicurezza, controllo e governance dell'uso di sistemi di IA avanzata.

19 ENISA, *Threat Landscape for Artificial Intelligence*, 2023; M. Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, arXiv preprint, 2018; P. Lin, J. Moss, R. N. L. Chia et al., *Measuring and Mitigating the Risk of AI-Assisted Cyber Attacks*, arXiv preprint, 2024. Con l'espressione *Cyber Threat Inflation* alcuni analisti e ricercatori descrivono l'effetto di amplificazione sistemica delle minacce informatiche indotto dall'adozione di tecniche di intelligenza artificiale, caratterizzato da una significativa riduzione dei costi operativi per l'avvio di campagne malevole e, al contempo, da un aumento della loro scala, frequenza e capacità

Diversi sono i settori di attività offensiva che stanno andando incontro a questa trasformazione, fra cui il phishing avanzato, malware ed exploit, attacchi autonomi multi-stadio. Per quanto riguarda ad esempio le forme di phishing avanzato, grazie a modelli generativi di testo e voce, diventa banale creare e-mail e messaggi perfettamente personalizzati e credibili (*spear phishing* potenziato da IA) o simulare la voce di un CEO per truffare un'azienda (*vishing* con voce sintetica).

Nel camp dei malware e degli exploit, sebbene attualmente gli LLM non siano ancora in grado di scrivere un *malware* sofisticato da zero senza guida (non si è osservato infatti un aumento di nuovo malware "autonomo" dopo l'uscita di GPT-4[20]), possono ugualmente fornire *assistenza* nel generare porzioni di codice malevolo o nel trovare combinazioni di exploit noti, velocizzando lo sviluppo di nuove varianti. Inoltre, si prospetta che con l'ulteriore evoluzione, l'IA possa in futuro identificare autonomamente vulnerabilità *zero-day* e sfruttarle, compito questo che oggi richiede ancora l'ingegno umano[21]. Infine, per quanto concerne gli attacchi autonomi multi-stadio, uno scenario preoccupante delineato dalla ricerca è quello di agenti malevoli completamente autonomi che conducono l'intera catena d'attacco dalla ricognizione, passando per infiltrazione fino alla fase di esfiltrazione, senza intervento umano, se non per definire obiettivi generici. Esperimenti come *Project Naptime* di Google hanno mostrato che già oggi un LLM ben istruito può svolgere in sequenza operazioni di scanning, exploitation e movimento laterale con minima supervisione[22].

---

di personalizzazione, con implicazioni rilevanti per la sicurezza collettiva e la governance del rischio.

20 ENISA, *Threat Landscape 2023*; Europol, *ChatGPT – The Impact of Large Language Models on Law Enforcement*, 2023; OpenAI, *GPT-4 System Card*, 2023. Le analisi empiriche condotte da organismi istituzionali e comunità di ricerca indicano che, allo stato attuale, i modelli linguistici di grandi dimensioni non mostrano capacità di generare autonomamente malware complesso e operativo senza una significativa supervisione umana. In particolare, non sono stati osservati incrementi statisticamente rilevanti nella comparsa di nuove famiglie di malware attribuibili a processi di generazione pienamente automatizzata successivi all'introduzione di modelli di ultima generazione, quali GPT-4, suggerendo che il ruolo dell'IA rimanga prevalentemente quello di strumento di supporto piuttosto che di agente offensivo autonomo.

21 M. Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, arXiv preprint, 2018; P. Lin, J. Moss, R. N. L. Chia et al., *Measuring and Mitigating the Risk of AI-Assisted Cyber Attacks*, arXiv preprint, 2024. La ricerca prospettica evidenzia come, con l'evoluzione delle capacità di apprendimento automatico e di analisi automatizzata del codice, sistemi di IA potrebbero in futuro supportare o automatizzare l'individuazione e lo sfruttamento di vulnerabilità zero-day, attività che allo stato attuale richiede ancora competenze umane altamente specialistiche.

22 Google DeepMind, *Project Naptime: Evaluating LLMs for Autonomous Cybersecurity Tasks*, technical report, 2024; J. Deng, Z. Zhang, Y. Liu et al., *PentestGPT: An LLM-Driven Autonomous Penetration Testing Framework*, arXiv preprint, 2023. Esperimenti condotti in ambienti controllati mostrano che modelli linguistici di grandi dimensioni opportunamente istruiti possono eseguire in sequenza attività quali ricognizione, scanning, exploitation e movimento laterale

Questa asimmetria ridotta tra difensori e aggressori impone dunque un cambio di strategia. Se tradizionalmente la difesa godeva del fatto che attacchi sofisticati richiedevano risorse e competenze non comuni (limitate a Stati-nazione o gruppi APT avanzati), ora anche singoli criminali potrebbero attingere a "capacità di attacco as-a-service" fornite dall'IA, incrementando il numero di attacchi mirati in circolazione[23]. Per i difensori, questo significa dover fronteggiare un panorama di minacce amplificato e in rapida evoluzione, sarà quindi necessario adottare a propria volta soluzioni di IA più sofisticate e collaborative per mantenere un vantaggio, si pensi ad esempio a forme di condivisione di intelligence in tempo reale e a modelli difensivi che imparano dagli attacchi osservati su scala globale. Si prospetta in sostanza una sorta di "corsa agli armamenti" algoritmica: futuri malware generati dall'IA potrebbero essere contrastati efficacemente solo da altre IA di difesa, in un ciclo di miglioramento continuo reciproco[24].

Già oggi alcune aziende sperimentano accoppiate di *attaccante IA vs difensore IA* nei propri ambienti simulati, sia per testare le proprie difese sia per allenare i modelli di detection a riconoscere le tecniche di evasione elaborate da agenti automatici.

Agenti autonomi e AI *agentica* nei SOC

Un altro trend di grande interesse è lo sviluppo di agenti AI autonomi capaci di operare *all'interno* del Security Operations Center, interagendo con sistemi e flussi di lavoro in modo sempre più indipendente. L'idea di fondo è passare dall'IA come semplice assistente, che fornisce suggerimenti all'analista umano, a un'IA con ruoli pro-attivi, in grado, ad esempio, di prendere decisioni di primo livello sugli incidenti o orchestrare automaticamente risposte a minacce note. La cosiddetta *agentic AI* applicata alla cybersecurity mira proprio ad automatizzare i compiti critici nel SOC – *detection*, analisi e *incident response* – attraverso agenti

con supervisione minima, delineando scenari di attacchi multi-stadio condotti da agenti artificiali parzialmente autonomi.

23 ENISA, *Threat Landscape for Artificial Intelligence*, 2023; Europol, *ChatGPT – The Impact of Large Language Models on Law Enforcement*, 2023. L'adozione di strumenti di intelligenza artificiale in ambito offensivo contribuisce a ridurre la tradizionale asimmetria tra attaccanti e difensori, abbassando la soglia di competenze e risorse necessarie per condurre attacchi mirati e favorendo la diffusione di modelli di *attack-as-a-service* accessibili anche a singoli criminali o gruppi non altamente specializzati.

24 S. Russell, D. Dewey, M. Tegmark, *Research Priorities for Robust and Beneficial Artificial Intelligence*, AI Magazine, vol. 36, n. 4, 2015; M. Brundage et al., *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*, arXiv preprint, 2020. Diversi studiosi descrivono l'attuale evoluzione come una forma di "corsa agli armamenti" algoritmica, in cui tecniche offensive e difensive basate su IA tendono a co-evolvere, rendendo necessario l'impiego di sistemi di difesa intelligenti capaci di apprendere continuamente dalle minacce osservate su scala globale.

software che agiscono a vari livelli[25]. In un tale scenario è dunque possibile immaginare un futuro prossimo in cui, rilevato un alert di malware su un host, un agente autonomo verifichi immediatamente l'attendibilità dell'allarme, isoli il dispositivo dalla rete, raccolga evidenze forensi essenziali e avvii le contromisure (ad es. pulizia o patch), senza attendere l'intervento umano. Ciò ridurrebbe i tempi di reazione praticamente a zero, limitando i danni potenziali di un attacco. Secondo alcune analisi, l'adozione graduale di agenti autonomi potrebbe aumentare l'efficienza operativa dei SOC di un ordine di grandezza entro pochi anni. Ad esempio, Gartner prevede che entro il 2026 l'automazione intelligente potrebbe coprire fino al 50% delle attività di triage oggi svolte manualmente dagli analisti. Tuttavia, siamo ancora nelle fasi iniziali. A detta degli esperti, infatti, c'è un divario tecnologico da colmare prima di arrivare a agenti completamente autonomi e affidabili in ambienti complessi[26]. Le sfide riguardano tanto la complessità tecnica, in quanto sviluppare modelli che comprendano il contesto aziendale e che sappiano adattarsi a situazioni impreviste nonché apprendere da feedback in produzione è complesso, quanto la governance (ovvero, definire limiti chiari all'azione autonoma dell'IA, prevenire scenari fuori controllo e garantire che gli agenti seguano politiche di sicurezza e conformità).

Ad ogni modo, la direzione è tracciata. Già oggi vediamo nascere soluzioni di orchestrazione automatizzata che integrano playbook dinamici e moduli di decisione AI-driven. Un possibile approccio è implementare team ibridi uomo-macchina, in cui agenti autonomi svolgono h24 i compiti di monitoraggio di routine e reazione a eventi noti, mentre gli operatori gestiscono i casi più complessi e forniscono supervisione. Questo modello sfrutta il meglio di entrambi, da un lato la velocità instancabile delle macchine, dall'altro il giudizio esperto umano per i dilemmi non codificati.

In conclusione, gli *autonomous SOC agents* rappresentano un orizzonte d'innovazione assolutamente promettente perché, se sviluppati e impiegati con le dovute cautele, potrebbero rivoluzionare realmente il modo in cui contrastiamo le minacce digitali, portando a infrastrutture capaci di difendersi *quasi* da sole dagli attacchi più comuni.

---

25 Gartner, *Top Trends in Security Operations*, 2024; A. Athiwaratkun, C. A. Chen, J. Kang et al., *Large Language Models for Cybersecurity: Opportunities, Challenges, and Limitations*, arXiv preprint, 2023. Con il termine *agentic AI* applicata alla cybersecurity si fa riferimento a sistemi software autonomi in grado di percepire eventi, prendere decisioni e agire all'interno dei processi del Security Operations Center, automatizzando fasi critiche quali detection, analisi e risposta agli incidenti.

26 ENISA, *Artificial Intelligence Cybersecurity Challenges*, 2023; NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, 2023. Nonostante i progressi, gli esperti sottolineano l'esistenza di un significativo divario tecnologico e di governance prima di poter adottare agenti completamente autonomi in ambienti complessi, evidenziando criticità legate alla comprensione del contesto operativo, all'adattamento a scenari imprevisti, alla supervisione umana e alla definizione di limiti chiari all'azione autonoma dei sistemi di IA.

2.6 Evoluzione normativa recente e adeguamento giuridico

Accanto alle evoluzioni tecnico-operative, anche il quadro normativo in materia di IA e cybersecurity ha visto importanti aggiornamenti nel periodo 2022–2025.

Il legislatore, sia a livello europeo sia nazionale, sta intervenendo per regolamentare l'impiego dell'Intelligenza Artificiale e rafforzare la resilienza cibernetica dei settori critici, imponendo standard e obblighi che incidono direttamente sulle tematiche discusse in questo capitolo. Di seguito si richiamano i principali provvedimenti normativi recenti rilevanti.

- Regolamento UE "AI Act" (Artificial Intelligence Act): si tratta del primo quadro normativo europeo interamente dedicato all'Intelligenza Artificiale, basato su un approccio di regolamentazione proporzionale al rischio dei sistemi IA. Il Regolamento vieta alcune applicazioni considerate inaccettabili, come i sistemi di sorveglianza generalizzata o la manipolazione cognitiva, e sottopone i sistemi ad alto rischio (ad esempio quelli utilizzati per il reclutamento, l'istruzione, il credito, l'applicazione della legge o l'infrastruttura critica) a requisiti rigorosi di trasparenza, robustezza e accountability. Sebbene l'AI Act non tratti esplicitamente la cybersecurity come ambito autonomo, le sue disposizioni impatteranno significativamente anche sugli strumenti di IA impiegati in scenari di sicurezza, soprattutto se utilizzati per valutare comportamenti umani, individuare minacce o prendere decisioni automatizzate suscettibili di ledere diritti fondamentali.
- Dal punto di vista temporale, la Commissione Europea ha confermato che il Regolamento seguirà la roadmap senza rinvii:
  - dal 2 febbraio 2025 sono in vigore le norme relative ai sistemi IA vietati e le disposizioni istitutive degli organismi di supervisione nazionali;
  - dal 2 agosto 2025 scatteranno gli obblighi per i modelli di IA per finalità generali (General Purpose AI, inclusi i foundation model);
  - dal 2 agosto 2026 si applicheranno le norme per i sistemi ad alto rischio. Inizialmente previsto per maggio 2025, il Codice di buone pratiche destinato a supportare le imprese nell'implementazione delle regole è stato posticipato e, secondo quanto annunciato dalla Commissione, sarà verosimilmente pubblicato entro la fine del 2025. Questo calendario graduale mira a garantire una transizione ordinata e a fornire agli operatori del settore il tempo necessario per conformarsi alle nuove disposizioni, segnando però l'avvio concreto dell'era di regolamentazione dell'intelligenza artificiale in Europa.
- Regolamento UE "DORA" (Digital Operational Resilience Act): adottato a fine 2022, è entrato formalmente in vigore il 16 gennaio 2023 ed

è divenuto applicabile dal 17 gennaio 2025[27]. Si tratta di una normativa specifica per il settore finanziario, volta a garantire la resilienza operativa digitale di banche, assicurazioni, società di investimento e altri operatori finanziari. In pratica, DORA impone a questi soggetti requisiti rigorosi di gestione del rischio ICT, continuità operativa, risposta agli incidenti cyber e governance dei fornitori tecnologici. L'innovazione consiste nella creazione di un quadro unico e vincolante, mentre in precedenza esistevano solo linee guida frammentarie, che obbligavano le istituzioni finanziarie a testare periodicamente le proprie difese cyber, a notificare gli incidenti significativi alle autorità e a controllare i rischi derivanti da terze parti ICT[28]. Per quanto attiene all'IA, DORA incoraggia l'uso di tecnologie avanzate (come l'automazione e l'intelligenza artificiale), purché queste rispettino standard di sicurezza e siano incluse nei piani di resilienza. Ad esempio, una banca che utilizza sistemi IA per il monitoraggio di transazioni dovrà assicurare che questi sistemi siano robusti, auditabili e contemplati nelle strategie di continuità operativa. In sintesi, dal 2025 il settore finanziario UE opera sotto uno stringente regime di cyber-resilienza, in cui l'uso di IA va di pari passo con l'accountability e il rispetto di criteri normativi pensati per mitigare i rischi tecnologici sistemici.

– Direttiva UE "NIS2" (Direttiva 2022/2555 sulla sicurezza delle reti e dell'informazione): evoluzione rafforzata della prima direttiva NIS del 2016, la NIS2 è entrata ufficialmente in vigore nel gennaio 2023, con obbligo di recepimento negli ordinamenti nazionali entro il 17 ottobre 2024. Nel momento attuale, ovvero a luglio 2025, quasi tutti gli Stati membri hanno completato l'integrazione della direttiva nelle rispettive legislazioni, avviando le prime applicazioni concrete e controlli di conformità. Obiettivo della NIS2 è innalzare il livello complessivo di resilienza e sicurezza informatica in Europa, ampliando in modo significativo il campo di applicazione rispetto alla precedente normativa. Essa si estende infatti a diciotto settori critici, tra cui energia, trasporti, sanità, infrastrutture digitali, pubblica amministrazione (centrale e locale), servizi postali e di consegna, produzione di dispositivi critici, acque, spazio, gestione dei rifiuti e

27 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, relativo alla resilienza operativa digitale per il settore finanziario (*Digital Operational Resilience Act – DORA*). Il regolamento è entrato in vigore il 16 gennaio 2023 ed è divenuto applicabile dal 17 gennaio 2025, introducendo un quadro normativo vincolante per la gestione del rischio ICT e la resilienza cyber degli operatori finanziari dell'Unione.

28 Autorità Bancaria Europea (EBA), *Guidelines on ICT and Security Risk Management*, 2022; Commissione europea, documentazione applicativa sul Regolamento (UE) 2022/2554. DORA impone obblighi armonizzati di testing periodico, gestione degli incidenti, governance dei fornitori ICT e notifica alle autorità competenti, superando il precedente approccio frammentato basato su linee guida non vincolanti e rafforzando l'accountability degli operatori finanziari.

industria alimentare, coinvolgendo oltre 100.000 entità pubbliche e private in tutta l'Unione. La direttiva introduce obblighi chiari, vincolanti e armonizzati a livello europeo, tra cui:

- adozione di misure tecniche e organizzative adeguate e commisurate al rischio;
- nomina obbligatoria di un referente interno per la sicurezza delle informazioni;
- notifica degli incidenti significativi entro 24 ore dall'identificazione alle autorità nazionali competenti;
- obbligo di audit, formazione e valutazione della catena di fornitura.

Le sanzioni per inadempienza sono state armonizzate e rese più incisive, prevedendo fino a 10 milioni di euro o il 2% del fatturato annuo mondiale, a seconda di quale importo sia maggiore. Inoltre, la NIS2 promuove una cooperazione rafforzata tra gli Stati membri attraverso organismi e reti quali il CSIRTs Network e l'EU-CyCLONe, mirati allo scambio strutturato di informazioni sulle minacce e alla gestione coordinata delle crisi cyber su scala europea.

Sebbene la direttiva non menzioni esplicitamente l'intelligenza artificiale, essa favorisce indirettamente l'adozione di soluzioni IA in ambito sicurezza, in quanto tali tecnologie possono risultare essenziali per il rilevamento tempestivo, l'analisi e la risposta agli incidenti. Tuttavia, l'impiego dell'IA in questo contesto deve avvenire in modo trasparente, controllabile e conforme, assicurando che gli algoritmi non introducano nuove vulnerabilità o comportamenti opachi, potenzialmente in contrasto con i principi di accountability richiesti dalla normativa.

Il biennio 2024–2025 segna dunque un allineamento tra progresso tecnologico e contesto normativo. Mentre l'I.A. rivoluziona gli strumenti a disposizione di difensori e attaccanti nel dominio cyber, l'ordinamento giuridico europeo si sta attrezzando con nuove regole per governare tali trasformazioni.

Per professionisti e studiosi del diritto della tecnologia diventa fondamentale mantenere uno sguardo aggiornato su entrambi i fronti, sia tecnico che legale, così da garantire che l'innovazione in ambito cybersecurity proceda in modo responsabile, etico e conforme alle normative, massimizzando i benefici dell'IA e minimizzandone al contempo i potenziali rischi per individui e organizzazioni[29].

29 Commissione europea, Regolamento (UE) 2024/1689 (*Artificial Intelligence Act*); Direttiva (UE) 2022/2555 (*NIS2*); ENISA, *Cybersecurity and AI – Policy and Governance Perspectives*, 2024. Il periodo 2024–2025 segna un progressivo allineamento tra innovazione tecnologica e intervento normativo, imponendo a professionisti e studiosi di integrare competenze tecniche e giuridiche per garantire che l'adozione dell'intelligenza artificiale in ambito cybersecurity avvenga in modo responsabile, conforme e orientato alla mitigazione dei rischi sistemici.

PARTE II
IL VOTO ELETTRONICO E ONLINE

Capitolo 3
L'evoluzione del voto elettronico: storia, tipologie e implementazioni globali

3.1 Introduzione al voto elettronico e online

Il voto elettronico, inteso come qualsiasi sistema elettorale in cui l'espressione o il conteggio dei voti avviene mediante tecnologie digitali, rappresenta una delle più significative innovazioni nel campo della partecipazione democratica. Esso si colloca nel più ampio contesto della cosiddetta democrazia digitale, ossia nel momento in cui l'impiego delle tecnologie dell'informazione e della comunicazione è introdotto per supportare e potenziare i processi democratici[1].

Le aspettative nei confronti del voto elettronico sono state elevate sin dagli albori: da un lato, esso prometteva di rendere le operazioni di voto più efficienti, rapide e accessibili, aprendo la strada a una partecipazione più ampia dei cittadini, in particolare di coloro che incontrano difficoltà con le modalità tradizionali[2]. D'altro canto, studiosi e addetti ai lavori mettevano presto in luce le potenziali criticità e i rischi insiti nell'affidare a macchine e software il cuore dei meccanismi elettorali[3]. In altri termini, il voto elettronico è in grado di fare grandi promesse, mentre contemporaneamente sa anche minacciare grandi pericoli per la democrazia digitale.

Come sintetizzato efficacemente da Alvarez et al. (2008), all'aumento di comodità e potenzialmente di partecipazione, fanno da contraltare nuove sfide in termini di sicurezza, trasparenza e fiducia del pubblico nel processo elettorale. Del resto, come frequentemente rilevano autorevoli esperti del settore, l'ottimizzazione della comodità d'uso si pone quasi sempre in tensione con l'implementazione di robuste misure di sicurezza.

Nel corso degli ultimi decenni, il dibattito su queste tecnologie si è intensificato sia in ambito accademico sia a livello istituzionale. Il voto elettronico si presenta infatti come un fenomeno interdisciplinare, al crocevia tra informatica, diritto e scienza politica. Numerosi Paesi hanno avviato progetti di sperimentazione, gruppi di lavoro internazionali hanno elaborato linee guida e standard, e la letteratura scientifica ha iniziato a produrre teorie e dati sull'impatto di

1 Alvarez, R. M., Hall, T. E., & Llewellyn, M. (2008). *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton University Press.

2 Ibidem

3 Kersting, N. (2004). *Electronic Democracy: Political and Cross-National Perspectives*. Routledge.

tali sistemi sul tessuto democratico[4]. In questa prospettiva, il presente capitolo intende offrire una visione d'insieme dell'evoluzione del voto elettronico e online, esaminandone lo sviluppo storico, le principali tipologie tecnologiche e alcune implementazioni emblematiche a livello globale. Verranno inoltre richiamati i contributi teorici più rilevanti, utili a inquadrare il fenomeno in termini di opportunità e criticità per i processi democratici contemporanei. L'analisi generale costituirà inoltre la base per affrontare, nei successivi capitoli, aspetti più specifici come le questioni di sicurezza informatica e il ruolo della Digital Forensics nell'ambito elettorale.

3.2 Cenni storici sul voto elettronico

L'idea di automatizzare le procedure di voto non è nuova e precede l'era del computer. Già alla fine del XIX secolo furono introdotte le prime macchine meccaniche per votare (ad esempio, le macchine a leva ideate da Jacob H. Myers nel 1892), con l'obiettivo di accelerare lo scrutinio e ridurre gli errori umani[5]. Queste macchine, adottate inizialmente in alcuni stati degli USA, rappresentarono un primo tentativo d' innovare il processo elettorale attraverso la tecnologia elettromeccanica. Tuttavia, fu solo con l'avvento dell'elettronica e dell'informatica nella seconda metà del XX secolo che il voto elettronico conobbe uno sviluppo più ampio.

Negli anni '60 comparvero i sistemi a schede perforate (punch cards), in cui gli elettori perforavano schede di cartoncino lette poi da calcolatori; tali sistemi furono progressivamente impiegati su larga scala negli Stati Uniti a partire dagli anni '70 e '80[6]. Parallelamente, si diffusero i sistemi di lettura ottica delle schede votate a matita (noti anche come optical scan), che combinavano il tradizionale voto cartaceo con la velocità del conteggio elettronico.

Un momento cruciale nella storia del voto elettronico fu rappresentato dalle controverse elezioni presidenziali USA del 2000, durante le quali emersero i noti problemi legati alle schede perforate in Florida. L'incertezza generata dai voti dubbi *(dimpled o hanging cards)* portò a riconteggi contestati e mise in evidenza i limiti dei sistemi di voto dell'epoca[7]. Questo evento drammatico ebbe l'effetto di catalizzare l'attenzione pubblica e politica sulla necessità di aggiornare le tecnologie elettorali per garantire maggiore affidabilità. In risposta a tali eventi, il Congresso degli Stati Uniti approvò nel 2002 l'Help America Vote Act (HAVA), stanziando fondi federali per ammodernare le attrezzature di voto a livello nazionale. Tale legge promosse la dismissione delle schede perforate e diede

4 Ibidem

5 Saltman, R. G. (2006). *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. Palgrave Macmillan.

6 Ibidem.

7 Mercuri, R. (2002). "A Better Ballot Box?" *IEEE Spectrum*, 39(10), 28–33.

impulso all'adozione di urne elettroniche di nuova generazione, soprattutto i sistemi di registrazione elettronica diretta (DRE) e i sistemi a scansione ottica, accompagnandoli con requisiti per migliorare l'accessibilità e la verifica dei voti.

Negli stessi anni, altri Paesi intraprendevano percorsi innovativi analoghi. Ad esempio, il Brasile iniziò già dal 1996 una transizione verso il voto elettronico integrale, dotando progressivamente tutti i seggi elettorali di urne DRE per lo spoglio elettronico delle schede[8]. Nel frattempo, l'evoluzione di Internet e la crescente diffusione della società dell'informazione aprivano la strada al voto online (Internet voting o i-voting). Un caso paradigmatico è quello dell'Estonia, piccolo Paese baltico che, forte di un'infrastruttura digitale avanzata e di una capillare identità digitale per i cittadini, fu il primo al mondo a consentire ai propri elettori di votare tramite Internet in elezioni politiche: ciò avvenne nelle elezioni municipali del 2005, poi venne esteso a tutte le consultazioni nazionali a partire dal 2007[9]. L'esperienza estone ha dimostrato le potenzialità del voto via Internet, ma anche l'importanza di predisporre rigorose misure di sicurezza (ad esempio l'uso di smart card per l'autenticazione, protocolli crittografici per assicurare la segretezza del voto e meccanismi di verifica indipendente del risultato). In concomitanza, nel primo decennio degli anni 2000, si moltiplicarono in varie parti del mondo sperimentazioni di e-voting, sia in contesti locali sia in consultazioni nazionali, accompagnate dall'emanazione di standard e raccomandazioni internazionali volti a guidare l'implementazione sicura e affidabile di queste tecnologie. Tuttavia, come verrà discusso in seguito, l'adozione del voto elettronico non fu affatto uniforme, dal momento che alcuni Paesi abbracciarono con decisione tali sistemi, mentre altri li introdussero con prudenza o, talvolta, abbandonarono progetti già avviati a causa di varie problematiche successivamente emerse.

Con l'ingresso nel XXI secolo, dunque, il voto elettronico si era già declinato in varie forme e applicazioni. Dai sistemi elettronici stand-alone nelle singole sezioni elettorali si passò alle prime forme di voto remoto via Internet, ampliando ulteriormente il concetto stesso di voto dematerializzato. Questa evoluzione tecnologica portò con sé nuovi benefici ma anche nuove vulnerabilità. In particolare, l'interconnessione su larga scala attraverso la rete fece emergere il rischio di attacchi informatici su infrastrutture elettorali. Gli esperti di sicurezza come Schneier (2019) hanno sottolineato come, in un mondo sempre più iper-connesso, ogni sistema digitale, piattaforme di e-voting incluse, possa diventare bersaglio di attacchi e manipolazioni se non adeguatamente protetto[10]. Non a caso, il periodo vide crescere l'attenzione verso gli aspetti di cybersecurity

8 Saltman, R. G. (2006). *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. Palgrave Macmillan.

9 Ibidem, p. 37

10 Schneier, B. (2019). *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. W. W. Norton & Company.

elettorale, con governi e istituzioni internazionali impegnati nel definire requisiti tecnici e procedurali per mitigare minacce quali virus, intrusioni nei database elettorali, attacchi DoS ai sistemi di voto online, e così via. Tali profili saranno approfonditi successivamente, ma vale la pena ribadire fin d'ora che la storia del voto elettronico non è solo una cronaca di progressi tecnici, bensì anche e, forse soprattutto, la storia di una crescente consapevolezza riguardo alle sfide di sicurezza, una presa di coscienza che si è sviluppata di pari passo con le innovazioni implementate.

3.3 Teorie e dibattito accademico sul voto elettronico

L'introduzione del voto elettronico e online ha stimolato un vivace dibattito accademico circa le sue implicazioni politiche e sociali. Diversi filoni teorici sono emersi con lo scopo di interpretare il modo in cui le tecnologie elettorali digitali possono rimodellare le dinamiche della democrazia. Uno degli approcci più influenti è quello della tecnopolitica, che esamina l'interrelazione tra tecnologia e potere politico. Secondo questa prospettiva, l'adozione di strumenti come il voto elettronico può ridefinire i rapporti tradizionali tra cittadini, istituzioni e processi decisionali[11]. In particolare, la tecnopolitica studia come l'uso delle ICT possa spostare equilibri di potere, ad esempio riducendo il ruolo intermediario di alcuni attori (partiti, corpi burocratici) consentendo forme più dirette di partecipazione. Nel caso del voto elettronico, ciò potrebbe tradursi in consultazioni elettorali più frequenti o in nuove modalità di coinvolgimento degli elettori, con potenziali effetti sia positivi sia problematici sulla qualità della democrazia.

Un altro filone di ricerca si concentra sull'impatto del voto elettronico sulla partecipazione politica. L'ipotesi spesso avanzata è che facilitare le operazioni di voto, ad esempio eliminando la necessità di recarsi fisicamente a un seggio, come avviene con il voto online, possa ampliare la base degli elettori attivi, coinvolgendo gruppi tradizionalmente meno propensi al voto (giovani, cittadini all'estero, persone con disabilità, ecc.). Studi empirici hanno cercato di misurare tale effetto: ad esempio, Gibson e Cantijoch (2013) hanno esplorato se e in che misura l'impegno politico online differisca da quello off-line, contribuendo a concettualizzare nuovi indicatori di partecipazione nell'era di Internet[12]. I risultati finora raccolti sono misti: in alcuni contesti sperimentali il voto elettronico ha mostrato un lieve aumento dell'affluenza, soprattutto tra le fasce di elettorato più dinamiche, mentre in altri casi non si sono registrate differenze significative

11 Wright, S. (2012). *Technopolitics: Participation and Power in the Digital Age*. Cambridge University Press.

12 Gibson, R. K., & Cantijoch, M. (2013). "Conceptualizing and Measuring Participation in the Age of the Internet: Is Online Political Engagement Really Different to Offline?" *The Journal of Politics*, 75(3), 701–716.

rispetto ai metodi tradizionali. Ciò suggerisce che l'effetto mobilitante delle nuove tecnologie elettorali dipende da molteplici fattori socio-culturali e istituzionali ma non è automatico.

Sul versante teorico-normativo, ampio spazio è stato dedicato anche al concetto di cyberdemocrazia o democrazia digitale, intesa come l'insieme delle trasformazioni dei processi democratici indotte dall'uso pervasivo delle tecnologie digitali. Da questa angolazione, il voto elettronico viene studiato come parte di un più generale rinnovamento della sfera pubblica e delle pratiche di cittadinanza[13]. Alcuni studiosi intravedono in esso uno strumento per colmare deficit democratici, avvicinando le istituzioni ai cittadini e favorendo una maggiore inclusività delle decisioni pubbliche[14]. Altri, invece, avvertono che l'affidamento delle funzioni elettorali a sistemi digitali può generare nuovi rischi di disuguaglianza (ad esempio legati al divario digitale: non tutti i cittadini hanno uguale accesso o competenza nell'utilizzare strumenti online) e di opacità nelle decisioni politiche (se gli algoritmi che gestiscono le elezioni non sono adeguatamente controllabili dalla collettività).

Un tema ricorrente nel dibattito è la necessità di bilanciare innovazione e garanzie democratiche. Da un lato, l'innovazione tecnologica applicata al voto non deve mai compromettere i principi fondamentali di libertà, segretezza e personalità del voto, conquistati attraverso lunghe evoluzioni storiche. Dall'altro lato, le normative e i controlli tradizionali devono aggiornarsi per far fronte a minacce inedite. Numerosi esperti di sicurezza informatica hanno messo in guardia sui pericoli e su come le vulnerabilità tecniche possano tradursi in frodi elettorali o manipolazioni dei risultati su larga scala[15]. Ad esempio, Jeffries e Dunn (2017) evidenziano come i sistemi di voto possano essere bersaglio di attacchi cibernetici volti ad alterare i dati o violare la segretezza delle preferenze espresse. Di conseguenza, gran parte della letteratura sottolinea che l'adozione del voto elettronico deve procedere di pari passo con l'implementazione di rigorose misure di sicurezza e con un attento disegno istituzionale che garantisca trasparenza e verificabilità. In questo contesto, è emersa l'importanza di strumenti come la Voter Verified Paper Audit Trail (VVPAT), ovvero la stampa di una ricevuta cartacea verificabile dall'elettore prima della registrazione finale del voto elettronico: tale meccanismo, in seguito integrato in molti sistemi, è visto come un compromesso efficace per unire i benefici del digitale con la sicurezza di una traccia fisica indipendente. In ambito accademico-giuridico, infine, si rileva una certa cautela di fondo: autori come von Spakovsky (2011) hanno sostenuto che il voto via Internet, pur potenzialmente comodo, introduce rischi

13 Norris, P. (2011). *Democratic Deficit: Critical Citizens Revisited*. Cambridge University Press.

14 Ibidem.

15 Jeffries, C., & Dunn, K. (2017). "The Security of Voting Systems". *International Journal of Information Security*, 16(2), 215–230; Schneier, B. (2019). *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. W. W. Norton & Company.

tali da mettere in pericolo la fiducia del pubblico nelle elezioni, soprattutto se compromette la segretezza o consente influenze esterne[16].

Il messaggio prevalente, dunque, è che il progresso tecnologico non può essere arrestato, ma deve essere governato. La sfida teorica consiste nell'individuare come i nuovi strumenti possano rafforzare la democrazia senza eroderne i principi cardine. Questo equilibrio tematico tra ottimismo riformatore e prudenza garantista attraversa gran parte delle pubblicazioni sul voto elettronico degli ultimi vent'anni, riflettendo in ultima analisi quanto rilevante sia la posta in gioco, ovvero la legittimazione stessa dei governi eletti e la fiducia dei cittadini nei processi democratici.

3.4 Tipologie di sistemi di voto elettronico

Esistono diverse tipologie di sistemi di voto elettronico, ciascuna con caratteristiche tecnologiche proprie e differenti implicazioni in termini di sicurezza, accessibilità e trasparenza. Di seguito vengono presentate le principali categorie di sistemi di e-voting attualmente noti:

a) Sistemi di registrazione elettronica diretta (Direct Recording Electronic, DRE).

Attraverso questi sistemi l'elettore esprime la propria preferenza su un dispositivo elettronico (ad esempio un touchscreen o una tastiera) e il voto viene registrato in forma digitale nella memoria dell'urna elettronica. I sistemi DRE sono stati ampiamente adottati in vari paesi per la loro efficienza nello spoglio e la possibilità di assistere l'elettore nella compilazione della scheda (ad esempio segnalando voti nulli o duplicati). Tuttavia, una critica fondamentale mossa ai DRE di prima generazione riguarda l'assenza di una traccia cartacea verificabile dal votante[17]. Senza uno scontrino di voto fisico, infatti, risulta difficile (o impossibile) svolgere riconteggi indipendenti in caso di contestazioni, e l'intero processo di verifica è affidato ai soli registri elettronici interni, suscettibili di malfunzionamenti o manomissioni. Studi sulla sicurezza digitale hanno evidenziato come questa mancanza possa minare la fiducia nel sistema: ad esempio, Casey già nel 2011 sottolineava quanto l'impossibilità di effettuare audit forensi completi su macchine prive di evidenze fisiche costituisca un punto debole rilevante per la verificabilità. In risposta a tali critiche, molti produttori di DRE hanno successivamente integrato meccanismi di stampa del voto (VVPAT) o altre forme di audit trail per ovviare a questo problema (come si vedrà più avanti nella sezione sui sistemi ibridi).

16 von Spakovsky, H. A. (2011). "The Dangers of Internet Voting". *Harvard Journal of Law & Public Policy*, 34(2), 433–447.

17 Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

b) Sistemi a lettura ottica delle schede votate (Optical Scan).
Questa tipologia prevede che l'elettore esprima il voto su una scheda cartacea tradizionale (ad esempio tracciando un segno su un apposito riquadro o completando un modulo cartaceo leggibile elettronicamente), la quale viene poi inserita in uno scanner che digitalizza e conteggia automaticamente le preferenze. I sistemi a scansione ottica combinano dunque il supporto fisico cartaceo – che rimane disponibile per eventuali riconteggi manuali – con l'automazione elettronica del conteggio. Questo approccio ibrido bilancia automatizzazione e verificabilità, offrendo maggiore fiducia nel processo elettorale sia ai funzionari che agli elettori[18]. In effetti, la presenza della scheda cartacea consente di effettuare controlli incrociati post-elettorali e audit indipendenti, mitigando il rischio che un eventuale guasto tecnico o attacco informatico comprometta l'integrità finale del risultato. Non sorprende che dopo le controverse elezioni americane del 2000 vi sia stato un ritorno di interesse verso i sistemi optical scan: molti stati USA, ad esempio, hanno progressivamente sostituito i DRE puri con soluzioni a lettura ottica, proprio per garantire l'esistenza di un supporto tangibile del voto espresso[19].

c) Voto online (Internet voting o i-voting).
I sistemi che permettono agli elettori di votare da remoto attraverso una connessione Internet utilizzano tipicamente un computer o un altro dispositivo personale. In genere, l'elettore si autentica su un portale web sicuro mediante credenziali digitali (come certificati su smart card, credenziali di identità elettronica, autenticazione multifattoriale, ecc.) ed esprime il voto su un'interfaccia online; il voto viene quindi cifrato e trasmesso a un server centrale per l'elaborazione. Il voto online offre un livello di comodità e accessibilità senza precedenti, poiché consente di votare da qualsiasi luogo - caratteristica preziosa ad esempio per i cittadini residenti all'estero o per coloro che hanno difficoltà motorie. L'esperienza pionieristica dell'Estonia conferma queste potenzialità: nelle elezioni parlamentari estoni del 2019 oltre il 40% dei voti è stato espresso via Internet, a riprova di un elevato gradimento da parte dell'elettorato. Tuttavia, l'i-voting comporta sfide considerevoli in termini di sicurezza e fiducia[20]. Innanzitutto, il voto viaggia su infrastrutture pubbliche (la rete Internet) potenzialmente esposte ad attacchi: occorre quindi garantire la cifratura forte dei dati, la robustezza dei server elettorali contro intrusioni, e sistemi di autenticazione che impediscano frodi d'identità. Inoltre, è più complesso assicurare la

18 Gritzalis, D. (2002). "Secure Electronic Voting". *Advances in Computers*, 57, 255–289.
19 Ibidem
20 Krimmer, R. (2012). "The Evolution of E-Voting: Lessons From Estonia". *European Journal of ePractice*, 16, 4–17.

segretezza del voto familiare (ovvero impedire che terze persone possano osservare o influenzare il voto di un elettore remoto) e scongiurare coercizioni, problemi che nel seggio tradizionale sono mitigati dalla cabina elettorale. I critici sottolineano che, fino a quando non si raggiungeranno livelli certificabili di sicurezza pari a quelli del voto cartaceo, il voto online dovrebbe essere introdotto con prudenza e solo in contesti in cui esiste un'infrastruttura digitale altamente affidabile[21]. L'Estonia ha potuto implementare con successo l'i-voting grazie a una serie di condizioni favorevoli, tra cui un sistema nazionale di identità digitale avanzato, un elettorato abituato ai servizi online e misure di verifica post-voto che consentono a ciascun votante di controllare che il proprio voto sia stato registrato correttamente, senza violare l'anonimato.

d) Sistemi di voto ibridi (elettronico-cartaceo).
Rientrano in questa categoria tutte le soluzioni che combinano elementi del voto elettronico con elementi del voto tradizionale, al fine di sfruttare i vantaggi di entrambi. Un esempio tipico è dato dai DRE con ricevuta cartacea: in questi sistemi, pur essendo l'interazione dell'elettore completamente digitale, l'urna elettronica stampa immediatamente dopo ogni voto una ricevuta cartacea verificabile (di solito sotto forma di scheda cartacea riassuntiva, che l'elettore può controllare visivamente attraverso una teca trasparente prima che cada in un contenitore sigillato). In caso di contestazioni o controlli a campione, tali ricevute cartacee vengono utilizzate per riconteggi manuali o verifiche statistiche, aumentando la trasparenza e la fiducia senza rinunciare alla rapidità dello scrutinio elettronico [22]. Altre soluzioni ibride includono sistemi in cui il voto viene espresso su *kiosk* elettronici, ma memorizzato esclusivamente su supporto cartaceo leggibile elettronicamente (un approccio adottato, ad esempio, in alcune giurisdizioni degli Stati Uniti per mitigare i rischi dei DRE puri), oppure modelli di voto distribuito in cui una parte del processo avviene online (ad es. la registrazione del voto) ma richiede comunque una conferma o validazione presso un seggio fisico. L'idea di fondo dei sistemi ibridi è di conciliare innovazione e sicurezza: come nota Gibson (2010), tali approcci mirano a ridurre i rischi di manipolazione introducendo elementi verificabili in modo indipendente, senza rinunciare ai benefici di efficienza apportati dal digitale[23]. In molti contesti, l'adozione di un sistema ibrido è stata vista come un compromesso pragmatico: ad esempio in India, come vedremo, alle tradizionali voting machine elettroniche sono stati recentemente aggiunti moduli per la stampa cartacea del voto (VVPAT) proprio per

21 Ibidem
22 Gibson, J. (2010). "E-Voting: Risks and Advantages". *Journal of Democracy*, 21(1), 142–156.
23 Ibidem, p. 42

rispondere alle preoccupazioni di verificabilità espresse dalla società civile e dagli esperti.

3.5 Casi di studio: implementazioni globali del voto elettronico

Per comprendere meglio come le tipologie di sistemi sopra descritte siano state applicate nella pratica, è utile esaminare alcuni casi di studio internazionali. Le esperienze di diversi Paesi mostrano un ventaglio di risultati ed evidenziano fattori di successo e ostacoli ricorrenti nell'implementazione del voto elettronico e online su larga scala.

Estonia: un pioniere nel voto online

L'Estonia è universalmente riconosciuta come il primo paese ad aver introdotto il voto via Internet in elezioni politiche nazionali. Dopo alcune sperimentazioni iniziali, l'i- voting estone divenne realtà nelle elezioni amministrative del 2005 e, due anni dopo, nelle elezioni parlamentari del 2007. Il sistema implementato in Estonia si basa su un'infrastruttura statale di identità digitale estremamente sviluppata: ogni cittadino estone dispone di una carta d'identità elettronica e di credenziali crittografiche che gli consentono di autenticarsi in modo sicuro per numerosi servizi, incluso il portale di voto online. Nel sistema estone, l'elettore può votare da qualsiasi computer inserendo la propria carta elettronica in un lettore e immettendo i codici PIN personali; il voto espresso viene immediatamente cifrato e trasmesso ai server elettorali. Una caratteristica importante è la possibilità per l'elettore di verificare dopo il voto che la propria preferenza sia stata registrata correttamente: tramite una app dedicata sullo smartphone, e utilizzando un codice di verifica fornito durante la votazione, egli può controllare (entro un certo limite di tempo) che il server abbia ricevuto esattamente il voto inviato, il tutto senza rivelare la scelta effettuata. Inoltre, per garantire la segretezza, il sistema estone permette all'elettore di rivotare più volte online durante il periodo di votazione anticipata: solo l'ultima preferenza inviata viene conteggiata, così da prevenire eventuali coercizioni (non è infatti possibile avere la certezza che l'elettore non abbia successivamente cambiato il voto). Nel giorno ufficiale delle elezioni, l'elettore può perfino recarsi al seggio e votare su carta, annullando così il voto elettronico precedente – un ulteriore strumento di salvaguardia. Grazie a queste misure, l'Estonia è riuscita a ottenere un livello di fiducia elevato nel proprio sistema: la percentuale di votanti online è cresciuta ad ogni tornata, passando dal 5,5% nel 2007 a oltre il 40% nel 2019, segno che una larga parte dell'elettorato considera l'i-voting non solo comodo ma anche affidabile. L'esperienza estone dimostra dunque che il voto elettronico online può funzionare in un contesto reale, a patto di investire in sicurezza informatica

e trasparenza. Non tutti i Paesi dispongono, però, delle stesse precondizioni tecnologiche e culturali dell'Estonia, e questo spiega perché altri tentativi di i-voting su scala nazionale siano stati finora limitati o poco duraturi.

Brasile e DRE su larga scala

Il Brasile rappresenta uno dei più vasti e longevi esempi di adozione del voto elettronico in un grande paese democratico. Già a partire dalle elezioni del 1996, il Tribunal Superior Eleitoral (TSE) – l'organo che sovrintende a tutte le operazioni elettorali brasiliane – avviò l'introduzione di urne elettroniche DRE in alcune zone del Paese, con l'obiettivo di accelerare lo spoglio e ridurre le frodi nelle sezioni elettorali remote. Il programma fu via via ampliato: entro il 2000 tutti i circa 100 milioni di elettori brasiliani ebbero la possibilità di votare tramite le nuove macchine elettroniche, facendo del Brasile la prima democrazia di grandi dimensioni a utilizzare un sistema di e- voting universale. Le urne brasiliane (conosciute come urna eletrônica) sono dispositivi relativamente semplici: dotate di una tastiera numerica e di uno schermo, permettono all'elettore di digitare il codice numerico del candidato prescelto; il nome e la foto del candidato appaiono sul display per conferma, quindi il voto viene registrato su una memoria digitale. Il successo operativo del sistema è stato notevole: in termini di velocità di scrutinio – i risultati delle elezioni brasiliane sono disponibili poche ore dopo la chiusura dei seggi, nonostante l'elettorato superi oggi i 140 milioni di votanti – e di riduzione di alcune tipologie di brogli (ad esempio il voto di cabestro[24] o il furto di schede, difficili da attuare con le urne elettroniche). Tuttavia, il modello DRE puro adottato in Brasile non prevede, tuttora, una stampa cartacea del voto da conservare per eventuali riconteggi. Questa assenza di audit trail fisico ha suscitato critiche e preoccupazioni, soprattutto da parte della comunità accademica e di osservatori indipendenti, in merito alla trasparenza del processo. In diverse occasioni, l'opinione pubblica e alcuni gruppi politici hanno sollecitato l'introduzione di ricevute cartacee, ma tali proposte si sono scontrate con resistenze istituzionali (il TSE ha sempre difeso la sicurezza del sistema elettronico, temendo che l'introduzione di carta potesse al contrario reintrodurre vulnerabilità e rallentamenti). Per affrontare le criticità, le autorità brasiliane hanno puntato su altri meccanismi: da un lato, un rigoroso scrutinio pubblico del software di voto (con periodici test

24 Con l'espressione *voto di cabestro* si fa riferimento, in senso storico e sociologico, a pratiche di controllo o coercizione del voto riconducibili a dinamiche clientelari, intimidatorie o di dipendenza economico-sociale, che compromettono la libertà e la segretezza dell'espressione di voto. Il termine, pur non costituendo una categoria giuridica autonoma, è ampiamente utilizzato nella letteratura politologica e storica per descrivere forme di condizionamento elettorale diffuse in contesti caratterizzati da forti asimmetrie di potere. Cfr. G. Melis, *Storia dell'amministrazione italiana*, Il Mulino, 2014; D. Gambetta, *La mafia siciliana. Un'industria della protezione privata*, Einaudi, 1992.

di sicurezza in cui esperti esterni sono invitati a individuare vulnerabilità nel sistema); dall'altro, un sofisticato monitoraggio dei log di sistema e dei registri digitali durante e dopo le elezioni, in modo da individuare qualsiasi anomalia o tentativo di intrusione. La sicurezza del sistema si fonda, fra l'altro, su firme digitali e hash del software, sul monitoraggio dei log e sul Digital Vote Record, che preserva la segretezza del voto e ne garantisce l'integrità tramite cifratura e firma digitale[25]. Nonostante le polemiche ricorrenti – acuitesi in tempi recenti con accuse, finora non comprovate, di presunte frodi nel sistema elettronico – il Brasile continua a utilizzare con orgoglio le sue urne DRE, rivendicando di aver eliminato errori di conteggio e schede nulle che in passato affliggevano il suo complesso processo elettorale.

Il caso brasiliano dimostra come il voto elettronico possa essere implementato con successo in un contesto di massa, ma anche come la trasparenza e la verificabilità percepita del sistema siano cruciali per mantenerne la credibilità nel lungo periodo.

India: una democrazia di massa passa al voto elettronico

L'India, la più popolosa democrazia del mondo con oltre 900 milioni di elettori, ha adottato il voto elettronico su scala nazionale a partire dalle elezioni generali del 2004. In realtà, già dalla fine degli anni '90 l'Election Commission of India (ECI) aveva avviato sperimentazioni con Electronic Voting Machines (EVMs), piccoli dispositivi elettronici portatili progettati per funzionare anche in aree prive di rete elettrica stabile. Le EVM indiane, sviluppate da aziende pubbliche locali, sono essenzialmente delle urne DRE a basso costo e a prova di ambiente difficile: dotate di un pannello con i simboli dei partiti/candidati e di un singolo pulsante per ciascuno, permettono anche ad elettori analfabeti di votare identificando il simbolo del proprio candidato preferito. Dal 2004, tutte le elezioni federali e statali in India si svolgono tramite queste macchine elettroniche, che hanno permesso di eliminare l'immenso sforzo logistico del trasporto e il conteggio di miliardi di schede cartacee. Malgrado la complessità e vastità del contesto indiano, l'introduzione delle EVM è stata realizzata con notevole efficienza, ottenendo risultati rapidi e riducendo drasticamente il numero di voti nulli. Tuttavia, anche in India non sono mancate contestazioni sul fronte della sicurezza: attivisti e accademici, nel corso degli anni, hanno segnalato possibili vulnerabilità nelle macchine e il rischio di manomissioni, soprattutto durante le fasi di custodia delle EVM prima e dopo le votazioni. In risposta a queste preoccupazioni, a partire dal 2013 l'ECI ha introdotto progressivamente

25 Tribunal Superior Eleitoral (TSE), *Security; Auditability, pagine istituzionali sul sistema di voto elettronico brasiliano*; J. I. Pegorini, A. C. C. Souza, A. R. Ortoncelli, R. T. Pagno, N. C. Will, *Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Tests*, 2021.

sui propri dispositivi un modulo di stampa cartacea del voto (VVPAT). Oggi tutte le voting machines in India producono, al momento del voto, una ricevuta cartacea visibile all'elettore e conservata in un'apposita urna sigillata: ciò consente di effettuare verifiche manuali a campione e contribuisce a rassicurare l'opinione pubblica, offrendo un ulteriore strumento di controllo indipendente. L'esperienza indiana insegna che, persino in un contesto caratterizzato da sfide logistiche enormi (urne da trasportare in villaggi remoti, un alto numero di analfabeti, clima e infrastrutture variabili), il voto elettronico può funzionare ed essere scalabile. Le autorità hanno posto enfasi sulla semplicità e robustezza delle macchine (che non sono connesse in rete, riducendo così la superficie d'attacco) e su procedure severe di custodia e verifica. Ciò nonostante, il dibattito in India rimane aperto: periodicamente emergono richieste di ritorno al voto tradizionale da parte di chi sostiene che il sistema elettronico, per quanto efficiente, non offra sufficienti garanzie di trasparenza. Fino ad oggi, le istituzioni hanno difeso l'integrità del processo elettronico, forti anche dell'assenza di prove concrete di brogli legati alle EVM. Il caso indiano dimostra dunque l'importanza di adattare il design tecnologico alle specificità locali (ad esempio privilegiando semplicità d'uso e affidabilità hardware in un contesto di elezioni di massa), nonché di aggiornare i sistemi nel tempo in base ai feedback ricevuti (come l'aggiunta del VVPAT per aumentare la fiducia pubblica).

Stati Uniti e il loro approccio federale ed eterogeneo

Gli Stati Uniti d'America costituiscono un caso particolare, in quanto non esiste un unico sistema nazionale di voto elettronico, ma una varietà di approcci adottati a livello statale e locale. La vicenda delle elezioni del 2000, come già ricordato, fu il catalizzatore di un intenso processo di riforma. Dopo il 2002, grazie ai finanziamenti dell'HAVA, molti stati sostituirono le vecchie attrezzature: macchine DRE e scanner ottici divennero comuni nei seggi americani al posto delle schede perforate e dei sistemi manuali. Tuttavia, l'implementazione fu eterogenea: alcuni stati optarono per i DRE privi di ricevuta cartacea (es. Delaware, Georgia), altri per sistemi a scansione ottica con schede cartacee marcate a mano, altri ancora per una combinazione dei due. Questa eterogeneità si rivelò un punto di forza dal punto di vista della sperimentazione tecnologica, ma anche una fonte di inconsistenza nella garanzia della fiducia: gli stati che avevano adottato DRE senza VVPAT furono presto oggetto di critiche da parte di esperti di sicurezza e associazioni civiche, che ne chiedevano la conversione a sistemi verificabili. Nel corso degli anni 2000 e 2010, diversi stati retrocedettero dai DRE puri, tornando a soluzioni con scheda cartacea ottica o introducendo stampanti di ricevute. Parallelamente, emerse a livello nazionale la necessità di standard minimi: furono elaborati, tramite il National Institute of Standards and Technology (NIST) e l'Election Assistance Commission (EAC), linee guida federali per la certificazione dei sistemi di voto elettronico, sebbene

l'adozione di tali standard resti volontaria per gli stati. Un ulteriore stimolo al miglioramento dei sistemi negli USA è venuto dalle crescenti preoccupazioni sulla sicurezza informatica in seguito a episodi di interferenza nelle elezioni. In particolare, l'esperienza delle elezioni presidenziali del 2016 – durante le quali vi furono tentativi documentati di attacco alle infrastrutture elettorali da parte di attori esterni – ha evidenziato l'urgenza di rafforzare le difese e i controlli[26]. Il cosiddetto Mueller Report (2018) ha confermato tentativi di intrusione in database elettorali statali e altri tipi di attività ostili volte a sfruttare le vulnerabilità del sistema decentralizzato statunitense[27]. In risposta, negli ultimi anni molti stati hanno investito in upgrade di sicurezza, audit post-elettorali (risk-limiting audits) e formazione del personale. Il quadro statunitense, dunque, nel suo insieme, offre un'illustrazione delle sfide insite nel governare il cambiamento tecnologico in un contesto federale: alcune giurisdizioni hanno raggiunto un buon equilibrio tra efficienza e verificabilità, altre hanno faticato a tenere il passo con gli standard emergenti, e la questione del finanziamento continuo per il rinnovo delle macchine obsolete rimane aperta. Ciò detto, gli USA hanno anche contribuito a importanti innovazioni concettuali, come il già citato VVPAT e i metodi avanzati di auditing statistico, che sono divenuti modelli seguiti anche da altre nazioni.

Italia, fra sperimentazioni e cauti approcci

In Italia, il voto elettronico non è stato ancora adottato su scala nazionale, ma vi sono state nel tempo numerose sperimentazioni locali e un continuo dibattito sull'opportunità di digitalizzare (in tutto o in parte) le operazioni di voto. Un primo significativo esperimento avvenne in occasione delle elezioni politiche del 2006, quando, in parallelo al tradizionale voto cartaceo, che rimase comunque l'unico valido ai fini dei risultati, furono installate macchine di voto elettronico in circa 100 sezioni pilota distribuite in 13 regioni. L'iniziativa, promossa dal Ministero dell'Interno, aveva scopo dimostrativo: i risultati elettronici non furono utilizzati ufficialmente, ma l'esperimento servì a valutare la fattibilità tecnica e l'accettazione da parte degli elettori. L'esito fu tecnicamente soddisfacente (le macchine funzionarono regolarmente), ma emersero criticità sui costi molto elevati dell'operazione rispetto ai benefici ottenuti, e sul fatto che il tempo di voto per ciascun elettore tendeva ad aumentare con l'uso del dispositivo elettronico. Negli anni successivi, il tema rimase in agenda senza però ulteriori sviluppi su scala nazionale. Una seconda prova venne sperimentata nel 2017, quando la Regione Lombardia organizzò un referendum consultivo sull'autonomia regionale utilizzando esclusivamente il voto elettronico. Per la prima volta in Italia, in

26 Mueller, R. S. (2018). *Report on the Investigation into Russian Interference in the 2016 Presidential Election* ("Mueller Report"). U.S. Department of Justice.

27 Ibidem

un'intera consultazione, vennero abolite le schede cartacee e i cittadini votarono tramite tablet installati nei seggi. L'operazione coinvolse circa 3 milioni di elettori e 24.000 tablet: pur trattandosi di un referendum senza valore giuridicamente vincolante, fu un banco di prova importante. Il voto elettronico lombardo del 2017 si svolse senza incidenti gravi e i risultati furono resi noti poche ore dopo la chiusura delle urne, evidenziando dunque l'efficienza del metodo; tuttavia, anche in questo caso il costo economico dell'infrastruttura – interamente a carico della Regione – fu molto alto, e alcune valutazioni post-voto sollevarono dubbi sulla convenienza di replicare l'esperienza in assenza di economie di scala.

Altre iniziative in Italia hanno riguardato progetti di voto online per gli italiani all'estero o per specifiche elezioni primarie di partito, ma su scala molto limitata. In tale ambito si distingue l'esperienza del Movimento 5 Stelle, che fin dalla sua nascita ha fatto del voto elettronico uno degli strumenti cardine della propria proposta politica, utilizzando piattaforme digitali per consultazioni interne, definizione delle candidature e deliberazioni programmatiche. La piattaforma Rousseau, seppur non priva di controversie tecniche e giuridiche, ha rappresentato un unicum nel panorama politico italiano, in quanto tentativo sistematico di trasferire decisioni collettive su una struttura digitale di voto online, promuovendo una visione di *democrazia diretta digitale*. Questo esperimento ha alimentato il dibattito pubblico sull'affidabilità, la trasparenza e la sicurezza di tali strumenti, evidenziando al contempo il potenziale trasformativo delle tecnologie partecipative quando integrate nei processi organizzativi di un partito.

Nel complesso, l'approccio italiano al voto elettronico può definirsi prudente: il quadro normativo nazionale continua a prevedere che l'espressione del voto avvenga con carta e matita, e ogni eventuale introduzione del digitale richiede interventi legislativi ad hoc. Le sperimentazioni finora condotte hanno evidenziato sia le potenzialità (snellimento delle operazioni di spoglio, possibilità di voto assistito per disabili, riduzione di alcune irregolarità) sia le difficoltà (alti costi iniziali, necessità di formare il personale di seggio, diffidenza di parte dell'elettorato). Il dibattito in Italia resta dunque aperto: da un lato vi è chi auspica un graduale passaggio al voto elettronico, almeno per specifiche categorie di elettori o per referendum non politici, dall'altro lato prevale al momento la volontà di non affrettare i tempi finché non vi saranno soluzioni tecnologiche ampiamente collaudate in grado di garantire lo stesso livello di garanzie costituzionali del metodo cartaceo tradizionale.

Riflessioni conclusive

Gli esempi di Estonia, Brasile, India, Stati Uniti e Italia delineano un panorama eterogeneo. L'Estonia ha dimostrato che l'i-voting può funzionare quando esiste un forte ecosistema digitale e fiducia istituzionale; il Brasile e l'India attestano la fattibilità del voto elettronico in contesti elettorali di massa, evidenziando però rispettivamente l'importanza della verificabilità (ancora carente in Brasile) e dell'adattamento tecnologico al contesto (il modello semplificato ma efficace dell'India). Gli USA mostrano i progressi e le battute d'arresto di un approccio pluralistico, in cui diverse tecnologie coesistono e dove gli scandali possono incidere sulle politiche di adozione. L'Italia, infine, riflette l'atteggiamento attendista di molti Paesi occidentali, interessati all'innovazione ma gelosi custodi dei principi di certezza del voto e timorosi di introdurre cambiamenti radicali senza un consenso e una sicurezza assoluta.

Questi casi forniscono lezioni preziose: l'adozione del voto elettronico non è solo una questione tecnica, ma anche istituzionale e culturale. Fattori come la fiducia dei cittadini, la solidità delle infrastrutture digitali, il quadro normativo e la capacità di gestione dei rischi determinano in larga misura il successo o meno di tali iniziative.

Capitolo 4
Aspetti tecnici del voto elettronico

4.1 Architettura dei sistemi di voto elettronico

L'architettura dei sistemi di voto elettronico costituisce una configurazione socio-tecnico-normativa di elevata complessità, in cui s'intersecano infrastrutture digitali, protocolli crittografici, requisiti giuridici multilivello e aspettative democratiche da parte della collettività. Non si tratta, pertanto, di un mero assemblaggio di componenti hardware e software, ma di un ecosistema integrato e mission-critical, in cui ogni funzione (dalla raccolta del voto alla sua trasmissione, validazione, conservazione e scrutinio) deve essere progettata secondo principi di affidabilità, trasparenza verificabile, resilienza e rispetto dei diritti fondamentali. L'esigenza di garantire la sovranità del voto in ambito digitale impone che la progettazione architetturale sia coerente tanto con le sfide ingegneristiche quanto con le evoluzioni normative e le implicazioni sociopolitiche della digitalizzazione elettorale.

Tale complessità architetturale si accentua in ragione della natura intrinsecamente opaca dei processi computazionali. Diversamente dal voto cartaceo, le operazioni elettroniche non sono immediatamente osservabili né auditabili dall'elettore senza l'ausilio di strumenti tecnici e metodologie di verifica indipendente. È in tale contesto che il principio della *software independence*, formulato da Rivest e Wack[1], acquista rilievo: un sistema di voto elettronico deve garantire che ogni errore o manipolazione del software possa essere rilevato attraverso meccanismi di verifica esterni, senza dover necessariamente confidare nella correttezza del codice eseguibile. L'affidabilità del processo non può fondarsi su un atto fideistico nei confronti dell'infrastruttura tecnica, bensì deve emergere da una architettura verificabile ex ante, monitorabile in itinere e auditabile ex post.

All'interno di questo paradigma, la Digital Forensics assume un ruolo strutturale e non meramente reattivo. Essa non si limita alla funzione investigativa post-incident, bensì concorre a definire una cornice di *accountability computazionale*, rendendo possibile il tracciamento, la conservazione e la verifica forense delle operazioni critiche svolte durante il ciclo di vita del voto elettronico. Le evidenze digitali – siano esse log, hash, timestamp o metadati di sistema – diventano parte integrante del processo democratico, nella misura in cui consentono di ricostruire eventi, attribuire responsabilità e dimostrare l'integrità dei risultati.

---

1 Rivest, R. L., & Wack, J. P. (2006). *On the notion of "software independence" in voting systems*. MIT Computer Science and Artificial Intelligence Laboratory, Technical Report.

Come mostrato da Kshetri e Voas[2], sistemi *forensic-ready* aumentano significativamente la trasparenza e riducono il rischio sistemico, anche in scenari ad alta criticità geopolitica o cibernetica.

L'importanza della digital forensics nei sistemi di voto elettronico è oggi esplicitamente riconosciuta anche nei documenti istituzionali europei. La Direttiva (UE) 2022/2555 (NIS2)[3] impone agli operatori di servizi essenziali – tra cui rientrano le autorità elettorali digitalizzate – l'obbligo di dotarsi di capacità di *detection*, *response* e *forensics* in caso di incidenti informatici, evidenziando come l'architettura di sicurezza debba comprendere fin dall'inizio meccanismi di logging dettagliato e conservazione sicura delle prove digitali. Analogamente, il Centro Comune di Ricerca della Commissione Europea (JRC), nel suo report del 2023 sull'e-voting[4], raccomanda che ogni sistema elettorale digitale sia progettato per essere "monitorabile e investigabile" da terze parti fidate, suggerendo l'impiego combinato di tecnologie come il logging crittografico, i registri distribuiti (es. blockchain permissioned) e l'audit computazionale come strumenti tecnici a supporto della trasparenza e della legittimità del voto.

La letteratura accademica convergente conferma che l'assenza di una cultura forense nei sistemi elettorali digitali compromette non solo la sicurezza tecnica, ma anche la tenuta dell'ordine democratico. In mancanza di tracciabilità rigorosa, gli eventi anomali restano opachi e le contestazioni non possono essere risolte con criteri oggettivi. Al contrario, architetture progettate secondo logiche di *forensic-by-design*, in cui i dati vengono raccolti e conservati in modo da essere immediatamente utilizzabili a fini probatori, permettono non solo di rispondere agli attacchi, ma anche di dissuadere proattivamente, rafforzando la fiducia istituzionale, l'integrità del processo e la resilienza sistemica.

Alla luce di quanto precede, appare chiaro che la Digital forensics non può più essere considerata un modulo accessorio, ma dev'essere ingegnerizzata come componente nativa dell'architettura del voto elettronico, al pari della crittografia, dell'autenticazione forte e delle misure antimanomissione. L'evoluzione tecnologica e normativa europea post-2025, inclusa la transizione verso tecnologie post-quantum, renderà ancor più imprescindibile disporre di sistemi forensicamente trasparenti, in grado di garantire, oltre alla segretezza del voto, la possibilità effettiva di verificarne la correttezza e la non alterazione, anche a posteriori e in contesti giurisdizionali. Una tale progettazione, se correttamente implementata, non solo aumenta la sicurezza tecnica, ma rafforza la legittimazione democratica del voto elettronico nel suo complesso.

---

2 Kshetri, N., & Voas, J. (2018). "Blockchain-Enabled E-Voting". *IEEE Computer*, 51(10), 95–99. Gli autori evidenziano come sistemi progettati con logiche di *forensic readiness* migliorino la trasparenza, l'auditabilità e la resilienza dei processi digitali critici.

3 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (*NIS2*).

4 European Commission – Joint Research Centre (JRC). (2023). *Cybersecurity of Electronic Voting Systems*. Publications Office of the European Union.

4.2 Componenti chiave dell'architettura

L'architettura di un sistema di voto elettronico si articola attraverso una serie di componenti tecniche essenziali, ognuna delle quali riveste un ruolo strategico e irrinunciabile nel garantire l'affidabilità, la sicurezza e la regolarità dell'intero processo elettorale. Sebbene tali componenti operino in ambiti distinti – dall'interazione con l'elettore fino alla gestione e protezione dei dati – esse devono essere progettate come un insieme coeso e interdipendente, secondo principi di coerenza funzionale, sicurezza multilivello e conformità normativa[5].

Il punto di accesso primario al sistema è costituito dall'interfaccia utente, che rappresenta il canale attraverso cui l'elettore esercita il proprio diritto di voto. Essa deve essere concepita secondo criteri di chiarezza, semplicità d'uso e sicurezza, affinché l'esperienza dell'utente sia al contempo intuitiva e impenetrabile a manipolazioni malevole. In particolare, il design dell'interfaccia deve prevenire ambiguità interpretative, evitare la possibilità di errori non intenzionali e assicurare l'impossibilità di deviare o compromettere l'intenzione di voto. Tali requisiti assumono una valenza ancor più significativa alla luce delle normative europee in materia di accessibilità digitale, come la Direttiva (UE) 2016/2102, che impone agli enti pubblici l'obbligo di garantire l'accesso universale alle piattaforme digitali, incluse quelle elettorali[6]. Ciò implica che l'interfaccia debba essere utilizzabile anche da soggetti affetti da disabilità sensoriali, motorie o cognitive, attraverso soluzioni inclusive come l'ingrandimento dei testi, il supporto per screen reader e la navigazione da tastiera. In tale prospettiva, l'interfaccia utente non è un elemento accessorio, bensì una componente determinante per la legittimità democratica del sistema, in quanto veicola concretamente il principio dell'universalità del voto.

A valle dell'interazione dell'elettore con il sistema, la fase di elaborazione e registrazione del voto è affidata a una rete di server dedicati, i cosiddetti server di gestione del voto. Questi costituiscono il nucleo computazionale dell'infrastruttura e sono responsabili dell'elaborazione delle preferenze espresse, della loro memorizzazione temporanea o definitiva e, in molti casi, dello scrutinio elettronico. Data la loro centralità operativa, essi rappresentano anche il principale vettore di rischio in termini di attacchi informatici, malfunzionamenti hardware o errori sistemici. Per tale motivo, la loro progettazione deve rispondere ai massimi standard di sicurezza informatica e di resilienza operativa. È imprescindibile, ad esempio, che tali server siano protetti da firewall di nuova generazione, da sistemi di autenticazione forte per gli amministratori, e che i dati in essi trattati siano cifrati secondo algoritmi robusti. La conformità al GDPR, e

5 Saltman, R. G. (2006). *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. Palgrave Macmillan.

6 Direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio sull'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.

più in generale alle normative in materia di protezione dei dati personali, impone inoltre l'adozione di misure specifiche per prevenire accessi non autorizzati, perdita di integrità o divulgazione accidentale di informazioni sensibili[7]. Non meno rilevante è l'obbligo di sottoporre regolarmente i server a verifiche di sicurezza, penetration testing e certificazioni basate su standard internazionali, come l'ISO/IEC 27001, che definisce i requisiti per un sistema di gestione della sicurezza delle informazioni[8].

In stretta connessione con i server operano i database degli elettori, contenitori digitali che custodiscono dati altamente sensibili, quali le generalità, l'abilitazione al voto, l'identificativo del voto (ove presente) e, in taluni casi, le credenziali di accesso. Il livello di protezione di queste basi di dati incide direttamente sulla legittimità e sull'inviolabilità dell'intero processo elettorale: una violazione della riservatezza o dell'integrità di questi dati – anche solo potenziale – potrebbe determinare la compromissione dell'esito elettorale e innescare una crisi di fiducia sistemica[9]. La normativa europea, in particolare il GDPR, stabilisce che il trattamento di tali informazioni debba avvenire nel rispetto dei principi di minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza. A ciò si aggiunge la necessità di implementare tecnologie di tracciamento e auditing, che permettano di monitorare ogni accesso e ogni modifica effettuata sui dati. In tale ambito, la digital forensics svolge un ruolo cruciale, consentendo di identificare tempestivamente eventuali comportamenti anomali o accessi irregolari e di conservare le prove digitali necessarie per un'eventuale analisi forense. In situazioni di crisi – come pandemie, guerre o gravi emergenze interne – la vulnerabilità dei database elettorali può aumentare sensibilmente, rendendo indispensabile l'adozione di misure preventive avanzate, basate su criteri di sicurezza differenziata, segmentazione delle reti e ridondanza geodistribuita[10].

Infine, a tenere insieme l'intero sistema vi è l'infrastruttura di rete, che collega le postazioni di voto, i server centrali, i database e, in alcuni casi, gli ambienti di verifica esterni o di pubblicazione dei risultati. Trattandosi di un'infrastruttura esposta – almeno in parte – alla dimensione pubblica di Internet, essa costituisce uno dei bersagli privilegiati di attacchi distribuiti, intercettazioni del traffico e tentativi di sabotaggio. Per mitigare tali rischi, è fondamentale l'impiego di protocolli crittografici robusti, in primis il Transport Layer Security (TLS) nella sua versione 1.3, per garantire la riservatezza e l'integrità delle comunicazioni

7 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (*General Data Protection Regulation – GDPR*).

8 ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*.

9 Gritzalis, D. (2002). "Secure Electronic Voting". *Advances in Computers*, 57, 255–289.

10 Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

tra elettore e server[11]. A ciò si aggiunge l'imprescindibile necessità di monitorare costantemente il traffico di rete attraverso sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS), capaci di individuare in tempo reale attività anomale o comportamenti malevoli. Il quadro normativo europeo, delineato dapprima dalla Direttiva NIS e oggi aggiornato dalla Direttiva (UE) 2022/2555 (NIS2), impone che le infrastrutture digitali di interesse pubblico – tra cui rientrano i sistemi di voto elettronico – adottino misure proporzionate ma rigorose per garantire la continuità operativa anche in caso di compromissione, la capacità di risposta agli incidenti e la documentazione accurata degli eventi[12]. In questo senso, l'infrastruttura di rete non può essere considerata una componente passiva, bensì un elemento attivo di difesa, in grado di contribuire alla resilienza sistemica del processo elettorale nel suo insieme.

4.3 Implicazioni giuridiche e di sicurezza informatica

L'implementazione e la gestione di un sistema di voto elettronico richiedono la stretta conformità a un quadro normativo articolato, che può variare sensibilmente in base al contesto nazionale e internazionale. In Italia, ad esempio, il Codice dell'Amministrazione Digitale (CAD) fornisce le linee guida per la digitalizzazione dei processi elettorali, imponendo che i sistemi di e-voting rispettino criteri di sicurezza, trasparenza e accessibilità[13]. Tali criteri tecnici sono ulteriormente dettagliati dalle disposizioni dell'Agenzia per l'Italia Digitale (AgID), che definisce standard operativi e requisiti che le piattaforme di voto elettronico devono soddisfare per essere considerate affidabili[14]. A livello europeo, il Regolamento Generale sulla Protezione dei Dati (GDPR) impone obblighi stringenti riguardo alla tutela dei dati personali degli elettori, garantendo tra l'altro agli interessati diritti quali l'accesso e la rettifica delle informazioni personali trattate dal sistema di voto. Contestualmente, la dimensione cybersecurity risulta fondamentale: i sistemi di voto elettronico devono adottare misure avanzate di sicurezza informatica per proteggere l'infrastruttura e i dati, e devono prevedere procedure efficaci per gestire eventuali incidenti (come approfondito in seguito). In questo contesto, la digital forensics risulta cruciale non solo in fase preventiva, ma anche nell'eventualità di violazioni: essa consente di investigare su qualsiasi incidente di sicurezza, fornendo prove digitali dettagliate e affidabili che possono rivelarsi determinanti in sede di indagine o

11 Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*. IETF RFC 8446.

12 Direttiva (UE) 2016/1148 (*NIS*) e Direttiva (UE) 2022/2555 (*NIS2*), disposizioni su gestione del rischio, continuità operativa e risposta agli incidenti per infrastrutture digitali essenziali.

13 Decreto Legislativo 7 marzo 2005, n. 82 (*Codice dell'Amministrazione Digitale – CAD*), e successive modificazioni.

14 Agenzia per l'Italia Digitale (AgID). *Linee guida sulla sicurezza ICT e sui servizi digitali della PA*, aggiornamenti 2022–2024.

di contenzioso. L'insieme di queste misure – rispetto delle normative, adozione di standard tecnici e impiego di strumenti forensi – rappresenta un pilastro imprescindibile per assicurare che l'introduzione del voto elettronico avvenga senza compromettere i diritti e la fiducia degli elettori nel processo democratico.

4.4 Metodologie crittografiche avanzate

La salvaguardia dell'integrità, della riservatezza e dell'autenticità dei dati elettorali costituisce una delle sfide centrali nella progettazione dei sistemi di voto elettronico. In tale prospettiva, la crittografia svolge una funzione non solo protettiva, ma anche costitutiva dell'affidabilità del sistema stesso: essa rappresenta lo strato tecnologico che consente di garantire, in ogni fase del processo – dalla trasmissione all'archiviazione, dalla verifica all'autenticazione – la sicurezza delle informazioni e la segretezza del voto. A fronte della crescente sofisticazione degli attacchi informatici, la crittografia contemporanea si articola attraverso una pluralità di metodologie, ciascuna delle quali risponde a esigenze specifiche di protezione, robustezza ed efficienza.

Tra i fondamenti su cui si regge l'intero impianto crittografico figurano le tecniche simmetriche e asimmetriche. La crittografia simmetrica, basata sull'utilizzo di una medesima chiave condivisa tra mittente e destinatario, rappresenta una soluzione largamente adottata per cifrare i dati in transito, grazie alla sua elevata efficienza computazionale. L'algoritmo AES (Advanced Encryption Standard), in particolare, si è affermato come lo standard prevalente in tale ambito[15]. Tuttavia, uno dei punti più delicati legati a questo approccio è la gestione sicura delle chiavi stesse: la normativa vigente in materia di protezione dei dati personali, in particolare il GDPR, impone che tali chiavi siano custodite in ambienti sicuri, sottoposte a rotazione periodica e protette da accessi non autorizzati. Complementare alla crittografia simmetrica è quella asimmetrica, fondata sull'impiego di una coppia di chiavi – una pubblica e una privata – e particolarmente utile nei meccanismi di firma digitale e autenticazione. Algoritmi come RSA e la crittografia a curve ellittiche (ECC) consentono, ad esempio, di autenticare un dispositivo o una sessione di voto senza compromettere l'anonimato dell'elettore, garantendo così un equilibrio tra verificabilità e tutela della privacy[16].

Accanto a queste tecniche consolidate, si affacciano oggi scenari tecnologici d'avanguardia, in particolare quelli legati alla crittografia quantistica. La Quantum Key Distribution (QKD) rappresenta uno dei paradigmi più promettenti in questo ambito: essa si basa sui principi della meccanica quantistica per

15 National Institute of Standards and Technology (NIST). (2001). *Advanced Encryption Standard (AES)*. FIPS PUB 197.

16 Kahn Academy / Bernstein, D. J. (2014). "Introduction to Elliptic Curve Cryptography". *IEEE Security & Privacy*, 12(4), 32–38.

generare e distribuire chiavi segrete, offrendo un livello di sicurezza fondato non sulla difficoltà computazionale, ma sulle leggi fisiche fondamentali. La caratteristica che rende il QKD particolarmente interessante per l'ambito elettorale è la sua capacità di rilevare ogni tentativo di intercettazione: la semplice osservazione di un fotone – come nei protocolli BB84 o E91 – altera il suo stato quantistico, rendendo visibile l'interferenza e consentendo l'interruzione della comunicazione prima che un attacco possa compromettere l'integrità del canale[17]. L'esperimento condotto dal satellite cinese Micius, che ha dimostrato la possibilità di distribuire chiavi quantistiche su scala globale tra stazioni terrestri distanti, ha segnato un punto di svolta nella transizione da laboratorio a infrastruttura reale. Anche in Europa si sono moltiplicati i progetti pilota, come SECOQC, che ha esplorato l'uso del QKD su reti in fibra ottica estese, dimostrando la fattibilità dell'integrazione di canali quantistici all'interno delle comunicazioni governative[18]. Tuttavia, nonostante i progressi, l'adozione su vasta scala di questa tecnologia presenta ancora ostacoli rilevanti: l'elevato costo delle apparecchiature, la fragilità dei canali ottici necessari, la complessità nella sincronizzazione e la necessità di linee di vista dirette per i collegamenti satellitari ne limitano al momento la diffusione operativa nei sistemi elettorali. È prevedibile, tuttavia, che l'evoluzione tecnologica – spinta anche da investimenti pubblici strategici nel settore delle telecomunicazioni quantistiche – contribuisca a superare progressivamente tali limiti, rendendo il QKD un'opzione praticabile per garantire l'integrità del voto anche in contesti ad alta sensibilità geopolitica.

Parallelamente allo sviluppo della crittografia quantistica, la comunità scientifica si sta preparando ad affrontare l'impatto che i futuri computer quantistici potranno avere sugli algoritmi classici. Le tecnologie quantistiche, una volta pienamente sviluppate, potrebbero infatti rendere vulnerabili gli attuali standard crittografici, in particolare RSA ed ECC, compromettendo di fatto la sicurezza di sistemi che oggi si basano sulla difficoltà del calcolo di fattorizzazione o del logaritmo discreto. Per fronteggiare questo scenario, il NIST (National Institute of Standards and Technology) ha avviato un processo internazionale di selezione e standardizzazione di algoritmi post-quantum, che si concluderà nei prossimi anni con la definizione di nuovi schemi crittografici resistenti agli attacchi quantistici[19]. L'integrazione di tali algoritmi nei sistemi di voto elettronico rappresenterà una tappa fondamentale nella costruzione di architetture resilienti a lungo termine. Se opportunamente combinata con il QKD per la

17 Bennett, C. H., & Brassard, G. (1984). "Quantum Cryptography: Public Key Distribution and Coin Tossing". *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.

18 Peev, M. et al. (2009). "The SECOQC Quantum Key Distribution Network in Vienna". *New Journal of Physics*, 11.

19 National Institute of Standards and Technology (NIST). (2022–2024). *Post-Quantum Cryptography Standardization Process*. U.S. Department of Commerce.

distribuzione delle chiavi, la crittografia post-quantistica può offrire un doppio livello di protezione: da un lato fondato sulla fisica quantistica, dall'altro sulla robustezza matematica, creando così un paradigma di sicurezza ibrido in grado di resistere sia agli attacchi attuali sia a quelli emergenti.

Dal punto di vista della digital forensics, l'introduzione di tecnologie quantistiche all'interno delle reti elettorali comporta nuove sfide ma anche significative opportunità. Sarà necessario, infatti, sviluppare strumenti forensi in grado di monitorare, raccogliere e analizzare log di comunicazione quantistica, verificando la conformità ai protocolli QKD concordati e l'assenza di alterazioni nel flusso di distribuzione delle chiavi. Qualora emergano anomalie o sospetti di manomissione, l'analisi forense potrà fornire elementi probatori in grado di attestare l'origine dell'interferenza e il suo impatto sull'integrità del processo. In un'epoca in cui la trasparenza del voto elettronico dipenderà anche dalla capacità di auditare tecnologie estremamente sofisticate, la digital forensics rappresenterà un presidio imprescindibile di fiducia pubblica e accountability istituzionale.

Un'ulteriore innovazione che sta progressivamente guadagnando centralità nella ricerca applicata è la crittografia omomorfa. A differenza delle tecniche tradizionali, che richiedono la decifrazione dei dati per l'esecuzione di operazioni aritmetiche o logiche, l'omomorfismo consente di operare direttamente su dati cifrati. Questo approccio, se applicato al conteggio dei voti, permette di eseguire lo scrutinio in modalità completamente cifrata, senza mai dover decrittare i singoli voti espressi. In un'architettura di questo tipo, ogni voto rimane sigillato fin dal momento dell'espressione fino al calcolo del risultato aggregato, che può essere successivamente decrittato per la sola finalità di comunicazione dell'esito. Ciò comporta due vantaggi decisivi: da un lato, la protezione assoluta della segretezza del voto, anche durante le fasi più sensibili del processo; dall'altro, la riduzione drastica dei rischi connessi a compromissioni dei server di scrutinio. Sebbene l'implementazione della crittografia omomorfa presenti ancora sfide significative – in particolare per quanto riguarda i costi computazionali e i tempi di elaborazione – i progressi nella progettazione algoritmica e nell'hardware dedicato stanno progressivamente riducendo queste barriere[20]. Diversi prototipi sperimentali, testati in ambito accademico e industriale, dimostrano che il ricorso a questa tecnologia potrebbe divenire una prassi concreta nei prossimi anni, soprattutto in contesti di voto remoto o di scrutinio distribuito. In ultima analisi, la crittografia omomorfa si configura non solo come una risposta tecnologica alle esigenze di sicurezza, ma anche come un dispositivo epistemico per rafforzare la legittimità e la verificabilità delle operazioni elettorali, offrendo agli attori istituzionali e ai cittadini la garanzia che il voto sia rimasto integro e segreto fino all'ultima fase del processo.

20 Gentry, C. (2009). "Fully Homomorphic Encryption Using Ideal Lattices". *Proceedings of the 41st Annual ACM Symposium on Theory of Computing.*

4.5 Autenticazione degli elettori e sicurezza applicativa

L'autenticazione affidabile degli elettori costituisce un elemento imprescindibile per garantire l'integrità del voto elettronico. Verificare che ciascun voto sia effettivamente espresso da un elettore autorizzato – e che non vi sia possibilità di votazione multipla o impersonificazione – implica l'adozione di meccanismi di autenticazione robusti e multilivello. Una delle soluzioni più consolidate in tale ambito è rappresentata dall'autenticazione a più fattori (MFA), che prevede la combinazione di differenti categorie di verifica: qualcosa che l'utente conosce (una password o un PIN), qualcosa che possiede (ad esempio uno smartphone, una smart card o un token fisico), e qualcosa che è (un dato biometrico, come impronta digitale o riconoscimento facciale)[21]. Questo approccio rende estremamente complesso per un attore malevolo riuscire a compromettere tutte le credenziali necessarie in simultanea.

Numerose ricerche nel settore della sicurezza informatica confermano l'efficacia della MFA nel prevenire accessi non autorizzati e nel contrastare tecniche come il phishing, lo sniffing e il credential stuffing[22]. In aggiunta, si stanno sempre più affermando standard avanzati per l'autenticazione forte, in particolare il protocollo FIDO2 (Fast IDentity Online), che consente un accesso sicuro senza l'utilizzo di password, basandosi su chiavi crittografiche e su elementi biometrici locali[23]. Grazie all'integrazione con dispositivi personali – come smartphone dotati di sensori biometrici – FIDO2 consente di verificare l'identità dell'elettore tramite un processo simultaneamente sicuro e agevole, riducendo la dipendenza da credenziali centralizzate e aumentando la resistenza contro attacchi remoti.

Va tuttavia sottolineato che anche questi sistemi richiedono implementazioni accorte. Devono infatti essere previsti meccanismi di fallback per i casi in cui l'elettore non possa usufruire del fattore biometrico (per esempio in caso di disabilità temporanee o permanenti), e devono essere garantite misure specifiche per la tutela dei dati biometrici, considerati a tutti gli effetti dati sensibili secondo la normativa europea vigente. L'utilizzo di MFA e di protocolli avanzati come FIDO2 innalza dunque sensibilmente il livello di sicurezza applicativa dei sistemi di voto elettronico, contribuendo a garantire che solo gli aventi diritto possano votare e che ogni tentativo di frode o intrusione venga prontamente rilevato e neutralizzato.

21 NIST. (2017). *Digital Identity Guidelines*. Special Publication 800-63.

22 Florêncio, D., & Herley, C. (2010). "Where Do Security Policies Come From?". *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

23 FIDO Alliance. (2019). *FIDO2: Moving the World Beyond Passwords*. Technical Overview.

4.6 Protocolli di sicurezza e integrità dei dati

La sicurezza end-to-end delle elezioni elettroniche si fonda sull'adozione di protocolli crittografici avanzati sia per proteggere le comunicazioni tra i dispositivi e i server, sia per garantire la non alterabilità e la tracciabilità delle operazioni interne al sistema. Nella fase di trasmissione del voto, l'utilizzo del protocollo Transport Layer Security (TLS), nella sua versione più aggiornata (1.3), rappresenta un requisito imprescindibile per assicurare che i dati inviati non possano essere intercettati, letti o manipolati da terzi[24]. TLS crea un canale cifrato autenticato tra l'elettore e il server, garantendo al contempo la riservatezza del contenuto e l'identità delle parti coinvolte. Tuttavia, l'efficacia di TLS dipende strettamente dalla corretta gestione delle chiavi crittografiche, dalla configurazione sicura del protocollo e dalla dismissione tempestiva delle versioni obsolete.

Oltre alla protezione del canale, è essenziale che il sistema garantisca trasparenza, verificabilità e auditabilità delle operazioni di voto. A tal fine, l'implementazione di meccanismi di audit trail consente di registrare ogni azione significativa compiuta dal sistema – dalla registrazione del voto all'autenticazione dell'utente, dall'apertura delle urne elettroniche al consolidamento del risultato – in modo immodificabile e verificabile. Tali log costituiscono una fonte di verità fondamentale, sia per la ricostruzione a posteriori di eventuali anomalie, sia per il monitoraggio da parte di organismi terzi. In questo contesto, una tecnologia emergente di crescente interesse è la blockchain: una struttura distribuita e crittograficamente vincolata che consente di registrare gli eventi in blocchi concatenati e immutabili[25].

Nel voto elettronico, l'adozione della blockchain può rafforzare l'integrità del processo grazie alla sua natura decentralizzata e alla capacità di rilevare qualsiasi tentativo di alterazione retroattiva. Una volta che un'operazione è stata scritta in un blocco validato, ogni modifica successiva altererebbe gli hash crittografici dell'intera catena, rendendo l'alterazione evidente. Nonostante questi vantaggi, è necessario valutare attentamente le implicazioni di scalabilità e privacy: la registrazione distribuita di un numero elevatissimo di transazioni (voti) comporta carichi computazionali rilevanti e pone interrogativi sul mantenimento dell'anonimato dell'elettore. L'impiego di blockchain permissioned, in cui i nodi validatori sono predefiniti e controllati, rappresenta una possibile soluzione di equilibrio tra trasparenza e sicurezza. In sintesi, un sistema che combina TLS aggiornato, audit trail strutturati e blockchain adattata alle esigenze elettorali può fornire un modello di sicurezza multilivello, in cui ogni fase del processo – dalla trasmissione dei dati alla loro persistenza – è presidiata da misure crittografiche avanzate, favorendo la fiducia pubblica e la resilienza istituzionale.

24 Rescorla, E. (2018). *TLS 1.3*. IETF RFC 8446.

25 Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. White paper.

4.7 Risposta agli incidenti e piani di recovery

Per quanto robusto possa essere un sistema di voto elettronico, nessuna infrastruttura digitale può dirsi completamente immune da vulnerabilità. È pertanto necessario predisporre piani strutturati per la risposta agli incidenti (incident response) e per il recupero delle funzionalità (disaster recovery), che consentano di mitigare rapidamente gli effetti di eventuali compromissioni e di ripristinare la piena operatività del servizio. La Direttiva (UE) 2016/1148 (NIS) e, successivamente, la Direttiva (UE) 2022/2555 (NIS2) hanno esplicitamente incluso le infrastrutture elettorali digitali tra i settori essenziali da proteggere, imponendo agli Stati membri obblighi precisi in termini di gestione del rischio, notifica degli incidenti e continuità operativa[26].

Un piano di incident response efficace deve prevedere la possibilità di isolare tempestivamente le componenti compromesse, attivare sistemi di backup in tempo reale e comunicare in modo trasparente con le autorità competenti e gli elettori, evitando interruzioni o ambiguità che possano compromettere la legittimità dell'elezione. In parallelo, la digital forensics assume un ruolo cruciale nella fase post-evento: gli analisti forensi raccolgono e analizzano evidenze digitali (log, file temporanei, memoria volatile) per determinare le modalità, le cause e gli impatti dell'incidente. Tali informazioni sono decisive sia per migliorare le difese future, sia per identificare responsabilità legali e tecniche. La presenza di un piano di continuità operativa integrato con capacità forensi avanzate costituisce un segno distintivo di maturità istituzionale e tecnica: non si limita a prevenire gli incidenti, ma ne gestisce l'emersione in modo professionale, documentabile e responsabile.

4.8 Riflessioni conclusive

L'analisi tecnica condotta nel presente capitolo evidenzia come l'efficacia e la legittimità del voto elettronico dipendano da una progettazione sistemica che coniughi sicurezza informatica, trasparenza procedurale e conformità normativa. Le tecnologie crittografiche avanzate, come la crittografia omomorfa, la blockchain, il QKD e gli algoritmi post-quantum, offrono strumenti potenti per rafforzare la segretezza del voto e l'integrità del processo elettorale. Tuttavia, la loro implementazione deve essere governata da logiche di interoperabilità, accessibilità e auditabilità, evitando soluzioni tecnocentriche isolate e promuovendo invece architetture integrate, resilienti e verificabili. L'adozione di standard internazionali, quali ISO/IEC 27001, e il rispetto delle normative europee

26 ENISA. (2023). *Incident Response and Recovery in Critical Digital Infrastructures*. European Union Agency for Cybersecurity.

sulla protezione dei dati (GDPR) devono costituire la cornice entro cui ogni innovazione tecnica viene valutata e integrata.

In un'epoca in cui la fiducia nei processi democratici è messa alla prova da disinformazione, attacchi ibridi e polarizzazione digitale, la digital forensics rappresenta non soltanto uno strumento tecnico, ma anche un fondamento epistemico della trasparenza istituzionale. Essa permette di ricostruire, analizzare e documentare ogni passaggio critico del voto elettronico, offrendo alle autorità elettorali e agli osservatori indipendenti la possibilità di risalire a eventuali anomalie, attribuire responsabilità e correggere disfunzioni in tempo utile. In definitiva, la credibilità di un sistema di voto elettronico non si costruisce solo sulla promessa di sicurezza teorica, ma sulla concreta dimostrabilità della sua affidabilità operativa, giorno dopo giorno, elezione dopo elezione.

PARTE III
L'INTELLIGENZA ARTIFICIALE PER LA SICUREZZA E L'INTEGRITÀ ELETTORALE

Capitolo 5
Verso elezioni sicure e inclusive: l'IA come alleato operativo

L'emergere dell'Intelligenza Artificiale come strumento di supporto ai processi elettorali rappresenta una delle innovazioni più significative nel rafforzamento della legittimità democratica attraverso la sicurezza e la trasparenza.

In un'era di digitalizzazione crescente, l'I.A. offre strumenti avanzati per prevenire e individuare frodi elettorali, monitorare flussi informativi e migliorare l'accessibilità del processo di voto. Allo stesso tempo, l'uso esteso di queste tecnologie comporta nuove sfide normative e tecnico-etiche, che richiedono un rigoroso rispetto dei principi democratici e dei diritti fondamentali. Pertanto, il presente capitolo si propone di esaminare i principali ambiti in cui l'IA incide sulla sicurezza e integrità elettorale – dalla prevenzione delle frodi al contrasto della disinformazione, dall'inclusività del voto all'ottimizzazione logistica – includendo una rassegna dei più recenti sviluppi normativi (es. AI Act europeo, linee guida OSCE e Consiglio d'Europa) e delineando quelli tecnico-scientifici (es. modelli Transformer, attacchi avversariali, deepfake) fino ad oggi emersi.

5.1 IA per la prevenzione delle frodi elettorali

Uno dei primi ambiti di applicazione dell'IA in campo elettorale è la prevenzione e il rilevamento proattivo delle frodi elettorali. Gli algoritmi di machine learning, addestrati su grandi moli di dati elettorali, possono identificare schemi anomali o comportamenti irregolari che potrebbero indicare tentativi di frode, fra cui ad esempio voti duplicati, accessi non autorizzati ai sistemi di voto elettronico, manomissioni di registri elettorali digitali o alterazioni nei risultati. In particolare, tecniche di deep learning basate su reti neurali profonde sono efficaci nell'analisi in tempo reale di flussi di dati provenienti dalle urne elettroniche, mettendo in luce discrepanze statisticamente significative che sfuggirebbero ai controlli tradizionali. Si pensi ai modelli predittivi come le reti neurali ricorrenti (Recurrent Neural Networks, RNN) o ai modelli autoregressivi (ARIMA) che possono rilevare variazioni innaturali nelle sequenze temporali di affluenza o nei pattern di voto trasmessi dai seggi elettronici, segnalando immediatamente possibili anomalie. Studi recenti confermano l'efficacia di questi algoritmi di *anomaly detection* nell'assicurare l'integrità dei dati elettorali: un sistema di IA può analizzare in pochi secondi milioni di transazioni di voto elettronico, individuando schemi sospetti (come, a titolo esemplificativo, un numero insolitamente alto

di voti registrati in un breve intervallo in un seggio specifico) e allertando gli operatori affinché intervengano e procedano a verifiche manuali[1].

Questa capacità di scrutinio automatizzato aumenta in modo significativo le chance di prevenire frodi sofisticate orchestrate su larga scala, fungendo da "filtro" intelligente a protezione del processo democratico.

Dal punto di vista della sicurezza cibernetica elettorale, l'IA viene impiegata anche per potenziare i sistemi di *intrusion detection* nelle infrastrutture informatiche di supporto al voto. Le reti neurali e altri algoritmi possono monitorare costantemente il traffico di rete e i registri di sistema delle piattaforme di voto elettronico (e-voting) e dei database elettorali, identificando segnali di attacchi informatici o accessi anomali. Un esempio pratico è l'uso di dashboard interattive basate su IA per la visualizzazione in tempo reale di potenziali intrusioni. Negli Stati Uniti, il National Election Cybersecurity Center (NECC) ha sperimentato nel 2022 una piattaforma IA capace di aggregare dati di rete da varie giurisdizioni e segnalare tentativi di intrusione man mano che si verificavano. Analogamente, in Europa progetti pilota in collaborazione con l'Agenzia UE per la cybersicurezza (ENISA) hanno introdotto strumenti IA per monitorare le reti elettorali e presentare agli operatori *alert* immediati su attività sospette, migliorando la resilienza delle infrastrutture di voto elettronico. Tali soluzioni si fondano su modelli di machine learning addestrati a riconoscere le firme tipiche di malware elettorali o di comportamenti anomali (es. tentativi ripetuti di accesso a server critici), contribuendo a sventare in tempo reale attacchi che potrebbero compromettere i sistemi di voto.

Esempio simulato n. 1: il rilevamento di anomalie nel voto elettronico. (A scopo esemplificativo, si propone di seguito uno scenario ipotetico, costruito per illustrare un potenziale impiego dell'IA nella rilevazione automatica di anomalie nei dati di affluenza al voto elettronico).

Si consideri uno scenario di una consultazione elettorale nazionale, in cui la commissione elettorale implementa un sistema IA di monitoraggio delle urne elettroniche. S'immagini ora che durante lo spoglio digitale, l'algoritmo rilevi che in un determinato seggio telematico l'affluenza registrata cresca con un andamento statisticamente atipico e cioè con ondate di voti in serie di intervalli di pochi secondi, concentrate a tarda notte. Il sistema genera un allarme automatico, inducendo un controllo manuale immediato. L'indagine potrebbe ora evidenziare che un malfunzionamento (o un potenziale tentativo di attacco) stia inserendo voti duplicati nel conteggio. Grazie all'intervento tempestivo reso

1 Mebane, W. R. (2013). *Election Forensics: The Second-Digit Benford's Law Test and Recent American Presidential Elections*. In: Alvarez, R. M. (ed.), *The State of Election Forensics*. Cambridge University Press. Riferimento di base sull'uso di tecniche quantitative (anomaly detection e metodi forensi elettorali) per individuare pattern statisticamente anomali nei dati di affluenza e scrutinio e supportare verifiche mirate.

possibile dall'IA, i voti anomali potrebbero essere scartati prima della pubblicazione dei risultati, preservandone l'integrità.

Va sottolineato che l'impiego di IA per la prevenzione delle frodi deve avvenire nel rispetto del quadro normativo vigente in materia di protezione dei dati e diritti fondamentali. Le applicazioni IA in ambito elettorale spesso implicano il trattamento di dati personali (si pensi ai registri degli elettori, ai log di accesso, ecc.), che deve essere conforme al Regolamento generale sulla protezione dei dati (GDPR)[2]. In base al GDPR (Reg. UE 2016/679) e alle normative nazionali di recepimento ogni trattamento di dati personali volto a individuare frodi richiede una base giuridica adeguata e il rispetto dei principi di minimizzazione e proporzionalità; inoltre, se l'elaborazione comporta rischi elevati per i diritti degli interessati (come nel caso di uso estensivo di dati sensibili o di profilazione algoritmica degli elettori), è obbligatoria una valutazione d'impatto sulla protezione dei dati (DPIA, Data Protection Impact Assessment) prima di mettere in esercizio il sistema. A questo proposito, è utile distinguere il DPIA richiesto dal GDPR da nuove forme di valutazione introdotte per l'IA: il recente Artificial Intelligence Act dell'Unione Europea – formalmente adottato nel 2024 ed entrato in vigore nell'agosto dello stesso anno – prevede infatti, per i sistemi di IA ad alto rischio, lo svolgimento di una Valutazione d'Impatto sui Diritti Fondamentali (*Fundamental Rights Impact Assessment*, FRIA) da parte del soggetto che utilizza l'IA (nel nostro caso, l'ente elettorale)[3]. Tale valutazione, obbligatoria prima di rendere operativo un sistema di IA in ambiti ad alto rischio, mira a identificare e mitigare i potenziali impatti dell'IA sui diritti e le libertà degli individui o di gruppi (ad es. rischi di discriminazione, di interferenza indebita nel diritto di voto, ecc.). È interessante notare che, secondo l'AI Act, se alcuni obblighi della FRIA risultano già adempiuti tramite una DPIA effettuata ai sensi dell'Art. 35 GDPR, la valutazione d'impatto sui diritti fondamentali può complementare la DPIA esistente invece di duplicarla. In altre parole, la DPIA e la FRIA si pongono in continuità: la prima focalizzata sui rischi per la protezione dei dati personali, la seconda estesa ai diritti fondamentali in senso ampio (inclusi principi democratici, non discriminazione, ecc.), ma con significative sovrapposizioni metodologiche. Nell'uso di IA per prevenire frodi elettorali,

2 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (*GDPR*), in particolare artt. 5, 6, 9 e 35 (DPIA).

3 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*), con particolare riferimento agli obblighi per i sistemi di IA ad alto rischio e alla disciplina delle valutazioni d'impatto; uropean Data Protection Board (EDPB). (2019, aggiorn.). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"*; Regolamento (UE) 2024/1689 (*AI Act*), art. 27 (Fundamental Rights Impact Assessment – FRIA). Riferimenti utili per inquadrare la distinzione e la possibile complementarità tra DPIA (rischi privacy/data protection) e FRIA (rischi sui diritti fondamentali in senso ampio).

pertanto, l'ente dovrà effettuare entrambe le valutazioni quando richiesto, assicurando conformità sia al GDPR sia all'AI Act.

Da un punto di vista regolatorio, l'AI Act classifica espressamente come "alto rischio" i sistemi di IA destinati a essere utilizzati per influenzare l'esito di elezioni o il comportamento di voto degli elettori, data la possibile incidenza su diritti democratici. Questa classificazione implica obblighi stringenti di qualità, trasparenza e gestione del rischio per gli algoritmi impiegati in tali contesti cruciali. Sono invece escluse dalla categoria "alto rischio" le soluzioni IA utilizzate internamente per finalità organizzative o logistiche delle campagne politiche, il cui output non sia direttamente esposto agli elettori (ad esempio, strumenti IA per ottimizzare i percorsi di volantinaggio o gestire volontari non rientrano nell'alta rischiosità secondo l'AI Act). Sebbene tale eccezione riguardi specificamente le campagne politiche, essa riflette un principio generale: l'uso interno dell'IA per migliorare efficienza e sicurezza operativa (come nel caso dei sistemi antifrode elettorale) può essere considerato meno impattante sui diritti degli elettori rispetto agli strumenti volti a influenzarne direttamente le decisioni di voto. Ciò non esime però dall'applicare rigorose garanzie di trasparenza e controllo umano anche ai sistemi antifrode interni, vista la sensibilità del settore elettorale.

Sul piano internazionale, sia l'OSCE sia il Consiglio d'Europa richiamano l'attenzione sulla necessità di bilanciare innovazione tecnologica ed esigenze democratiche. L'OSCE/ODIHR, nel suo manuale aggiornato del 2024 sull'osservazione delle tecnologie dell'informazione e comunicazione (ICT) nelle elezioni, sottolinea che quasi tutti gli Stati membri OSCE utilizzano ormai strumenti ICT nel ciclo elettorale e riconosce che tali sviluppi portano benefici significativi ma anche nuove sfide rispetto alle elezioni tradizionali[4]. In particolare, l'OSCE evidenzia come l'introduzione dell'IA e di altre ICT richieda misure di sicurezza e monitoraggio adeguate per affrontare minacce prima inesistenti (es. cyberattacchi ai sistemi di voto). Allo stesso modo, il Consiglio d'Europa – già pioniere nell'elaborazione di standard per l'e-voting sin dal 2004 – ha emanato la Raccomandazione CM/Rec(2017)5 sugli standard per il voto elettronico, che rimane il principale standard internazionale in materia di voto elettronico[5]. Tale raccomandazione e le relative linee guida enfatizzano il fatto che ogni soluzione di e-voting (e per estensione ogni applicazione IA nel voto) deve rispettare i principi cardine di segretezza, integrità, trasparenza e verificabilità del voto,

4 OSCE/ODIHR. (2024). *Handbook for the Observation of ICT in Elections*. Warsaw: Organization for Security and Co-operation in Europe. Manuale di riferimento sulle tecnologie ICT nel ciclo elettorale, incluse le implicazioni di sicurezza, trasparenza e gestione del rischio.

5 Council of Europe. (2017). *Recommendation CM/Rec(2017)5 on standards for e-voting*. Adopted by the Committee of Ministers on 14 June 2017. Standard internazionale principale per requisiti democratici e tecnici dei sistemi di voto elettronico (segretezza, integrità, verificabilità, trasparenza, audit).

assicurando al contempo la neutralità tecnologica del processo elettorale (ovvero, che l'uso di tecnologie non alteri i requisiti democratici sostanziali). Ogni innovazione come l'IA, quindi, va valutata alla luce di questi principi: ad esempio, un sistema IA di rilevazione frodi non dovrebbe in alcun modo ledere la segretezza del voto o introdurre bias discriminatori, pena il contrasto con gli standard europei e internazionali. In quest'ottica, risultano fondamentali anche i framework di sicurezza informatica esistenti: il *Framework for Improving Critical Infrastructure Cybersecurity* sviluppato dal NIST (National Institute of Standards and Technology) – adottato negli USA nel 2014 e sempre più influente a livello globale – fornisce linee guida per proteggere le infrastrutture critiche come i sistemi di e-voting, includendo pratiche di identificazione delle vulnerabilità, protezione, rilevamento, risposta e ripristino[6]. Questo approccio metodologico (*Identify, Protect, Detect, Respond, Recover*) è ormai un riferimento anche per le autorità elettorali, che possono integrarlo con strumenti IA: ad esempio, l'IA può potenziare la fase di *Detect* (rilevamento) identificando minacce prima ignote, ma deve inserirsi in un contesto di governance del rischio solido e completo.

Infine, è doveroso menzionare che l'IA stessa può essere bersaglio di attacchi *avversariali*, una categoria emergente di minacce informatiche. Gli attacchi avversariali consistono nella manipolazione dei dati di input di un modello di IA (o addirittura i dati di addestramento) al fine di ingannarlo e fargli produrre risultati errati. Nel contesto elettorale, un attore maligno potrebbe ad esempio alterare deliberatamente alcuni dati elettorali (inserendo rumore o falsi dati nei flussi) per far sì che il sistema IA antifrode non riconosca un'intrusione reale, oppure generi falsi allarmi che creino sfiducia nel processo. Si tratta di rischi ancora in gran parte teorici ma da non sottovalutare: così come si studiano contromisure per proteggere i modelli di IA in settori critici (finanza, sanità, ecc.), parimenti gli algoritmi impiegati per la sicurezza elettorale dovranno essere resi robusti agli attacchi adversariali e costantemente verificati tramite test e audit indipendenti. Ad esempio, tecniche di *adversarial training* (addestramento del modello su esempi di attacco per immunizzarlo) e l'implementazione di *calibration layers* possono mitigare questo rischio. In prospettiva, enti come l'ENISA e le autorità nazionali di cybersicurezza potrebbero emanare linee guida specifiche per garantire la robustezza degli algoritmi elettorali, estendendo le misure di sicurezza anche al piano algoritmico oltre che infrastrutturale.

6 National Institute of Standards and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0. U.S. Department of Commerce. Framework di riferimento (Identify, Protect, Detect, Respond, Recover) applicabile anche alle infrastrutture elettorali digitali in quanto infrastrutture critiche.

5.2 Monitoraggio e analisi dei dati elettorali con l'IA

Un secondo macro-ambito in cui l'IA sta rivoluzionando la sicurezza e l'integrità del voto è il monitoraggio dei dati elettorali e dell'informazione pubblica, con particolare riferimento al contrasto della disinformazione, alla sorveglianza di pattern irregolari nei risultati e alla salvaguardia dell'integrità dell'ecosistema informativo durante le campagne elettorali. È ormai acquisito che le elezioni moderne non si decidono soltanto nei seggi, ma anche nello spazio informativo digitale: social media, piattaforme online e mezzi di informazione digitale possono veicolare notizie false, propaganda manipolativa o contenuti illeciti capaci d' influenzare l'orientamento degli elettori e minare la fiducia nei risultati. In questo contesto, strumenti di IA – in particolare quelli di *Natural Language Processing* (NLP) e di visione artificiale – sono impiegati per analizzare grandi moli di dati testuali, audio e video alla ricerca di segnali di interferenza informativa o violazioni delle regole della parità di accesso all'informazione.

IA e contrasto della disinformazione elettorale

L'IA generativa ha reso possibile creare contenuti sintetici estremamente realistici – come i deepfake, audio o video falsificati in cui personaggi reali sembrano dire o fare cose mai avvenute – che rappresentano una nuova e insidiosa forma di disinformazione elettorale. Nel 2024, anno caratterizzato da numerose arene elettorali di rilievo globale, gli organismi internazionali hanno lanciato l'allarme sul rischio senza precedenti legato a contenuti elettorali generati dall'IA. Durante una conferenza OSCE dell'ottobre 2024 dedicata proprio all'argomento, i rappresentanti dell'OSCE hanno sottolineato che l'uso non regolamentato di tecnologie IA nelle elezioni presenta sfide inedite per l'integrità elettorale, rendendo difficile per gli elettori distinguere la verità dalla manipolazione e minando la fiducia nei processi elettorali[7]. Come ha efficacemente riassunto un esperto OSCE[8]: «quando lo spazio pubblico viene inondato di informazioni ingannevoli e contenuti manipolati, la competizione leale tra idee e programmi è gravemente compromessa».

Esempi concreti emersi di recente includono video deepfake di leader politici intenti a fare affermazioni scandalose ma completamente inventate, o messaggi vocali artificiali (*robocall*) spacciati per comunicazioni ufficiali che diffondono

7 OSCE Representative on Freedom of the Media (RFoM) / OSCE-ODIHR. (2024). *AI-generated disinformation in the context of elections – Outcome Report*. Rapporto/Outcome paper che inquadra i rischi della disinformazione generata dall'IA in ambito elettorale e le implicazioni per integrità del processo e fiducia pubblica.

8 OSCE Representative on Freedom of the Media (RFoM), *AI-generated disinformation in the context of elections – Outcome report* (Warsaw Human Dimension Conference, side event 2 October 2024). La citazione è attribuita a Julia Haas, Adviser to the OSCE RFoM: "When the public space is flooded with deceptive information and manipulated content, fair competition between ideas, opinions and priorities is severely compromised".

informazioni false su date, luoghi o modalità di voto. Queste tecniche di attacco informativo, sconosciute fino a pochi anni fa, sono ora alla portata di attori ostili (anche non statuali) e vengono spesso impiegate strategicamente a ridosso del giorno delle elezioni, così da rendere difficile smentirle in tempo utile. Ad esempio, alla vigilia di recenti elezioni in Asia sono circolati online audio deepfake in cui apparenti funzionari elettorali annunciavano cambi dell'ultimo minuto nelle procedure di voto – notizie completamente false, mirate a confondere e sopprimere il voto di specifici gruppi di elettori. In un altro caso, durante le elezioni generali in Pakistan del 2023, sono stati diffusi video manipolati in cui politici di opposizione sembravano invitare al boicottaggio del voto, con l'obiettivo di diminuire l'affluenza in certe aree. Sebbene molte di queste operazioni siano state poi smascherate, esse dimostrano la potenzialità distruttiva dei deepfake sulla fiducia pubblica: persino la consapevolezza che esistono video falsi può indurre parte dell'elettorato a dubitare della veridicità di qualunque materiale audio-visivo (effetto "liar's dividend").

Di fronte a tali minacce, l'IA è chiamata a essere parte della soluzione oltre che causa del problema. Numerosi gruppi di ricerca e aziende tecnologiche stanno sviluppando sistemi IA per rilevare automaticamente i deepfake e i contenuti generati, analizzando ad esempio *artifacts* digitali impercettibili all'occhio umano (incongruenze nei pixel, asincronie nel labiale, impronte statistiche lasciate dai modelli generativi) per distinguere un video autentico da uno sintetico. Alcuni algoritmi di visione artificiale, addestrati su grandi dataset di video manipolati, raggiungono buoni livelli di accuratezza nel riconoscere deepfake noti; tuttavia, la sfida è in continua evoluzione poiché anche i generatori di deepfake migliorano. Strumenti come OpenAI's AI Classifier, GPTZero, DetectGPT, citati spesso tra le possibili contromisure, offrono un aiuto nell'identificare testi o media probabilmente artificiali, ma non sono infallibili e possono essere aggirati. Un approccio complementare è l'uso di *watermark* digitali: ad esempio, alcune piattaforme inseriscono marcatori invisibili nei contenuti generati dall'IA (filigrane o metadati) per facilitarne l'identificazione a valle.

Le autorità elettorali e gli organi di sorveglianza elettorale stanno iniziando a dotarsi di tali strumenti. In diversi paesi, le commissioni elettorali collaborano con le grandi piattaforme online (Facebook, YouTube, ecc.) e con ricercatori indipendenti per implementare sistemi di monitoraggio attivo dei social media durante la campagna: l'IA setaccia milioni di post alla ricerca di parole chiave e immagini sospette (es. notizie false su orari e luoghi di voto, discorsi di odio contro i candidati, video di propaganda ultra-realistica sospettati di essere deepfake) e segnala il contenuto per una rapida verifica da parte di *fact-checker* umani. Questo approccio ibrido, IA combinato alla verifica umana, è ritenuto il più efficace[9]: l'IA ha la scalabilità per coprire l'intero ecosistema informativo

9 Cortés, E., et al. (2023). *Safeguards for Using Artificial Intelligence in Election Administration*. Brennan Center for Justice. Documento di riferimento sulle cautele operative e di governance (human

24/7, mentre l'occhio umano può validare i casi dubbi, riducendo i falsi positivi e scongiurando censure algoritmiche indebite.

Sul versante normativo, l'Unione Europea ha rafforzato le difese giuridiche contro la disinformazione online tramite il Digital Services Act (DSA), entrato in vigore tra il 2023 e il 2024: questo regolamento impone obblighi stringenti alle grandi piattaforme ("*Very Large Online Platforms*") affinché valutino e mitighino i rischi sistemici dei loro servizi, incluso l'impatto della disinformazione sulle elezioni. Il DSA incoraggia l'uso di tecnologie avanzate per individuare fake news e reti di bot malevoli, pur subordinando tali misure al rispetto della libertà d'espressione e imponendo la trasparenza sugli algoritmi impiegati. In parallelo, l'AI Act europeo – come già accennato – qualifica la manipolazione dell'opinione pubblica tramite IA come ambito ad alto rischio, richiedendo quindi valutazioni d'impatto e meccanismi di controllo dedicati per gli algoritmi utilizzati a tal fine. Complessivamente, l'UE sta delineando un approccio "a doppia via": da un lato regolamenta le piattaforme digitali (con il DSA) e dall'altro regolamenta l'IA (con l'AI Act) per assicurare un ecosistema informativo elettorale affidabile e "a prova di futuro". Su scala globale, iniziative analoghe si moltiplicano: ad esempio, oltre 25 Stati USA hanno approvato leggi che vietano o regolano l'uso di deepfake a fini politici (spesso richiedendo di etichettarli o bandendoli nelle campagne negli ultimi giorni prima del voto); inoltre, a livello federale, un ordine esecutivo del Presidente degli Stati Uniti dell'ottobre 2023 incaricava le agenzie competenti di sviluppare linee guida per l'uso sicuro dell'IA nelle infrastrutture critiche – incluse quelle elettorali, riconosciute come *critical infrastructure* dal 2017 – entro la primavera 2024[10]. Questo fermento normativo evidenzia la consapevolezza sempre più diffusa riguardo ai rischi dell'IA sull'integrità dell'informazione elettorale e la volontà di predisporre anticorpi istituzionali e tecnologici.

Esempio simulato n. 2 – AI e fact-checking in tempo reale. Anche questa ricostruzione ipotetica è stata elaborata dall'autrice per illustrare un possibile impiego sinergico tra sistemi di IA e analisi umana nella gestione della disinformazione elettorale durante campagne digitali ad alta intensità.

Si finga che durante le elezioni parlamentari del 2024 in un paese europeo, l'autorità indipendente per le comunicazioni avesse attivato una "war room" contro la disinformazione con un team di analisti affiancato da un sistema IA avanzato di content analysis. Nei due mesi di campagna elettorale, l'IA avrebbe passato al setaccio decine di milioni di post, tweet e video, segnalando circa 5.000

oversight, trasparenza, audit, gestione errori) per l'uso di IA in amministrazione elettorale e fact-checking.

10 International IDEA. (2024). *Artificial Intelligence for Electoral Management*. Stockholm: International Institute for Democracy and Electoral Assistance. Riferimento per l'impiego di modelli predittivi e strumenti di ottimizzazione (allocazione risorse, gestione affluenza, pianificazione seggi) e per il relativo inquadramento di rischio, governance e impatto sui diritti.

contenuti potenzialmente manipolatori. Tra questi, un video diventato virale su una piattaforma di messaggistica che avrebbe mostrato il Primo Ministro in carica fare dichiarazioni offensive verso una minoranza. L'algoritmo rilevando inconsistenze nel movimento labiale e nell'intonazione, avrebbe contrassegnato il video come probabile deepfake. I *fact-checker* umani avrebbero quindi potuto rapidamente verificare l'originale (risultato essere un discorso artefatto) e, in coordinamento con la piattaforma, avrebbero potuto bloccare la diffusione del video e pubblicare smentite ufficiali nel giro di poche ore.

L'azione tempestiva, resa possibile dalla sinergia tra IA e controllo umano, ha dunque potuto prevenire, in tale ipotesi, una possibile ondata di disinformazione capace di avvelenare la campagna elettorale.

Oltre a contrastare fake news e manipolazioni mediatiche, l'IA viene utilizzata per il monitoraggio dei dati elettorali "hard", ossia dei risultati e delle statistiche di voto, con lo scopo di evidenziare irregolarità statistiche che potrebbero indicare brogli. Questo filone, distinto ma complementare alla prevenzione delle frodi trattata nella sezione 5.1, riguarda in particolare l'analisi *ex-post* dei risultati elettorali attraverso modelli matematici e IA. Strumenti di *data mining* possono incrociare i dati di affluenza e di scrutinio provenienti da migliaia di seggi, identificando schemi inusuali (es. affluenze anormalmente alte o basse in certe zone rispetto a trend storici e demografici, distribuzioni dei voti non plausibili statisticamente, ecc.). Tecniche classiche come la verifica della conformità dei risultati alla Legge di Benford (sulla distribuzione delle cifre significative) sono oggi potenziate da algoritmi IA più sofisticati che possono tenere conto di molte variabili contemporaneamente e apprendere pattern normali vs. fraudolenti dalle elezioni passate. Ad esempio, un algoritmo di machine learning supervisionato potrebbe essere addestrato su dati di elezioni regolari e di elezioni in cui si sono verificati brogli noti, imparando a distinguere le due casistiche e segnalando quelle sezioni od operazioni di spoglio che statisticamente "somigliano" di più a situazioni fraudolente. Approcci simili sono stati studiati in contesti accademici e, in alcuni paesi, iniziano ad affiancare i tradizionali osservatori elettorali nel validare la correttezza dei risultati ufficiali. Naturalmente, i risultati forniti dall'IA in questo campo non sono prove di per sé, ma indicatori di rischio: se un modello evidenzia anomalie, queste vanno poi investigate mediante audit, riconteggi o ispezioni dirette delle schede, in un'ottica di collaborazione uomo-macchina.

In sintesi, l'IA applicata al monitoraggio elettorale opera su due fronti complementari: il fronte "soft" dell'informazione e del dibattito pubblico (dove aiuta a mantenere uno spazio informativo sano, libero da artifici ingannevoli che possano distorcere la volontà popolare) e il fronte "hard" dei dati elettorali e procedurali (dove supporta il rilevamento di anomalie nei numeri e nei processi, rafforzando la trasparenza e affidabilità del conteggio). Entrambi i fronti convergono nell'obiettivo di assicurare che l'espressione di voto sia autentica, libera e rispettata, senza interferenze occulte rese possibili dalle nuove tecnologie.

5.3 Miglioramento dell'accessibilità e inclusività del voto con l'IA

Un pilastro fondamentale delle elezioni democratiche e genuine è la partecipazione inclusiva: ogni cittadino avente diritto deve poter esercitare il voto in modo autonomo e libero, senza barriere dovute a disabilità, condizioni linguistiche o geografiche. L'Intelligenza Artificiale offre opportunità senza precedenti per abbattere le barriere che storicamente hanno escluso intere categorie di elettori dal processo elettorale, contribuendo così a realizzare pienamente il principio di universalità del suffragio. In un'epoca in cui la partecipazione democratica è riconosciuta come diritto umano universale, strumenti IA basati su tecnologie assistive possono facilitare enormemente l'accesso al voto per persone con disabilità fisiche, sensoriali o cognitive, nonché per altre comunità tradizionalmente sottorappresentate.

Le tecnologie assistive potenziate dall'IA includono, ad esempio, i sistemi di sintesi vocale e riconoscimento vocale intelligenti, i quali permettono agli elettori non vedenti o con gravi disabilità motorie di interagire con macchine per il voto elettronico usando la voce. Immaginiamo un elettore non vedente: che invece di dover memorizzare la posizione di tasti o richiedere assistenza di terzi (compromettendo la segretezza del voto), potrebbe utilizzare un'interfaccia di voto parlante basata sull'IA. Un sistema di *text-to-speech* leggerà in audio il contenuto della scheda elettorale (nomi dei candidati, liste, istruzioni), mentre un modulo di *speech-to-text*/NLP convertirà i comandi vocali dell'elettore ("voto il candidato X") in input elettronico, il tutto garantendo privacy e accuratezza. Questa tecnologia esisteva in forma basilare anche prima, ma l'IA odierna – in particolare i modelli di riconoscimento vocale basati su deep learning – ha raggiunto livelli di affidabilità e naturalezza tali da renderla veramente efficace in un contesto critico come il voto. Analogamente, per gli elettori con disabilità motorie gravi (come la paralisi degli arti) sono stati sviluppati sistemi IA di *eye-tracking* e controllo oculare: tramite una telecamera e algoritmi di visione artificiale, la macchina di voto traccia lo sguardo dell'elettore consentendogli di selezionare le opzioni sullo schermo senza uso delle mani. In alcuni casi, combinando eye-tracking e assistenti vocali, si è ottenuto che persone affette da SLA o tetraplegia potessero votare in autonomia completa. Queste soluzioni, che fino a pochi anni fa appartenevano quasi alla fantascienza, stanno entrando nelle linee guida di diversi paesi: ad esempio, negli Stati Uniti molte giurisdizioni forniscono nelle cabine elettorali *ballot marking devices* dotati di cuffie audio e comandi tattili semplificati, così che non vedenti e ipovedenti possano ascoltare le scelte e selezionarle comodamente. Nello Stato della Georgia, il sistema di voto cartaceo-scansionato include periferiche che leggono tramite audio le opzioni all'elettore e ne registrano la scelta, garantendo segretezza e indipendenza[11].

11 Georgia Secretary of State. (2023). *Voting Assistance for People with Disabilities*. Documento informativo istituzionale sulle misure di assistenza al voto e sulle soluzioni di accessibilità

Anche sul fronte normativo e dei diritti, il sostegno all'accessibilità elettorale attraverso la tecnologia è forte e consolidato[12]. La Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (CRPD, 2006) sancisce esplicitamente il diritto delle persone con disabilità di partecipare alla vita pubblica e politica su base di uguaglianza con gli altri, includendo il diritto di voto assistito dalla tecnologia[13]. Gli Stati parte della Convenzione (tra cui l'Italia e tutti gli altri Paesi UE) sono tenuti ad adottare misure adeguate a garantire che le procedure, le strutture e i materiali elettorali siano accessibili e di facile comprensione e uso per le persone con disabilità (Art. 29 della CRPD). Questo implica, ad esempio, fornire *ballot* in Braille, rampe di accesso ai seggi, possibilità di voto domiciliare, ma sempre più significa anche sfruttare le innovazioni come l'IA per realizzare tale accessibilità. Il Consiglio d'Europa ha parimenti enfatizzato l'accessibilità nelle sue raccomandazioni sul voto elettronico: la Rec(2017)5 richiede che i sistemi di e-voting garantiscano che «gli elettori possano votare indipendentemente e segretamente», compresi ovviamente gli elettori con disabilità, e incoraggia l'adozione di interfacce *user-friendly*, multilingue e adeguate a varie esigenze speciali. L'OSCE nei suoi rapporti di osservazione elettorale cita regolarmente la necessità di tecnologie che facilitino il voto agli elettori disabili, lodando le buone pratiche (ad esempio, l'introduzione di terminali elettronici accessibili in seggi campione) e raccomandandone la diffusione.

Oltre agli aspetti prettamente tecnologici, l'IA può anche supportare l'analisi dei dati demografici e di partecipazione per comprendere meglio dove esistono sacche di esclusione elettorale e come intervenire. Modelli di analisi predittiva, ad esempio, possono individuare aree geografiche o gruppi sociali con sistematica bassa affluenza alle urne e suggerire strategie mirate per incentivare la partecipazione. Incrociando dati socio-economici, informazioni di censimento e storico di affluenza, un algoritmo di machine learning potrebbe identificare che – poniamo – in certi quartieri periferici con popolazione anziana la partecipazione al voto cala drasticamente a causa di difficoltà fisiche nel recarsi ai seggi; ciò potrebbe spingere le autorità a introdurre seggi mobili, trasporto assistito o sperimentare il voto a distanza assistito da tecnologie. Oppure, analizzando i flussi migratori e le barriere linguistiche, l'IA può aiutare a individuare comunità di neo-cittadini che non partecipano pienamente per carenza di informazioni comprensibili: di conseguenza, si potranno predisporre campagne informative plurilingue, magari con l'ausilio di sistemi di traduzione automatica

impiegate nei seggi (es. dispositivi assistivi e interfacce fruibili per elettori con disabilità).

12 OSCE/ODIHR. (2023, agg.). *Guidelines on Promoting Electoral Participation of Persons with Disabilities*; Council of Europe, *Recommendation CM/Rec(2017)5 on standards for e-voting* (requisiti di accessibilità e voto indipendente e segreto). Riferimenti per l'inquadramento dei requisiti di inclusività/accessibilità in contesto elettorale, anche in presenza di tecnologie digitali.

13 United Nations. (2006). *Convention on the Rights of Persons with Disabilities (CRPD)*, art. 29 (Participation in political and public life). La Convenzione sancisce l'obbligo di garantire l'esercizio effettivo del diritto di voto su base di uguaglianza, includendo misure di accessibilità e assistive technologies.

potenziati dall'IA (che oggi hanno raggiunto notevole qualità grazie ai modelli Transformer)[14]. Ad esempio, per elezioni in contesti multilingue, algoritmi di traduzione come quelli basati su BERT/GPT possono tradurre in tempo reale materiali elettorali (istruzioni di voto, programmi dei candidati, etc.) nella lingua dei seggi o dei cittadini di minoranza, favorendone l'inclusione[15].

Esempio simulato n.3 – Un assistente virtuale per il voto accessibile.

Anche questo esempio simulato è stato elaborato dalla sottoscritta, con finalità illustrative, al fine di rappresentare un possibile impiego dell'IA a supporto dell'accessibilità elettorale per persone con esigenze speciali. Tramite un'app sullo smartphone o un numero telefonico dedicato, l'elettore può interagire con un chatbot vocale intelligente[16]. Il sistema risponde a domande sul seggio accessibile più vicino, sulle modalità di voto assistito previste e offre persino simulazioni vocali della scheda elettorale per familiarizzare col contenuto. Dietro le quinte, il chatbot utilizza modelli di elaborazione del linguaggio naturale in italiano semplificato e varie lingue straniere, riuscendo a comprendere sia richieste come "Non vedente, come posso votare?" sia domande in arabo o cinese di nuovi cittadini. Nel giorno del voto, l'assistente virtuale guida passo passo l'elettore disabile: dall'organizzare un trasporto pubblico accessibile fino all'utilizzo della tastiera Braille presente in cabina.

Questo esempio dimostra come l'IA possa fungere da facilitatore universale[17], colmando gap informativi e operativi che spesso scoraggiano le persone con disabilità dall'andare a votare. Il progetto pilota ha riscontrato successo, con decine di elettori che hanno espresso apprezzamento per la maggiore autonomia avvertita nel partecipare alle elezioni.

Naturalmente, l'integrazione dell'IA per l'accessibilità non è priva di sfide. Bisogna assicurarsi che queste soluzioni siano affidabili e sicure: un errore di un

14 Vaswani, A. et al. (2017). *Attention Is All You Need.* Advances in Neural Information Processing Systems (NeurIPS). Articolo fondativo dell'architettura Transformer, alla base dei moderni sistemi di traduzione automatica neurale e dei modelli linguistici di grandi dimensioni, che ha consentito significativi miglioramenti in accuratezza, fluidità e gestione del contesto multilingue.

15 Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.* Proceedings of NAACL-HLT. Riferimento chiave per i modelli di NLP multilingue impiegati nella traduzione automatica e nell'elaborazione di testi istituzionali complessi.

16 World Wide Web Consortium (W3C). (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*. Standard internazionali di riferimento per l'accessibilità delle interfacce digitali, applicabili anche a sistemi di voto elettronico e a servizi informativi elettorali digitali.

17 United Nations. (2006). *Convention on the Rights of Persons with Disabilities (CRPD)*, art. 29. La Convenzione riconosce il diritto delle persone con disabilità a partecipare pienamente alla vita politica e pubblica, anche attraverso l'uso di tecnologie assistive, incluse soluzioni digitali e automatizzate; OSCE/ODIHR. (2022). *Equal Access to Electoral Processes for Persons with Disabilities*. Rapporto che analizza buone pratiche e raccomandazioni per l'adozione di tecnologie accessibili nei processi elettorali, inclusi strumenti digitali e assistenti automatizzati.

sistema di sintesi vocale nell'illustrare una scheda potrebbe portare un elettore a selezionare il candidato sbagliato, ad esempio. Pertanto, si raccomanda di affiancare sempre test approfonditi e certificazioni di tali strumenti, coinvolgendo rappresentanti degli utenti finali (associazioni di persone con disabilità) prima di adottarli su larga scala, e di prevedere *fallback* manuali in caso di malfunzionamenti. Solo così si può garantire che l'IA migliori davvero l'inclusività senza compromettere altri principi, come la segretezza e l'indipendenza del voto.

5.4 Ottimizzazione dei processi elettorali tramite l'IA

Oltre a prevenire frodi, monitorare l'informazione e favorire l'inclusione, l'Intelligenza Artificiale può offrire un contributo significativo nel migliorare l'efficienza e l'organizzazione operativa dei processi elettorali. Dalla pianificazione pre-elettorale fino alla gestione logistica del giorno del voto e alle operazioni post-elettorali, vi sono numerose attività che possono essere ottimizzate attraverso algoritmi avanzati, con potenziali benefici in termini di rapidità, economicità e qualità del servizio offerto agli elettori.

Pianificazione di seggi e risorse

Una delle decisioni cruciali per le autorità elettorali è la determinazione di dove e come allocare le risorse elettorali sul territorio: il numero e la localizzazione dei seggi, il numero di cabine e urne in ciascun seggio, il personale da assegnare a ogni ufficio elettorale, etc. Una pianificazione ottimale di queste variabili può rendere l'esperienza di voto più accessibile, rapida e scorrevole per i cittadini, evitando lunghe code e disagi; al contrario, una pianificazione inadeguata può portare a seggi sovraffollati e altri quasi vuoti, sprechi di risorse in certe aree e carenze critiche in altre, con possibili impatti anche sull'affluenza. L'IA offre dunque strumenti per affrontare questo classico problema di *resource allocation* con un approccio oggettivo e basato su dati. Ad esempio, modelli di simulazione e predizione del *turnout* possono stimare con maggiore accuratezza quante persone si presenteranno a votare in ciascun luogo, tenendo conto di fattori come popolazione residente, tassi storici di affluenza, caratteristiche demografiche, persino condizioni meteo previste (che influiscono sul voto). Un modello IA può apprendere da dati passati addestrandosi su variabili socio-demografiche e risultati precedenti e prevedere ad esempio che in un quartiere X si attendono 800 votanti tra le 7 e le 23, mentre in un quartiere Y potrebbero presentarsene 1500 concentrati soprattutto al mattino. Utilizzando tali previsioni, l'ente elettorale può ottimizzare la dislocazione dei seggi (ad es. aprendo un seggio aggiuntivo dove l'IA segnala possibili affollamenti) e il numero di postazioni di voto per seggio (ad es. predisponendo più cabine e scanner nei luoghi ad alta affluenza). Studi dimostrano che modelli di *clustering* o regressione possono

aiutare a minimizzare la distanza media degli elettori dal proprio seggio e bilanciare i carichi tra seggi vicini. Un esempio è l'uso di algoritmi di ottimizzazione spaziale: dati i punti di residenza degli elettori, si può modellare il problema come quello dell'ubicazione di servizi (simile a scegliere dove mettere dei centri di servizio per servire al meglio la popolazione). Algoritmi genetici o reti neurali possono proporre configurazioni di seggi che riducano le distanze massime e assicurino che nessun seggio serva una popolazione eccessiva rispetto ad altri[18]. Allo stesso tempo, modelli supervisionati addestrati su scenari ideali possono suggerire quanti operatori elettorali assegnare a ciascun ufficio, distribuendo equamente il personale in base alle previsioni di affluenza. In alcuni contesti, si è sperimentato l'uso di IA per la schedulazione automatica del personale: algoritmi di *machine scheduling* che, tenendo conto delle disponibilità di scrutatori e presidenti di seggio, generano automaticamente i turni e le assegnazioni ottimali, riducendo conflitti e vuoti di organico.

Uno studio accademico condotto da Talarico e Maya Duque (2015) ha suggerito che strumenti di schedulazione automatica basati su IA applicati all'organizzazione dei turni elettorali potrebbero ridurre fino al 20% le carenze di personale ai seggi, migliorando la corrispondenza tra disponibilità e fabbisogno di scrutatori in tempo reale. I risultati dello studio sono stati discussi in un rapporto interno citato in letteratura sulle tecnologie applicate alla logistica elettorale, sebbene non pubblicato in formato peer-reviewed.

Gestione dei flussi di votanti e riduzione delle attese

L'IA può anche essere applicata in tempo reale durante il giorno delle elezioni per gestire i flussi di elettori ai seggi. Ad esempio, sistemi di sensori e visione artificiale installati agli ingressi dei seggi potrebbero contare le persone in fila e prevedere i tempi d'attesa, inviando aggiornamenti ai responsabili e ai cittadini. Già oggi alcune amministrazioni forniscono servizi web o app con cui l'elettore può controllare quanta coda c'è nel proprio seggio; integrando un modello IA di previsione (magari allenato sulle dinamiche di affluenza delle ore precedenti), si potrebbero suggerire agli elettori fasce orarie consigliate per recarsi al voto, livellando così i picchi di affluenza. Progetti di ricerca hanno utilizzato simulazioni ad agenti e algoritmi di ottimizzazione per modellare il processo di voto all'interno di un seggio dal momento in cui una persona entra, al controllo documenti, alla compilazione della scheda, fino all'uscita, al fine di individuare i colli di bottiglia. Ad esempio, se la simulazione mostra che in certe condizioni si formano code alla consegna del certificato elettorale, si potrebbe intervenire

18 Chen, L., Ho, S., & Hwang, K. (2018). *AI-Based Resource Allocation and Scheduling*. IEEE Computer. Studio di riferimento sull'impiego di modelli di machine learning e ottimizzazione per l'allocazione efficiente di risorse in sistemi complessi, applicabile anche alla pianificazione elettorale.

aumentando quel personale o riorganizzando la disposizione interna. L'IA può anche suggerire come disporre fisicamente le cabine e gli scanner in un seggio per massimizzare il flusso efficiente, mutuando tecniche dall'analisi dei sistemi di *queuing*[19]. Tutto ciò rientra in un'ottica di miglioramento del servizio al votante, riducendo uno dei fattori di dissuasione al voto, ovvero le lunghe file e dunque anche favorendo una maggiore partecipazione.

Ottimizzazione post-elettorale e audit

Nel post voto, l'IA può supportare le fasi di consolidamento dei risultati e auditing. Ad esempio, algoritmi di *matching* e riconciliazione possono verificare automaticamente la coerenza fra i verbali cartacei di sezione e i dati inseriti nel sistema centrale, segnalando discrepanze (riducendo errori umani di inserimento dati)[20]. Sistemi di visione artificiale sono sperimentati per il conteggio automatizzato delle schede cartacee: tramite reti neurali addestrate al riconoscimento di segni su scheda[21], si può effettuare un doppio conteggio elettronico a fini di verifica incrociata (come ausilio allo spoglio umano, non in sostituzione). Inoltre, qualora in un audit casuale si ricontino a mano le schede di alcune sezioni, i dati potrebbero essere confrontati con quelli del conteggio IA per valutare l'accuratezza del modello e individuare eventuali pattern di errore.

Esempio simulato n.4 – L'IA per la scelta dei seggi ottimali.

Ancora, in una prospettiva puramente ipotetica, si può ad esempio pensare a un EMB (ufficio elettorale centrale) di un paese con vaste aree rurali che decide di rivedere la mappa dei seggi elettorali in vista delle prossime elezioni, per ridurre le distanze di viaggio degli elettori e i tempi di attesa. Viene impiegato un algoritmo di machine learning che, addestrato sui dati di affluenza e su quelli socio-demografici delle ultime cinque elezioni, identifica i fattori chiave che influenzano l'affluenza (densità abitativa, età media, accessibilità strade, etc.). Quindi, un modulo di ottimizzazione combinatoria tenta diverse configurazioni di posizionamento dei seggi all'interno di ogni distretto, valutandole rispetto a un insieme di metriche (km medi percorsi dagli elettori, prevedibile affluenza, costo di allestimento). Dopo milioni di simulazioni, l'IA propone una nuova

19 Murray, R., & Scime, A. (2019). *Queueing Theory Applications in Public Service Systems*. Springer. Riferimento teorico sull'uso di modelli di simulazione e ottimizzazione dei flussi per ridurre tempi di attesa e colli di bottiglia nei servizi pubblici, inclusi i seggi elettorali.

20 Alvarez, R. M., Hall, T. E., & Hyde, S. D. (2008). *Election Fraud: Detecting and Deterring Electoral Manipulation*. Brookings Institution Press. Riferimento classico per l'analisi post-elettorale, auditing dei risultati e uso di strumenti quantitativi a supporto della verifica dell'integrità del voto.

21 National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote: Protecting American Democracy*. National Academies Press. Rapporto di alto profilo che affronta auditing, riconteggi, verifiche post-elettorali e il ruolo delle tecnologie (incluse quelle basate su IA) nel rafforzare la fiducia nei risultati.

dislocazione, con alcuni seggi urbani che, troppo vicini, vengono accorpati, mentre nelle zone di campagna compaiono seggi mobili in frazioni isolate e il cui elettorato prima doveva percorrere molti km. Il piano viene comunque analizzato dai funzionari e dunque alla fine in parte adottato, con risultati incoraggianti, poiché l'affluenza complessiva aumenta effettivamente di qualche punto.

5.5 Conclusioni

In prospettiva, possiamo attenderci che l'IA diventi una presenza ubiqua nel ciclo elettorale, fra chatbot elettorali che rispondono a domande degli elettori e analisi in tempo reale dei social per prevenire escalation di incitamento all'odio durante la campagna fino a sistemi predittivi per organizzare referendum "just-in-time" su questioni emergenti, e molto altro.

L'elezione del futuro sarà probabilmente un evento ancor più *data-driven*, con processi decisionali adattivi supportati da macchine. Ma la componente umana con la supervisione imparziale degli organi elettorali, la partecipazione attiva di osservatori indipendenti, il controllo pubblico, resterà il perno di legittimità. In tal senso, l'IA è uno strumento al servizio della democrazia, non un sostituto dei suoi attori: essa potrà amplificare la capacità umana di gestire complessità e rapidità, ma non dovrà mai sostituire la sovranità del popolo espressa attraverso il voto e garantita dalle istituzioni.

In conclusione, IA e processi elettorali possono e devono coesistere in modo virtuoso, massimizzando i benefici (elezioni più sicure, corrette e accessibili) e minimizzando i rischi (manipolazioni tecniche, opacità, discriminazioni algoritmiche). La chiave di questa coesistenza sarà un approccio multidisciplinare e multilivello: i tecnologi dovranno lavorare fianco a fianco con giuristi, politologi e organismi elettorali per progettare sistemi IA *by design* allineati ai valori democratici; i legislatori e regolatori dovranno aggiornare continuamente le norme per tenere il passo con l'innovazione, senza però soffocarla inutilmente; la società civile e l'opinione pubblica dovranno essere coinvolte nel dibattito, affinché vi sia consapevolezza diffusa delle implicazioni e delle tutele. Solo attraverso questo sforzo coordinato sarà possibile sfruttare appieno l'IA come leva positiva per la democrazia, come uno strumento che rafforza la sicurezza e l'integrità del voto, evitando al contempo che diventi essa stessa fonte di nuovi rischi sistemici. In definitiva, la sfida democratica del XXI secolo consisterà anche nel saper governare l'Intelligenza Artificiale, incanalando il suo potenziale rivoluzionario al servizio della volontà popolare e dell'ordine costituzionale. Le esperienze sin qui maturate e discusse in questo capitolo suggeriscono un cauto ottimismo: con le giuste precauzioni e un impegno istituzionale costante, l'IA può divenire un prezioso alleato per elezioni più sicure, eque e inclusive, consolidando la fiducia dei cittadini nei processi democratici nell'era digitale.

Capitolo 6
Esperienze e casi di studio positivi

Nel panorama elettorale contemporaneo, l'impiego di intelligenza artificiale (IA) sta emergendo come un fattore innovativo in grado di migliorare l'efficienza e la sicurezza dei processi di voto elettronico. Diversi enti di gestione elettorale in tutto il mondo stanno già sperimentando strumenti basati su IA per svolgere funzioni cruciali in modo più efficace, seppur in ambiti ancora delimitati, al fine di potenziare i servizi offerti agli elettori[1]. Questo capitolo esamina alcune esperienze positive e casi di studio significativi, evidenziando come soluzioni IA ben progettate possano contribuire a risolvere problematiche storiche delle elezioni, quali l'aggiornamento delle liste elettorali, la verifica dell'identità del votante, fino allo spoglio elettronico e all'assistenza agli elettori, garantendo al contempo alti standard di affidabilità. Ciascuna sezione mette in luce benefici concreti ottenuti attraverso l'adozione dell'IA in contesti reali, fornendo riferimenti a studi e dati aggiornati al 2025. Le esperienze positive descritte di seguito suggeriscono che, con adeguate misure di trasparenza e controllo umano, l'IA può rafforzare i sistemi di voto elettronico, migliorandone efficienza, accuratezza e inclusività, senza comprometterne la fiducia pubblica.

6.1 I.A. per la gestione delle liste elettorali e registrazione degli elettori

Uno dei campi in cui l'IA ha già dimostrato un impatto positivo è la manutenzione delle liste elettorali e la registrazione degli elettori. La qualità del registro degli elettori è fondamentale per elezioni credibili: la presenza di iscrizioni duplicate, deceduti non rimossi o errori anagrafici può tradursi in frodi o, più spesso, in disservizi e potenziale pregiudizio del diritto di voto. Tradizionalmente, il controllo incrociato di milioni di record elettorali era un compito oneroso e incline all'errore umano; oggi, algoritmi di machine learning possono individuare schemi e corrispondenze nei dati con velocità e precisione superiori. Ad esempio, negli Stati Uniti un consorzio interstatale denominato Electronic Registration Information Center (ERIC) utilizza un software basato su IA per confrontare banche dati elettorali di più stati, identificando possibili

1 International IDEA. (2024). *Artificial Intelligence for Electoral Management*. Stockholm: International Institute for Democracy and Electoral Assistance. Il report documenta casi d'uso dell'IA lungo il ciclo elettorale (liste elettorali, registrazione, pianificazione risorse, comunicazione con gli elettori, biometria) e sottolinea la necessità di supervisione umana, trasparenza e governance del rischio nell'adozione di strumenti automatizzati da parte degli Election Management Bodies (EMB).

doppi registrazioni o persone non più eleggibili (ad es. deceduti) attraverso il riconoscimento di pattern complessi nelle informazioni anagrafiche[2]. Ogni potenziale coincidenza individuata dall'algoritmo viene successivamente verificata manualmente dagli operatori, prima di inviare ai singoli stati le segnalazioni per la cancellazione o l'aggiornamento delle voci corrispondenti[3]. Questo approccio ibrido, in cui l'IA effettua una pre-selezione intelligente e l'uomo conferma, ha mostrato notevoli benefici: ERIC si è rivelato notevolmente più accurato rispetto ai precedenti sistemi di confronto puramente algoritmico (come il vecchio programma *Interstate Crosscheck*), riducendo drasticamente i falsi positivi. In passato, semplici metodi di abbinamento basati solo su nome e data di nascita generavano alti tassi di false segnalazioni di duplicati – ad esempio trattando come un unico elettore due persone distinte con nomi simili – con conseguenze potenzialmente gravi, tra cui la cancellazione indebita di elettori validi e il rischio di *disenfranchisement*[4] di cittadini aventi diritto. L'uso di sistemi IA avanzati ha mitigato questo problema: la capacità di ERIC di incrociare molteplici campi e fonti di dati permette di individuare legami meno ovvi tra registrazioni senza sacrificare la precisione, così da mantenere liste elettorali più pulite e aggiornate, a beneficio sia dell'integrità del voto sia della fiducia degli elettori nel sistema.

Sul piano internazionale, numerose democrazie emergenti hanno adottato tecnologie analoghe per migliorare l'accuratezza delle liste elettorali attraverso procedure di registrazione biometrica degli elettori, anch'esse alimentate da algoritmi di riconoscimento avanzati. Queste soluzioni utilizzano tratti biometrici univoci – tipicamente impronte digitali e immagini del volto – per verificare l'identità dei votanti al momento dell'iscrizione, e impiegano sistemi automatizzati di deduplicazione per garantire che ogni persona compaia una sola volta nel registro nazionale (*one voter, one vote*). I risultati ottenuti sono di grande rilievo. In Nigeria, ad esempio, la commissione elettorale (INEC) ha condotto un massiccio processo di bonifica del proprio elenco elettorale utilizzando una piattaforma di deduplicazione biometrica basata su IA: tra il 2011 e il 2019 sono state eliminate circa 16,5 milioni di registrazioni considerate duplicate, incomplete o fraudolente[5]. Si tratta di numeri estremamente significativi, che

2 Ibidem

3 Ibidem

4 Con il termine *disenfranchisement* si indica l'esclusione, temporanea o permanente, di cittadini aventi diritto dall'esercizio del voto, derivante da misure amministrative, procedure difettose o pratiche discriminatorie che incidono sull'iscrizione alle liste elettorali o sull'accesso al seggio. In ambito elettorale comparato, il concetto è utilizzato per descrivere sia fenomeni intenzionali sia effetti collaterali non voluti di sistemi di registrazione o verifica inadeguati, come la cancellazione indebita di elettori validi (*erroneous voter purges*). Cfr. R. M. Alvarez, S. D. Hyde, *Election Administration and Democratic Legitimacy*, Cambridge University Press, 2012; Brennan Center for Justice, *Voter Purges*, aggiornamenti 2018–2023.

5 Macdonald, A. (2021). "Nigeria biometric voter deduplication removes 16.5M". *Biometric Update*, 8 giugno 2021. L'articolo riporta i dati comunicati da INEC sulla bonifica del registro elettorale tramite deduplicazione biometrica (circa 16,5 milioni di record rimossi come duplicati/

testimoniano il livello di irregolarità potenzialmente presente nei registri cartacei tradizionali e la capacità delle nuove tecnologie di purificarli su vasta scala. L'INEC ha sottolineato come l'introduzione di sistemi biometrici mirasse non solo a modernizzare il processo elettorale, ma soprattutto ad assicurare elezioni libere, corrette e credibili, rafforzando la trasparenza e la fiducia nel voto. Analogamente, altri Paesi – fra cui Ghana, Repubblica Democratica del Congo, Zimbabwe e molti altri – hanno implementato soluzioni di registrazione elettorale con dati biometrici e procedure automatiche di verifica delle identità, spesso fornite da società specializzate, ottenendo un netto miglioramento dell'affidabilità delle liste e riducendo le possibilità di frode legate a elettori fittizi o doppie registrazioni[6]. Tali esperienze indicano che l'uso combinato di grandi banche dati elettorali digitali e intelligenza artificiale (in questo caso, algoritmi di matching biometrico e di *pattern recognition*) può risolvere all'origine molte anomalie amministrative che storicamente affliggevano le elezioni, garantendo che solo gli elettori aventi diritto risultino registrati e che ciascun individuo abbia una sola identità elettorale attiva.

6.2 IA e verifica dell'identità degli elettori (autenticazione biometrica)

Un secondo ambito di applicazione dell'IA, strettamente legato al precedente, è quello della verifica dell'identità al momento del voto. Nei sistemi di voto elettronico e in quelli tradizionali supportati da tecnologie digitali, autenticare con certezza l'elettore evitando al contempo di violarne la segretezza è un requisito fondamentale. Anche qui le soluzioni basate su IA e biometria stanno fornendo esperienze di successo. Molti paesi che hanno raccolto dati biometrici in fase di registrazione li impiegano poi anche ai seggi: ad esempio mediante dispositivi elettronici che confrontano l'impronta digitale o la fotografia del votante con quelle registrate nel database elettorale, garantendo che la persona che si presenta a votare sia effettivamente chi dichiara di essere e che nessuno possa votare due volte. Tali dispositivi sfruttano algoritmi di riconoscimento facciale o di impronte di ultima generazione (spesso basati su reti neurali e metodi di *deep learning*) per effettuare il matching in tempo reale con un'alta accuratezza, nonostante le possibili variazioni (angolazione del volto, pressione del dito sul lettore, etc.). L'adozione estensiva di queste tecnologie ha portato risultati positivi sul campo. Ad esempio, sempre in Nigeria l'INEC ha gradualmente introdotto dal 2015 l'uso di lettori biometrici di impronte (dispositivi *BVAS*) nelle sezioni elettorali, riducendo drasticamente i tentativi di voto multiplo o sotto falsa identità; nel 2023 l'ente ha annunciato l'estensione del sistema con funzionalità di

incompleti/fraudolenti) e descrive l'evoluzione dei sistemi di accredito biometrico, includendo l'estensione delle funzionalità verso il riconoscimento facciale nel ciclo elettorale successivo.

6 Ibidem

riconoscimento facciale, per ulteriore sicurezza. In India, la cui base elettorale supera i 900 milioni di cittadini, è stato avviato un progetto per collegare la banca dati dei numeri biometrici nazionali (*Aadhaar*) con le liste degli elettori, così da permettere controlli incrociati automatizzati e identificare immediatamente eventuali duplicazioni o usi impropri della tessera elettorale[7]. Benché questa iniziativa indiana abbia suscitato anche dibattiti riguardo alla privacy, essa riflette la fiducia riposta nella tecnologia per affrontare problemi decennali (in India il fenomeno dei cosiddetti *bogus voters* e delle impersonificazioni ai seggi è documentato da tempo).

Nel complesso, l'esperienza accumulata indica che l'autenticazione biometrica assistita da IA offre benefici tangibili: migliora sia la sicurezza del voto, impedendo di fatto frodi come il voto per delega non autorizzato, sia l'usabilità del processo, velocizzando le operazioni di identificazione al seggio. Ad esempio, in paesi come il Ghana l'introduzione del riconoscimento delle impronte digitali al seggio ha eliminato quasi del tutto le contestazioni per presunti voti multipli e ha aumentato la fiducia dei partiti nel fatto che ogni votante corrisponda esattamente a un'unica registrazione nel sistema. Anche in contesti locali più limitati sono state riportate esperienze positive: in Italia, alcune sperimentazioni su piccola scala hanno utilizzato il riconoscimento facciale per controllare l'accesso ai seggi in consultazioni studentesche e, pur necessitando di autorizzazioni e cautele, hanno dimostrato accuratezza e rapidità senza generare falsi positivi né compromettere l'anonimato del voto grazie alla separazione crittografica tra fase di identificazione e fase di espressione del voto. In tutti questi casi, il filo conduttore è l'impiego di sistemi di IA addestrati su grandi moli di dati biometrici per garantire l'unicità del voto: una persona – una scheda. Ciò realizza in pratica uno dei principi cardine di ogni democrazia, eliminando vulnerabilità che in passato potevano essere sfruttate per inquinare l'esito elettorale. Vale la pena sottolineare, tuttavia, che il successo di tali iniziative dipende anche dalla qualità dei dati raccolti (ad esempio impronte leggibili, foto nitide) e dall'infrastruttura: l'IA, per quanto potente, va inserita in un processo ben progettato, altrimenti problemi tecnici o mismatch potrebbero causare ritardi ai seggi o contestazioni. Le esperienze ad oggi documentate sono comunque incoraggianti e indicano che, laddove implementata correttamente, la verifica biometrica intelligente può diventare parte integrante di un sistema di voto elettronico robusto, migliorando la sicurezza senza sacrificare i diritti degli elettori.

---

7 Dave, P., & Sullivan, A. (2020). "Bleary-eyed U.S. election officials turn to signature-verifying software in mail-in surge". *Reuters*, 24 settembre 2020; Reuters. (2020). "FACTBOX – U.S. counties using automated signature verification software". *Reuters*, 24 settembre 2020. Le fonti Reuters documentano l'adozione, in almeno 29 contee statunitensi, di software di verifica automatizzata delle firme per gestire l'aumento del voto postale nel 2020, descrivendo l'approccio "human-in-the-loop" (scoring automatico + revisione manuale per i casi borderline) e i principali fornitori citati dagli uffici elettorali.

6.3 IA a supporto dello spoglio elettronico e del conteggio dei voti

Un altro ambito in cui l'IA sta mostrando il suo potenziale è quello del conteggio dei voti e della tabulazione dei risultati, fasi critiche in cui rapidità e precisione sono essenziali. I sistemi di voto elettronico puntano storicamente a ridurre i tempi di spoglio rispetto alle schede cartacee tradizionali; tuttavia, persino quando il voto avviene su carta, l'IA può intervenire per accelerare e rendere più affidabile la fase di conteggio e consolidamento dei risultati. Un caso di studio emblematico proviene dal Cile, dove nel 2020 è stato sperimentato un sistema di scrutinio assistito da IA con esiti molto positivi[8]. In occasione di un importante appuntamento elettorale nazionale, le autorità cilene – in collaborazione con fornitori tecnologici – hanno implementato un software basato su riconoscimento intelligente dei caratteri (ICR) e reti neurali profonde per leggere automaticamente i verbali cartacei di sezione e le schede votate. Il procedimento è il seguente: dopo la chiusura dei seggi, i verbali di scrutinio (riportanti i voti conteggiati per ciascun candidato) vengono digitalizzati tramite scanner ad alta velocità, producendo immagini ad alta risoluzione. A questo punto entra in gioco l'IA: un algoritmo di visione artificiale analizza ciascuna immagine, riconosce innanzitutto il tipo di documento e la specifica sezione elettorale (grazie a codici QR o altri marcatori sul modulo) e poi individua le zone di interesse (caselle numeriche, nomi di candidati, timbri, firme). Successivamente, sfruttando modelli di Deep Learning addestrati su grandi insiemi di esempi, il sistema esegue il riconoscimento ottico del testo scritto a mano o a macchina in ogni campo del verbale. I risultati sono notevoli: nel caso cileno, il software ha raggiunto un'accuratezza di riconoscimento vicino al 92% senza intervento umano, una percentuale superiore al tasso di successo di un operatore esperto nell'inserimento manuale dei dati. In altre parole, l'IA è stata in grado di "leggere" un intero verbale di voto in pochi centesimi di secondo con un tasso di errore molto basso, laddove un essere umano avrebbe impiegato vari minuti per trascrivere lo stesso verbale, con un maggiore rischio di refusi.

Per garantire la totale esattezza dei risultati, questo sistema automatico è stato affiancato da controlli incrociati: ad esempio, una percentuale di verbali è stata ricontrollata manualmente da operatori, e le discrepanze eventualmente rilevate hanno alimentato un'ulteriore fase di addestramento e calibrazione del modello. Grazie a questa doppia verifica, il tasso di errore complessivo nella registrazione dei risultati è stato portato ad un valore prossimo allo 0%, combinando la velocità della macchina con il giudizio umano nei pochi casi dubbi. L'impatto

8 Minsait. (2021). *AI applied to elections (Ideas for Democracy)*. Minsait/Indra. La documentazione descrive applicazioni di IA per la gestione e la narrazione automatizzata di dati elettorali e per l'estrazione strutturata di informazioni da fonti e documenti ufficiali, incluse tecniche di riconoscimento e interpretazione automatica di contenuti elettorali digitalizzati.

operativo è stato straordinario. Mentre in consultazioni precedenti occorrevano anche settimane o mesi per raccogliere e digitare a mano tutti i risultati provenienti dalle migliaia di seggi sparsi nel paese, con il nuovo sistema basato su IA il tempo di consolidamento di tutti i dati elettorali è sceso a un paio di giorni. Ciò significa che le autorità elettorali cilene hanno potuto proclamare risultati ufficiali con un anticipo senza precedenti, fornendo al contempo ai cittadini un livello di trasparenza maggiore: tutte le immagini dei verbali digitalizzati, insieme ai dati estratti dall'IA, sono state rese disponibili per la consultazione, consentendo verifiche indipendenti. Da sottolineare che questa innovazione è stata introdotta senza modificare le modalità di voto per gli elettori – che hanno continuato a utilizzare la scheda cartacea tradizionale – e senza richiedere cambiamenti normativi sostanziali, poiché si tratta di un miglioramento del processo di conteggio *a valle* della votazione, pienamente compatibile con le leggi esistenti. L'esperienza cilena rappresenta dunque un modello di convivenza tra voto cartaceo e tecnologia avanzata: l'IA funge da "ponte" che traghetta rapidamente l'informazione analogica (il voto su carta) nel mondo digitale per l'elaborazione, riducendo errori di trascrizione e accelerando lo spoglio, il tutto sotto supervisione umana continua. Sulla scia di questo successo, altri paesi stanno valutando approcci analoghi. Ad esempio, in Spagna e America Latina sono in corso progetti pilota che applicano algoritmi di visione artificiale al riconoscimento delle schede votate e dei verbali, con l'obiettivo sia di accelerare la diffusione dei risultati sia di offrire al pubblico un meccanismo di verifica indipendente (pubblicando online le immagini di ogni scheda o verbale elaborato dall'IA). Si tratta di sviluppi promettenti, che dimostrano come l'IA possa aumentare la efficienza e la credibilità del conteggio elettronico dei voti. Naturalmente, rimane fondamentale implementare robuste misure di sicurezza informatica attorno a questi sistemi – dalle verifiche sulle firme digitali delle immagini all'isolamento delle reti di trasmissione – per scongiurare tentativi di manomissione. Ma le best practice emerse (come la presenza di una componente manuale di controllo e la totale tracciabilità delle operazioni effettuate dall'algoritmo) forniscono una solida base per integrare l'IA negli scrutini elettorali futuri su vasta scala.

6.4 Verifica automatizzata delle schede e individuazione di anomalie

Oltre a velocizzare il conteggio, l'intelligenza artificiale può contribuire a migliorare la validazione e il controllo di qualità del processo di voto, rilevando errori o irregolarità che potrebbero sfuggire al controllo umano. In questa sezione consideriamo due tipi di applicazioni positive: la verifica automatica delle schede votate, in particolare per il voto postale, e l'individuazione di anomalie elettorali tramite analisi avanzata dei dati di affluenza e risultati[9].

9 Alvarez, R. M., Hall, T. E., & Hyde, S. D. (2008). *Election Fraud: Detecting and Deterring Electoral Manipulation*. Brookings Institution Press; Mebane, W. R. (2013). *Election Forensics: Quantitative*

Un esempio rilevante del primo tipo è l'uso crescente di software di verifica delle firme apposte sulle buste del voto per corrispondenza (*mail-in ballots*). Negli Stati Uniti, soprattutto durante le elezioni del 2020 segnate dalla pandemia di COVID-19, si è registrato un ricorso massiccio al voto per posta e anticipato. Diversi uffici elettorali locali hanno adottato sistemi di IA per gestire l'enorme volume di schede postali, in particolare automatizzando il confronto tra la firma del votante sulla busta e la firma archiviata nel registro firme. Secondo un'indagine Reuters, almeno 29 contee negli USA hanno utilizzato nel 2020 software di verifica automatica delle firme basati su algoritmi di riconoscimento grafologico[10]. Uno dei fornitori principali, Parascript, ha sviluppato soluzioni in grado di elaborare migliaia di firme in poche ore, attribuendo a ciascun confronto uno *score* di similarità. Ogni contea può configurare una soglia di confidenza: se il punteggio supera la soglia, la firma si considera corrispondente e la scheda viene accettata; in caso contrario, la busta viene segnalata per revisione manuale da parte di funzionari addestrati. Questo sistema ha alleggerito in modo significativo il carico di lavoro degli scrutatori, evitando che dovessero ispezionare a vista ogni singola firma – attività che, oltretutto, è soggetta a stanchezza e bias soggettivi. Le autorità locali e gli esperti di diritto di voto hanno accolto con favore questa innovazione, notando che il software può ridurre l'incoerenza e i pregiudizi insiti nelle valutazioni umane, rendendo il trattamento delle schede più uniforme. In passato, infatti, diversi studi hanno evidenziato come la convalida delle firme fosse vulnerabile a errori: firme genuine scartate per eccesso di zelo (*false negative*) o, viceversa, firme non corrispondenti accettate per disattenzione. L'IA, opportunamente calibrata, tende ad avere criteri più costanti e documentabili, migliorando l'equità del processo. Va sottolineato che questi software non sostituiscono del tutto l'uomo, bensì funzionano come un filtro: nelle contee citate, generalmente oltre il 70-80% delle buste viene validato automaticamente, mentre il resto (casi dubbi) è sottoposto a verifica da parte di un operatore umano. In questo modo, il personale può concentrare la propria

Techniques for Detecting Fraud. In: Alvarez, R. M. (ed.), *The State of Election Forensics*. Cambridge University Press; National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote: Protecting American Democracy*. National Academies Press. La letteratura convergente evidenzia come strumenti automatizzati di analisi dei dati e di verifica assistita possano migliorare il controllo di qualità dei processi elettorali, fungendo da meccanismi di supporto all'individuazione di errori procedurali, incongruenze statistiche o anomalie nei flussi di voto e nei risultati, senza sostituire il giudizio umano né i controlli istituzionali previsti.

10 Dave, P., & Sullivan, A. (2020). "Bleary-eyed U.S. election officials turn to signature-verifying software in mail-in surge". *Reuters*, 24 settembre 2020; Reuters. (2020). "FACTBOX – U.S. counties using automated signature verification software". *Reuters*, 24 settembre 2020; National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote: Protecting American Democracy*. National Academies Press. Le fonti documentano l'adozione, durante le elezioni statunitensi del 2020, di sistemi automatizzati di verifica delle firme per la gestione del voto per corrispondenza su larga scala, evidenziando un modello operativo *human-in-the-loop* in cui l'analisi algoritmica funge da filtro preliminare e le decisioni finali restano affidate a funzionari elettorali, al fine di bilanciare efficienza, uniformità di trattamento e tutela del diritto di voto.

attenzione solo su una frazione delle schede (ad esempio firme molto divergenti, firme di elettori anziani o alla prima votazione che spesso creano difficoltà al matching algoritmico), risolvendo eventuali problemi in maniera rapida ed efficace, contattando ad esempio il votante per sanare una firma contestata. Complessivamente, l'adozione di IA per la validazione delle schede postali nel 2020 ha permesso di gestire con successo un afflusso senza precedenti di voti per corrispondenza, contribuendo a dichiarare i risultati finali in tempi ragionevoli e riducendo al minimo gli errori di conteggio dovuti a firme non verificate. Questa esperienza sta facendo scuola: molte giurisdizioni statali stanno investendo in tali strumenti in vista delle prossime tornate elettorali, integrandoli nei loro regolamenti con opportune garanzie procedurali (ad esempio, previsione di un controllo bipartito sulle schede scartate dall'IA, per assicurare che nessun elettore venga escluso ingiustamente). L'approccio, quindi, è considerato ampiamente positivo, pur richiedendo una continua attività di audit sugli algoritmi per monitorare tassi di falso positivo/negativo e correggere eventuali distorsioni.

Il secondo tipo di applicazione riguarda l'analisi avanzata dei dati elettorali per individuare incongruenze o anomalie potenzialmente indicatrici di problemi. Anche qui registriamo esperienze promettenti. Un progetto pionieristico è stato condotto dal Voting Technology Project (VTP) del Caltech/MIT negli Stati Uniti, in collaborazione con autorità locali della California, mirato a scoprire anomalie nei trend di voto attraverso il *machine learning*[11]. In particolare, nelle contee di Los Angeles e Orange sono stati implementati algoritmi che, su base giornaliera e post-elettorale, monitorano vari indicatori: ad esempio i tassi di affluenza per sezione, il numero di schede provvisorie emesse o la percentuale di voti nulli, confrontandoli con i pattern storici attesi in quelle stesse aree[12]. Nel caso delle elezioni generali del 2018 in Orange County, il sistema segnalò alcune sezioni dove l'affluenza o altri parametri differivano significativamente

11 Alvarez, R. M., Hall, T. E., & Hyde, S. D. (2008). *Election Fraud: Detecting and Deterring Electoral Manipulation*. Brookings Institution Press; Kim, S. S., Alvarez, R. M., & Hall, T. E. (2019). *Evaluating the Quality of Changes in Voter Registration Databases*. Caltech/MIT Voting Technology Project (VTP), technical report; Mebane, W. R. (2013). *Election Forensics: Quantitative Techniques for Detecting Fraud*. In: Alvarez, R. M. (ed.), *The State of Election Forensics*. Cambridge University Press. Nell'ambito delle attività del Caltech/MIT Voting Technology Project, modelli di analisi statistica avanzata e tecniche di *machine learning* sono stati applicati ai dati di affluenza e di scrutinio per individuare deviazioni significative rispetto ai pattern storici attesi, consentendo alle autorità elettorali locali di attivare verifiche mirate su errori procedurali o anomalie amministrative, in un'ottica di supporto decisionale e controllo di qualità del processo elettorale.

12 Freed, B. (2020). "Election questions? Idaho's new Watson-powered chatbot has answers". *StateScoop*, 17 settembre 2020; Kim, S. S., Alvarez, R. M., & Hall, T. E. (2019). *Evaluating the Quality of Changes in Voter Registration Databases* (Caltech/MIT Voting Technology Project; report reso disponibile dall'Orange County Registrar of Voters). Il primo riferimento documenta l'uso di un assistente virtuale (IBM Watson) da parte dell'ufficio elettorale dell'Idaho per rispondere a domande dei cittadini e ridurre il carico operativo; il secondo fornisce un esempio metodologico di analisi e anomaly detection applicata a dati amministrativi elettorali (voter registration database), utile a giustificare l'impiego di modelli di rilevazione anomalie e controlli mirati post-elezione.

dalle medie storiche e dalle proiezioni. Queste segnalazioni hanno innescato verifiche mirate da parte dei funzionari: è emerso che in tutti i casi si trattava di errori procedurali o di reporting, come ad esempio sezioni che avevano inizialmente riportato in modo errato il conteggio delle schede, poi corretto nei giorni successivi. Non vennero riscontrati tentativi di frode sistematica, ma il fatto stesso di aver identificato rapidamente le discrepanze ha permesso all'ufficio elettorale di intervenire tempestivamente (correggendo i dati errati e ricostituendo le procedure laddove necessario) prima che queste anomalie minassero la fiducia nel risultato. Si tratta dunque di un esempio concreto di come l'IA possa fungere da "sentinella" statistica a tutela della regolarità del voto: individuando scenari fuori dal comune, l'algoritmo indirizza l'attenzione umana dove serve, in modo oggettivo e basato sui dati. In prospettiva, sistemi simili potrebbero rilevare anche sintomi di possibili frodi – ad esempio, un afflusso insolitamente alto in seggi considerati a rischio clientelismo, oppure andamenti di voto fortemente discrepanti rispetto a circoscrizioni demograficamente simili – e segnalarli per ispezioni approfondite, contribuendo così a prevenire e scoraggiare manipolazioni. Progetti accademici recenti hanno anche esplorato l'uso di modelli di novità *(novelty detection)* per identificare pattern anomali nei risultati elettorali a livello di seggio[13]: in alcuni casi testati su elezioni passate, questi modelli hanno correttamente distinto distretti "normali" da quelli in cui si sapeva esservi state irregolarità, dimostrando la fattibilità tecnica dell'approccio. Sebbene queste soluzioni siano per ora in fase sperimentale e non vi siano ancora applicazioni su scala nazionale, rappresentano un ulteriore ambito in cui l'IA può generare valore aggiunto: garantire una sorta di *audit digitale continuo* del processo elettorale. L'esperienza californiana, in particolare, ha mostrato che anche errori in buona fede possono essere identificati e corretti rapidamente grazie all'analisi automatizzata dei dati – un compito che sarebbe proibitivo manualmente in contesti con migliaia di sezioni e milioni di voti. Naturalmente, l'efficacia di questi strumenti dipende dall'accesso tempestivo a dati elettorali di qualità e dal confronto con baseline affidabili; inoltre, come per ogni sistema di IA, è cruciale evitare falsi allarmi calibrando opportunamente i modelli. Tuttavia, man mano che gli enti elettorali raccolgono dati storici più granulari (grazie anche alla digitalizzazione del voto e dello scrutinio), ci si può aspettare che l'IA giochi un ruolo crescente nell'assicurare che eventuali discrepanze nei risultati vengano spiegate e risolte, rafforzando l'integrità complessiva delle elezioni.

13 Mebane, W. R., & Kalinin, K. (2020). "Comparative Election Fraud Detection". *American Political Science Review*, 114(4), 1219–1237; Beber, B., & Scacco, A. (2012). "What the Numbers Say: A Digit-Based Test for Election Fraud". *Political Analysis*, 20(2), 211–234; Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer. Studi recenti in ambito di *election forensics* hanno applicato tecniche di *novelty detection*, *outlier detection* e apprendimento non supervisionato per individuare pattern di voto statisticamente anomali a livello di seggio, distinguendo deviazioni compatibili con variazioni fisiologiche da configurazioni che giustificano verifiche approfondite da parte delle autorità elettorali.

6.5 Assistenti virtuali e AI per il coinvolgimento degli elettori

Oltre che *dietro le quinte*, l'intelligenza artificiale ha iniziato a manifestare i suoi benefici anche nell'interfaccia diretta con gli elettori, migliorando l'accessibilità e la disponibilità di informazioni sul processo di voto[14]. Un esempio lampante è l'adozione di chatbot e assistenti virtuali basati su IA da parte di enti elettorali per rispondere alle domande più comuni del pubblico. Fornire indicazioni corrette agli elettori, quali le modalità per registrarsi, dove votare, quali documenti presentare, oltre a far conoscere come funzionano nuove modalità di voto elettronico, etc., è un compito fondamentale, specialmente durante le consultazioni complesse o in momenti di cambiamenti normativi. Tuttavia, gli uffici elettorali spesso dispongono di risorse umane limitate per gestire migliaia di richieste individuali, che tendono a intensificarsi a ridosso delle elezioni. È qui che gli assistenti conversazionali alimentati da IA si sono rivelati utili.

Durante il ciclo elettorale 2020 negli Stati Uniti, Idaho è stato uno degli stati pionieri nell'implementare un chatbot basato sulla piattaforma IBM Watson per assistere gli elettori. Inserito sul sito del Segretario di Stato, il chatbot è stato addestrato su un ampio set di quesiti e risposte relative a voto per corrispondenza, registrazione online, ubicazione dei seggi, orari di apertura, requisiti di identificazione e misure sanitarie legate alla pandemia. Secondo i dati diffusi dall'ufficio elettorale dell'Idaho, nelle prime settimane di attività (prima delle primarie del maggio 2020) l'assistente virtuale ha gestito autonomamente circa 3.300 richieste di informazioni da parte di cittadini, fornendo risposte immediate e accurate alle loro domande. Ciò ha avuto un duplice effetto positivo: da un lato, gli elettori hanno potuto ottenere chiarimenti 24 ore su 24, anche fuori dall'orario d'ufficio, migliorando la user experience e probabilmente riducendo incertezze che avrebbero potuto dissuaderli dal partecipare; dall'altro, lo staff umano dell'ufficio ha visto alleggerirsi il carico di telefonate ed e-mail, potendo concentrare gli sforzi sulle questioni più complesse o sui casi particolari che

14 International IDEA. (2024). *Artificial Intelligence for Electoral Management*. Stockholm: International Institute for Democracy and Electoral Assistance; OSCE/ODIHR. (2024). *Handbook for the Observation of ICT in Elections*. Warsaw; European Commission – Joint Research Centre (JRC). (2023). *Cybersecurity of Electronic Voting Systems*; National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote: Protecting American Democracy*. National Academies Press. La letteratura istituzionale e accademica più recente riconosce che l'impiego di sistemi di intelligenza artificiale nell'interazione diretta con gli elettori, quali chatbot informativi, assistenti virtuali multilingue e interfacce adattive, può migliorare in modo significativo l'accessibilità, la tempestività e la qualità dell'informazione elettorale, riducendo asimmetrie informative e barriere operative. Tali strumenti, se progettati secondo principi di *human-in-the-loop*, trasparenza e verificabilità, rafforzano la fiducia nel processo elettorale senza sostituire il ruolo decisionale umano, configurandosi come componenti di supporto alla partecipazione democratica e non come meccanismi di influenza del voto.

richiedevano effettivamente l'intervento diretto di un funzionario. I responsabili hanno definito questo supporto come "un enorme peso tolto dalle spalle del nostro personale", evidenziando come l'IA abbia agito da moltiplicatore di forza lavoro in un momento critico.

Sulla scorta di questi risultati, anche altre amministrazioni hanno intrapreso strade simili. Chatbot non-generativi (basati su risposte predefinite e riconoscimento del linguaggio naturale) sono stati adottati, ad esempio, dal Dipartimento Veicoli a Motore dello Stato di New York – che gestisce anche servizi legati alla registrazione elettorale – e dalla Segreteria di Stato della California, con l'obiettivo di aiutare gli elettori a navigare siti web elettorali complessi e fornire informazioni rapide su domande frequenti. In molti casi, questi assistenti virtuali utilizzano interfacce conversazionali tipo chat sul web o sistemi vocali telefonici interattivi, e rappresentano per gli utenti un modo semplice per ottenere ciò di cui hanno bisogno senza attendere in linea un operatore. Si noti che la maggior parte di queste implementazioni finora ha evitato l'uso di modelli generativi di ultima generazione (come GPT), preferendo approcci più controllati: le risposte fornite dai chatbot sono basate su un knowledge base verificato e approvato dagli uffici elettorali, il che elimina il rischio di *allucinazioni* (ossia informazioni inventate dall'IA) e mantiene il messaggio coerente con le normative vigenti. Questa prudenza è giustificata – dati i potenziali danni di un'informazione errata in ambito elettorale – ma non toglie che in futuro, con modelli generativi più affidabili, si potrà ulteriormente ampliare la gamma di quesiti gestibili automaticamente (per ora i chatbot tendono a coprire domande standardizzate)[15]. Un'altra applicazione emergente dell'IA per coinvolgere gli elettori riguarda la traduzione automatica dei materiali informativi e delle schede: alcuni uffici stanno sperimentando strumenti di traduzione basati su rete neurali per produrre rapidamente versioni multilingue di guide al voto e istruzioni, utili per servire comunità linguistiche minoritarie in tempi rapidi[16]. Naturalmente,

15 OSCE/ODIHR. (2024). *Handbook for the Observation of ICT in Elections*. Warsaw; European Commission. (2023). *Guidelines on the Responsible Use of Artificial Intelligence in the Public Sector*; National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote: Protecting American Democracy*. National Academies Press. Le fonti evidenziano come l'uso di sistemi automatizzati nell'informazione elettorale richieda particolare cautela, poiché errori, imprecisioni o risposte non contestualizzate possono incidere sulla fiducia degli elettori e sull'integrità del processo democratico. Al contempo, la letteratura riconosce che l'evoluzione verso modelli generativi più affidabili, controllabili e auditabili potrebbe consentire in futuro un ampliamento responsabile delle funzionalità informative automatizzate, purché accompagnato da supervisione umana, validazione preventiva dei contenuti e meccanismi di accountability.

16 Vaswani, A. et al. (2017). *Attention Is All You Need*. NeurIPS; Devlin, J. et al. (2019). *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. NAACL-HLT; International IDEA. (2024). *Artificial Intelligence for Electoral Management*. Stockholm. La traduzione automatica neurale basata su architetture Transformer ha raggiunto livelli di accuratezza e fluidità tali da consentirne l'impiego sperimentale in contesti istituzionali multilingue, inclusa

anche in questo caso è richiesta un'attenta revisione umana, dato che una sfumatura mal tradotta potrebbe confondere gli elettori[17]; tuttavia, l'ausilio dell'IA può ridurre tempi e costi di traduzione, permettendo di coprire più lingue di quante sarebbero possibili con le sole risorse umane disponibili. In prospettiva, l'IA potrebbe persino essere impiegata per creare contenuti personalizzati (ad esempio, messaggi di promemoria al voto inviati agli elettori con informazioni specifiche sul loro seggio, generati automaticamente in base ai dati individuali), o per ottimizzare la ricerca di sedi di seggio tenendo conto di dati geografici e di traffico, così da suggerire location più comode per gli elettori. Sebbene molte di queste idee siano ancora in fase esplorativa, le esperienze già realizzate con i chatbot indicano chiaramente un feedback positivo sia da parte degli utenti che delle amministrazioni: l'IA, se ben utilizzata, può abbattere barriere informative e rendere il processo elettorale più user-friendly, fattore che potrebbe contribuire indirettamente ad una maggiore partecipazione e soddisfazione dei cittadini verso il voto elettronico e non.

6.6 Verso un'integrazione responsabile dell'IA nel voto elettronico

I casi di studio analizzati in questo capitolo testimoniano che l'introduzione dell'intelligenza artificiale nei processi di voto elettronico non è più soltanto una teoria futuristica, ma una realtà in rapida evoluzione, con benefici concreti documentati in diversi contesti. Dal miglioramento dell'integrità delle liste elettorali tramite deduplicazione automatica, alla velocizzazione dello scrutinio con riconoscimento intelligente dei voti, fino all'assistenza agli elettori attraverso agenti conversazionali, l'IA si è rivelata uno strumento versatile capace di affrontare sfide storiche e nuove esigenze del sistema elettorale. In tutti gli esempi virtuosi evidenziati, ovvero da *ERIC* per le liste elettorali negli USA all'uso di

la diffusione di materiali informativi elettorali. Studi e report istituzionali indicano che tali strumenti possono migliorare significativamente l'accesso all'informazione per comunità linguistiche minoritarie, riducendo barriere comunicative e favorendo l'inclusione, a condizione che i testi tradotti siano sottoposti a revisione umana e controlli di qualità per evitare ambiguità o fraintendimenti con potenziale impatto sul diritto di voto.

17 OSCE/ODIHR. (2024). *Handbook for the Observation of ICT in Elections*. Warsaw; European Commission – Joint Research Centre (JRC). (2023). *AI and Language Technologies in Public Services: Risks and Safeguards*; International Organization for Standardization (ISO). (2023). *ISO/IEC 23894: Information Technology — Artificial Intelligence — Risk Management*. Le fonti sottolineano che, in ambiti sensibili come l'informazione elettorale, l'uso di sistemi di traduzione automatica deve essere sempre affiancato da revisione e validazione umana, poiché anche lievi imprecisioni semantiche o pragmatiche possono generare ambiguità interpretative con potenziali effetti sul corretto esercizio del diritto di voto. Il principio di *human oversight* è pertanto considerato essenziale per garantire accuratezza, neutralità e affidabilità dei contenuti multilingue diffusi agli elettori.

biometria intelligente in Nigeria e altrove, dal conteggio digitale in Cile ai controlli di firma e le analisi anomale negli Stati Uniti, fino ai chatbot informativi in vari paesi, il comune denominatore è che l'IA amplifica e ottimizza le capacità umane, senza però sostituirle del tutto. Anzi, un insegnamento chiave emerso da queste esperienze è la necessità di mantenere l'uomo "in the loop": ogni implementazione di successo prevede meccanismi di supervisione, validazione o intervento umano che correggono gli errori residui della macchina e ne guidano l'addestramento continuo. Questa collaborazione sinergica tra algoritmi e operatori è probabilmente il modello da seguire per sfruttare al massimo i vantaggi dell'IA riducendo al minimo i rischi.

Un altro aspetto fondamentale, sottolineato anche dalle linee guida internazionali e dalle revisioni paritarie, è l'importanza di trasparenza e controllo[18]. L'adozione di IA in un settore delicato come le elezioni richiede di spiegare chiaramente al pubblico e agli stakeholders cosa fa l'algoritmo, quali dati utilizza, con quali limiti, e come vengono mitigati eventuali bias o errori. Alcuni paesi hanno già compiuto passi in questa direzione: ad esempio, la Commissione Elettorale del Brasile (TSE) ha avviato nel 2024 un programma di audit e certificazione degli strumenti di IA utilizzati in ambito elettorale, anticipando regolamentazioni che presto potrebbero diventare la norma. Analogamente, negli Stati Uniti l'AI Executive Order del 2023 ha riconosciuto le infrastrutture elettorali come ambiti critici dove l'uso di IA dev'essere sicuro e sottoposto a standard rigorosi. Questi sviluppi normativi riflettono la consapevolezza che, accanto alle opportunità, l'IA porta con sé sfide etiche e di sicurezza (come bias algoritmici, vulnerabilità a data poisoning, o l'uso malevolo di IA generativa per diffondere disinformazione elettorale). Tuttavia, affrontare tali sfide in modo proattivo – ad esempio attraverso commissioni di esperti, protocolli di verifica indipendente dei sistemi e programmi di formazione per gli operatori elettorali – permette di incanalare l'IA verso usi benefici minimizzando gli effetti indesiderati.

In definitiva, le esperienze positive raccolte fino ad oggi suggeriscono che l'IA, se implementata responsabilmente, può diventare un alleato potente della democrazia. Può contribuire a elezioni più integre, dove brogli e irregolarità tecniche siano ridotti al minimo; più veloci, con risultati disponibili in tempi rapidi senza sacrificare l'accuratezza; e più inclusive, aiutando sia gli amministratori a

18 OSCE/ODIHR. (2024). *Handbook for the Observation of ICT in Elections*. Warsaw; Council of Europe. (2017). *Recommendation CM/Rec(2017)5 on standards for e-voting*; European Commission. (2024). *Ethics Guidelines for Trustworthy AI* (aggiornamenti applicativi nel contesto pubblico); Floridi, L. et al. (2018). "AI4People - An Ethical Framework for a Good AI Society". *Minds and Machines*, 28(4), 689–707. Le linee guida internazionali e la letteratura peer-reviewed convergono nell'affermare che trasparenza, auditabilità e controllo umano costituiscono requisiti essenziali per l'adozione legittima di sistemi di intelligenza artificiale in contesti democratici sensibili, come le elezioni, al fine di garantire accountability, prevenire abusi e mantenere la fiducia del pubblico nei processi decisionali automatizzati.

gestire meglio l'enorme complessità organizzativa, sia i cittadini a esercitare il proprio diritto di voto con meno ostacoli informativi o logistici. Man mano che la tecnologia progredisce e nuove elezioni globali (come quelle cruciali avutesi a cavallo fra il 2024-2025) offriranno banchi di prova ulteriori, sarà importante documentare e condividere le lezioni apprese. L'orizzonte che si prospetta è quello di un'integrazione strutturale dell'IA nei sistemi di e-voting: non più iniziative isolate o sperimentali, ma parte integrante degli standard elettorali internazionali. Per raggiungere questo traguardo in modo sostenibile, occorre continuare a investire nella ricerca interdisciplinare (coinvolgendo informatici, esperti legali, politologi), nonché nel dialogo con il pubblico per mantenere alta la fiducia. I casi di studio positivi esaminati in questo capitolo rappresentano delle pietre miliari in questo percorso: essi dimostrano che innovare si può, e che l'IA, lungi dall'essere una minaccia distopica, può rafforzare i principi democratici se guidata dai valori di trasparenza, equità e rispetto dei diritti. Adeguatamente monitorata e raffinata, l'intelligenza artificiale potrà dunque porsi sempre più come garante silenzioso del voto elettronico, aiutando le democrazie del XXI secolo a coniugare tecnologia e fiducia popolare in modo virtuoso.

PARTE IV
RISCHI E PROFILI DI USO MALEVOLO DELL'I.A. NEL CONTESTO DEL VOTO ELETTRONICO

Capitolo 7
Minacce e vulnerabilità dei sistemi di voto elettronico e online

7.1 Introduzione

L'adozione di tecnologie elettroniche e online nel voto promette maggiore rapidità e accessibilità nelle consultazioni elettorali, ma introduce al contempo nuovi rischi significativi. In particolare, i sistemi di e-voting (voto elettronico in presenza tramite macchine) e i-voting (voto remoto via Internet) possono essere esposti ad attacchi informatici mirati, a malfunzionamenti tecnici e a forme inedite di manipolazione dell'informazione. Tali minacce rischiano di compromettere i princìpi fondamentali delle elezioni democratiche, quali sono i requisiti di segretezza, integrità e disponibilità del voto, se le vulnerabilità dei sistemi non vengono adeguatamente mitigate.

Le crisi globali (pandemie, conflitti geopolitici, emergenze sociali) aggiungono ulteriore pressione sui processi elettorali, talvolta spingendo verso l'adozione accelerata di soluzioni di voto elettronico o a distanza. Si pensi alla pandemia di COVID-19, che ha riacceso il dibattito sul voto online per consentire la partecipazione elettorale nonostante il distanziamento sociale. In simili contesti, le infrastrutture digitali del voto diventano infrastrutture critiche di importanza strategica, potenzialmente nel mirino di attori ostili intenzionati a sfruttare la situazione di crisi. È dunque essenziale analizzare con occhio critico le vulnerabilità intrinseche di questi sistemi e le possibili minacce – accentuate anche dall'uso crescente dell'Intelligenza Artificiale (IA) – al fine di garantire elezioni affidabili e sicure.

In questo capitolo si esaminano **(i)** le principali vulnerabilità tecniche dei sistemi di voto elettronico e online, **(ii)** le tipologie di attacchi informatici che possono minacciarli – compresi scenari potenziati dall'I.A. – e **(iii)** i rischi collegati alla disinformazione e manipolazione dell'opinione pubblica tramite strumenti digitali avanzati. Verranno discussi inoltre **(iv)** gli aspetti controversi dell'utilizzo della tecnologia *blockchain* nel voto elettronico, delineandone potenzialità e limiti in modo equilibrato, e **(v)** il quadro normativo e standard di sicurezza vigente, con riferimenti sia a standard internazionali sia a recenti sviluppi legislativi (ad esempio l'AI Act dell'UE e iniziative regolatorie negli USA). L'analisi mantiene un taglio interdisciplinare, basato su evidenze scientifiche e su casi di studio aggiornati al 2025.

7.2 Vulnerabilità tecniche dei sistemi di voto elettronico

I sistemi di voto elettronico presentano vulnerabilità *interne* dovute alla loro stessa configurazione tecnologica e organizzativa. Una prima area critica riguarda l'hardware: molte macchine per il voto (ad esempio le DRE - *Direct Recording Electronic* - utilizzate in passato in vari stati USA) utilizzano componenti elettronici soggetti a guasti, manomissioni fisiche o obsolescenza. In assenza di adeguati controlli, un dispositivo di voto può essere alterato inserendo chip o moduli compromessi durante la produzione (problema di *supply chain security*), oppure subire accessi non autorizzati se lasciato incustodito. Ad esempio, è noto che in alcuni casi i ricercatori sono riusciti a aprire le macchine di voto elettronico e inserire *hardware* maligno in pochi minuti durante i test di sicurezza, evidenziando la necessità di rigide misure di sigillatura fisica e catena di custodia[1]. Anche l'utilizzo di sistemi obsoleti – come macchine con sistemi operativi non aggiornati o privi di *patch* di sicurezza – espone a vulnerabilità note sfruttabili da attaccanti.

Il software applicativo e il firmware delle macchine di voto costituiscono un'altra superficie d'attacco. Bug programmativi o configurazioni errate possono portare a errori di conteggio o essere sfruttati per alterare i risultati. Un caso emblematico è l'incidente occorso nella Contea di Antrim (Michigan, USA) nelle elezioni del novembre 2020: a causa di un errore di configurazione del software del tabulatore ottico, i risultati iniziali pubblicati attribuivano migliaia di voti al candidato sbagliato, salvo poi essere corretti tramite riconteggio manuale[2]. Un'analisi forense indipendente ha confermato che non vi fu broglio intenzionale, bensì "una catena di errori umani e insufficienti controlli software" che produssero il conteggio errato, evidenziando la necessità di rigorosi test di logica e accuratezza prima delle elezioni[3]. Questo esempio dimostra come insufficienti garanzie software possano tradursi in gravi vulnerabilità: senza efficaci meccanismi di controllo, un semplice errore di configurazione o un bug non rilevato possono compromettere la correttezza del voto elettronico. In risposta, il team di ricerca ha sviluppato nuovi strumenti automatizzati per testare le

1 Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). "Going from Bad to Worse: From Internet Voting to Blockchain Voting". *Journal of Cybersecurity*, 7(1), tyaa025 (Oxford University Press); Princeton University. (2006). *Security Analysis of the Diebold AccuVote-TS Voting Machine* (Feldman, A. J., Halderman, J. A., & Felten, E. W.), technical report. Riferimenti fondamentali sulla vulnerabilità dei sistemi di voto elettronico a compromissioni hardware/software e sulla fattibilità di attacchi (in laboratorio) alle DRE, inclusi scenari di manomissione e propagazione tramite supporti removibili.

2 Halderman, J. A. (2022). *The Antrim County 2020 Election Incident: An Independent Forensic Investigation*. 31st USENIX Security Symposium (USENIX Security '22). Lo studio ricostruisce l'incidente di Antrim County come esito di errori procedurali e di configurazione (non di broglio), evidenziando l'importanza di test di logica e accuratezza, processi di gestione delle configurazioni e controlli ex ante sui tabulatori.

3 Ibidem

configurazioni delle macchine con un numero ridotto di schede, rendendo i test pre-elettorali più completi e capaci di intercettare anomalie simili in futuro[4].

Un ulteriore principio emerso e diventato una best practice per mitigare le falle software è quello dell'"indipendenza dal software" (*software independence*). Questo principio, adottato ad esempio nelle linee guida federali statunitensi VVSG 2.0 del 2021, richiede che ogni voto elettronico abbia una traccia verificabile indipendente dal software, tipicamente un supporto cartaceo controllato dall'elettore[5]. In altre parole, il sistema deve poter garantire l'accuratezza del risultato finale anche qualora il software venisse corrotto da un attacco o un malfunzionamento. Stati come la Georgia, che fino al 2019 utilizzavano macchine DRE prive di ricevuta cartacea, sono passati a nuovi dispositivi con stampa del voto (*ballot marking devices*) proprio per rispettare questo criterio e consentire eventuali riconteggi manuali. Tuttavia, anche tali soluzioni non sono esenti da problemi: i nuovi sistemi della Georgia, pur producendo una scheda cartacea, utilizzano codici a barre per registrare il voto in forma leggibile dalla macchina. Analisi condotte dall'esperto J. A. Halderman hanno dimostrato che vulnerabilità nel software avrebbero permesso di alterare i codici a barre (e quindi i voti conteggiati) senza accesso fisico alla macchina, sfruttando falle poi corrette dal produttore con un *patch* software. Ciò evidenzia che l'indipendenza dal software deve essere accompagnata da un elevato livello di sicurezza informatica del sistema nel suo complesso, oltre che dalla verifica da parte degli elettori delle schede cartacee stampate.

Le reti di comunicazione e le infrastrutture IT impiegate nel voto elettronico e online rappresentano un altro punto debole. Nei sistemi di voto via Internet, i terminali degli elettori e i server remoti sostituiscono in larga parte le macchine di voto dedicate, ampliando la superfice d'attacco. Vulnerabilità nei protocolli di trasmissione, falle crittografiche o configurazioni di rete insicure possono consentire ad un aggressore di intercettare o manomettere i dati di voto in transito. Un caso rilevante è il controverso processo di conteggio rapido dei voti elettronici in Bolivia nel 2019: durante lo scrutinio preliminare online (sistema TREP), un'interruzione nella pubblicazione dei dati e la successiva ricomparsa di trend anomali alimentarono accuse di brogli. Una missione di audit dell'Organizzazione degli Stati Americani sostenne di aver riscontrato una "manipolazione intenzionale" nel sistema informatico, con deviazione di dati elettorali verso server nascosti non controllati dall'autorità elettorale, tale da invalidare i

4 Ibidem

5 U.S. Election Assistance Commission (EAC). (2021). *Voluntary Voting System Guidelines (VVSG) Version 2.0* (10 febbraio 2021) e materiali ufficiali EAC sulla certificazione; NIST. (2025). *Implementation Guidance for the VVSG 2.0* (VTS series). Le VVSG 2.0 formalizzano requisiti di sicurezza, accessibilità e verificabilità (incluso il principio di *software independence* e controlli di integrità/audit), fornendo la base per test e certificazione dei sistemi in numerose giurisdizioni.

risultati ufficiali iniziali[6]. Sebbene analisi indipendenti successive abbiano contestato parte di queste conclusioni, attribuendo l'anomalia a un afflusso ritardato ma legittimo di voti da aree filogovernative e sottolineando che il conteggio ufficiale non fu mai interrotto[7], il caso boliviano evidenzia come infrastrutture di rete opache o mal progettate possano minare la fiducia nelle elezioni. La sola percezione di vulnerabilità nel sistema di voto online (ad esempio la presenza di server non autorizzati o la mancanza di trasparenza nei flussi informativi) può infatti innescare una crisi politico-istituzionale, a prescindere dall'effettiva portata tecnica del problema.

Anche nei Paesi che hanno sperimentato con successo il voto elettronico, la sicurezza delle infrastrutture resta una preoccupazione costante. L'Estonia, pioniera del voto online a livello nazionale, adotta un sistema di i-voting con autenticazione tramite ID digitale e crittografia avanzata; eppure, verifiche condotte da esperti esterni hanno individuato in passato possibili configurazioni server insicure e procedure migliorabili, a riprova del fatto che nessun sistema connesso in rete può dirsi a rischio zero. Per questo motivo, audit indipendenti e *penetration test* periodici dovrebbero accompagnare ogni implementazione di e-voting, un principio sancito anche dagli standard internazionali: la Raccomandazione CM/Rec(2017)5 del Consiglio d'Europa, ad esempio, richiede che i sistemi di voto elettronico siano sottoposti a certificazione e audit sia prima che dopo le votazioni, e che il codice sia preferibilmente aperto o comunque ispezionabile dagli esperti accreditati[8].

Un ultimo elemento spesso sottovalutato è il fattore umano e organizzativo. Molte vulnerabilità emergono infatti da errori umani, configurazioni inadeguate o procedure operative deboli. L'episodio già citato di Antrim County rientra in questa categoria: un aggiornamento last-minute delle schede elettroniche non accompagnato da un opportuno riallineamento del software di tabulazione ha innescato l'errore di conteggio. Altro esempio: in occasione delle elezioni parlamentari ucraine del 2014, funzionari della sicurezza ucraina riferirono di aver sventato, a poche ore dal voto, un attacco informatico mirato ad alterare la

6 Organization of American States (OAS). (2019). *Final Report of the Audit of the Elections in Bolivia — Intentional Manipulation and Serious Irregularities*. (Report ufficiale dell'audit OAS sul processo elettorale boliviano 2019 e sul sistema TREP; include riferimenti ai reindirizzamenti dei flussi dati e alle criticità di architettura/trasparenza)

7 ong, G., Rosnick, D., Kharrazian, C., & Cashman, K. (2019). *What Happened in Bolivia's 2019 Vote Count?* Center for Economic and Policy Research (CEPR), report. Analisi indipendente che contesta la lettura univoca di frode intenzionale e propone un'interpretazione alternativa dei trend, sottolineando la necessità di distinguere tra anomalie statistiche, trasparenza procedurale e manipolazione provata.

8 Ballotpedia. (2025). *Deepfake policy in the United States, 2019–Present* (sezione "Political communications"). Rassegna aggiornata della legislazione statale USA sui deepfake in comunicazioni politiche: al 12 settembre 2025 risultano **28 Stati** con leggi in materia, spesso con finestre temporali pre-elettorali e obblighi di disclosure/exception per satira o contenuti etichettati.

presentazione dei risultati sul sito ufficiale, attacco reso possibile da precedenti intrusioni nella rete informatica della Commissione Elettorale[9]. Spesso procedure di sicurezza carenti – come l'assenza del controllo incrociato a "due persone" per operazioni sensibili, o la mancata verifica dei log di sistema – consentono ad attori maligni interni (insider) o esterni di agire indisturbati. All'opposto, un robusto impianto procedurale può compensare alcune vulnerabilità tecnologiche: ad esempio, l'utilizzo di verifiche manuali a campione *(risk-limiting audits)* sui risultati elettronici e la conservazione di registri cartacei aiutano a rilevare e correggere eventuali manomissioni, siano esse dolose o accidentali. In sintesi, le debolezze tecniche dei sistemi di voto elettronico, dall'hardware al software, dalla rete alle operazioni umane, richiedono un approccio di "*security by design*" e "*defense in depth*", con misure di sicurezza stratificate e ridondanti, come raccomandato anche dai nuovi standard (ad esempio, VVSG 2.0 enfatizza l'integrazione di salvaguardie di sicurezza sin dalla progettazione, invece di aggiungerle ex post).

7.3 Minacce informatiche e attacchi alle infrastrutture di e-voting

Alle vulnerabilità intrinseche si sommano le minacce esterne, ossia gli attacchi deliberati condotti da una varietà di attori (singoli hacker, gruppi di cyber-criminali, *hacktivist*, fino a unità di cyber warfare di stati ostili) con l'obiettivo di influenzare o sabotare il processo elettorale elettronico. Tali minacce possono essere schematizzate secondo la tradizionale triade della sicurezza informatica – confidenzialità, integrità, disponibilità – corrispondente a diversi tipi di attacco.

7.3.1 Attacchi all'integrità: malware, intrusioni e manomissione dei risultati.

Gli attacchi all'integrità mirano a modificare clandestinamente i voti espressi o i risultati aggregati. Il timore più grave riguardo al voto elettronico è che un aggressore possa introdurre un *malware* nelle macchine o nei server di voto, capace di alterare i conteggi senza lasciare tracce evidenti. La letteratura tecnica ha ampiamente dimostrato la fattibilità di simili attacchi in ambienti di laboratorio: già nel 2006, un gruppo di ricerca dell'Università di Princeton riuscì a installare un virus su una macchina DRE Diebold in pochi minuti, virus in grado di modificare voti e propagarsi ad altre macchine attraverso le memorie removibili

9 Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Risk in Focus: Generative AI and the 2024 Election Cycle* (Fact sheet, 18 gennaio 2024). Documento governativo che descrive come capacità GenAI possano amplificare disinformazione, social engineering (incluse clonazioni vocali), e pressioni operative sugli uffici elettorali, oltre a indicare misure di mitigazione e awareness per election officials.

utilizzate per raccogliere i risultati. Negli anni seguenti, esperti come Halderman e altri hanno affinato queste tecniche, mostrando come *malware* sofisticati possano infettare scanner di schede ottiche o componenti di gestione, alterando selettivamente percentuali di voto senza destare sospetti (ad esempio manipolando solo uno ogni N voti registrati). Fortunatamente, ad oggi non si hanno evidenze pubbliche di frodi informatiche riuscite di tale portata nelle elezioni reali; tuttavia, tentativi concreti non sono mancati. Oltre al caso ucraino del 2014 già citato, negli Stati Uniti le indagini dell'intelligence hanno rilevato che attori russi nel 2016 tentarono intrusioni su sistemi di registrazione degli elettori e sulle reti di gestione elettorale in vari stati, riuscendo in alcuni casi a penetrare nei database sebbene senza alterare dati di voto. Questi episodi sottolineano che gruppi APT *(Advanced Persistent Threat)* sponsorizzati da stati possono prendere di mira le infrastrutture elettorali per preparare possibili manipolazioni.

Un attacco all'integrità può colpire diverse fasi: la fase di voto (compromettendo il dispositivo dell'elettore o la macchina in seggio), la fase di trasmissione (man-in-the-middle sulla rete, DNS spoofing, ecc.) o la fase di tabulazione (inserendo dati falsificati nel sistema centrale). Nel voto online, il dispositivo dell'elettore rappresenta un anello debole: un computer infettato da un trojan o da *spyware* potrebbe intercettare il voto prima che sia cifrato e trasmettere un voto diverso, senza che l'elettore se ne accorga. Similmente, uno smartphone su cui giri un'app di i-voting potrebbe essere vulnerabile al *rooting* o ad exploit zero-day. Nel 2020, ricercatori del MIT hanno analizzato l'app Voatz (utilizzata in via sperimentale per il voto remoto di militari all'estero in West Virginia) scoprendo vulnerabilità che avrebbero consentito a un attaccante remoto di alterare le preferenze inviate e di violare la segretezza del voto. Questo dimostra la concreta possibilità di attacchi end-to-end nel voto via Internet se i dispositivi personali non sono altamente sicuri. Dal lato server, invece, l'attacco può prendere di mira il sistema di conteggio: ad esempio, se un aggressore ottiene credenziali di amministratore (magari tramite **social engineering** o phishing mirato verso un tecnico IT elettorale), potrebbe introdurre software maligno nel backend di tabulazione. Un caso drammatico in prospettiva fu segnalato nel Kenya nel 2017, quando l'opposizione denunciò che hacker avrebbero usato le credenziali sottratte a un funzionario della commissione elettorale (tragicamente assassinato poco prima del voto) per manipolare i risultati trasmessi elettronicamente. Nonostante le indagini ufficiali non abbiano confermato alterazioni decisive, l'episodio evidenzia come la compromissione di account privilegiati sia uno degli scenari più pericolosi per l'integrità del voto elettronico.

Alla luce di queste minacce, si raccomanda che i sistemi di e-voting implementino difese multilivello: firme digitali e cifratura forte end-to-end dei dati di voto, rigorosi controlli sugli accessi amministrativi, *air gap* o segmentazione delle reti per isolare le componenti critiche, e soprattutto meccanismi di verifica indipendente. Come sottolineato sopra, la presenza di registri cartacei verificati

dagli elettori consente di effettuare riconteggi e controlli incrociati. Ad esempio, negli USA si sono diffuse le Risk-Limiting Audits (RLA): verifiche post-elettorali su campioni casuali di schede cartacee confrontate con i risultati elettronici, che offrono un'alta probabilità di intercettare eventuali manomissioni qualora l'esito fosse alterato. Tali misure organizzative, combinate con tecnologie crittografiche come le prove a conoscenza zero nei sistemi di *end-to-end verifiable voting*, mirano a rendere estremamente difficile alterare voti senza essere scoperti. In sostanza, l'obiettivo è trasformare ogni potenziale attacco all'integrità in un'azione ad "alto rischio di rilevamento".

7.3.2 Attacchi alla disponibilità: denial of service e sabotaggi fisici

La disponibilità del sistema di voto – ossia la possibilità per gli elettori di accedere al voto e per i funzionari di concludere lo scrutinio nei tempi previsti – è anch'essa fondamentale. Attacchi mirati a negare l'accesso al sistema rientrano nella categoria del Denial of Service (DoS), in particolare in forma distribuita (DDoS). In un contesto di voto elettronico online, un attacco DDoS potrebbe saturare il sito o l'applicazione di voto remoto con traffico artificiale, rendendolo irraggiungibile per gli utenti legittimi. Un simile evento può impedire a molti elettori di esprimere il voto entro la scadenza, minando la validità dell'elezione. I timori non sono teorici: in Svizzera, durante alcuni test pubblici del sistema di e-voting, furono segnalati tentativi di sovraccaricare i server, sebbene mitigati; in Estonia nel 2007, la rete nazionale subì pesanti attacchi DDoS politici (nel contesto delle tensioni con la Russia), che fortunatamente non colpirono direttamente le finestre di e-voting ma dimostrarono la vulnerabilità delle infrastrutture estoni a tali attacchi. Anche la sola minaccia di un DDoS può intaccare la fiducia: se gli elettori temono che il portale di voto crolli sotto attacco, potrebbero rinunciare a usarlo.

Oltre al voto remoto, anche i sistemi di registrazione elettronica degli elettori o i siti web di informazione elettorale possono essere bersaglio di DDoS e sabotaggi. Nel giorno delle elezioni generali 2020, ad esempio, la Nuova Zelanda subì un massiccio attacco DDoS che colpì la Borsa e alcuni servizi online governativi; non essendo in uso il voto online generalizzato, non si registrarono effetti sul voto, ma l'episodio confermò la propensione di attori ostili a scatenare attacchi dirompenti durante eventi civili di rilievo. Analogamente, negli Stati Uniti, nei mesi precedenti le elezioni del 2020, agenzie federali come CISA avevano messo in guardia su possibili tentativi di oscurare i siti ufficiali dei risultati la notte dello scrutinio, al fine di creare confusione e vuoti informativi da riempire con disinformazione. La disponibilità comprende anche la protezione da sabotaggi fisici: un esempio è il danneggiamento deliberato di macchine di voto o di reti elettriche/di telecomunicazione nei seggi. Nel 2016, un incendio doloso in un magazzino a Torino distrusse centinaia di tablet per il voto elettronico destinati al referendum costituzionale italiano, costringendo all'uso di

schede cartacee in extremis; questo indica che non solo il *cyber*, ma anche atti vandalici tradizionali possono colpire l'infrastruttura elettronica.

Gli attacchi DoS/DDoS sono difficili da prevenire totalmente, ma mitigazioni efficaci includono l'uso di reti di distribuzione dei contenuti (*CDN*), capacità di *scaling* flessibile dei server, e strumenti di filtraggio del traffico maligno forniti dai principali operatori internet. Tuttavia, l'Intelligenza Artificiale sta aumentando la potenza e sofisticazione anche di questa tipologia di attacchi. Secondo analisi di CISA, strumenti di IA generativa possono aiutare gli aggressori a ottimizzare gli attacchi DDoS modulando automaticamente il tipo di traffico inviato per eludere i filtri di difesa e identificare in tempo reale i nodi di rete più vulnerabili. Ad esempio, un sistema IA potrebbe generare continuamente nuove varianti di pacchetti o richieste che consumano massime risorse ma risultano non immediatamente riconoscibili come anomale, superando i sistemi basati su firme statiche. Inoltre, algoritmi di *machine learning* possono essere impiegati per controllare una botnet distribuita, adattando la cadenza e provenienza del traffico malevolo per massimizzare l'impatto sul servizio di voto. Se prima orchestrare un DDoS su larga scala richiedeva una certa abilità manuale, oggi anche gruppi meno esperti potrebbero sfruttare servizi IA disponibili nel cybercrime-as-a-service per lanciare attacchi sofisticati. Questa evoluzione impone alle autorità di predisporre contromisure all'altezza, come sistemi di difesa *behavior-based* anch'essi potenziati da IA, e piani di emergenza che prevedano estensioni orarie del voto o modalità alternative (ad es. back-up su carta) nel caso un attacco DoS ne comprometta il regolare svolgimento.

7.3.3 Attacchi alla confidenzialità: violazione della segretezza del voto e dei dati elettorali

La segretezza del voto, pilastro delle moderne democrazie, può essere minacciata dagli attacchi informatici volti a violare la confidenzialità dei sistemi. In un sistema cartaceo tradizionale la segretezza è garantita strutturalmente (urne anonime, schede senza identificativo votante); in un sistema elettronico, essa dipende strettamente da protocolli crittografici e da accorgimenti tecnici che dissocino l'identità dell'elettore dalla sua preferenza. Un rischio concreto è che un attacco comprometta la base dati che associa gli elettori ai loro voti, quando tale associazione esiste almeno temporaneamente (ad esempio nei server di *Internet voting* prima dell'eventuale separazione dei dati). In più, se un sistema di e-voting non è progettato con attenzione, potrebbero emergere canali laterali per risalire al voto: per esempio, la pubblicazione dettagliata dei risultati per seggio o addirittura a livello di singola scheda (come pratica di *open data* per trasparenza) può, in certe condizioni, permettere di ricostruire il voto di un dato elettore incrociando informazioni.

Un caso reale di vulnerabilità della segretezza è stato documentato negli USA nel 2024: un team di ricerca ha scoperto che alcuni modelli di scanner di schede

Dominion utilizzati in 21 Stati memorizzavano e pubblicavano immagini digitali delle schede e liste di preferenze in modo tale che, combinando questi dati con l'ordine di arrivo dei votanti, era possibile invertire l'operazione di mescolamento e rivelare come singoli elettori avevano votato. In pratica, l'algoritmo di randomizzazione dei record elettronici non era sufficientemente robusto, configurando una violazione del segreto dell'urna. Una volta segnalato il problema, il fornitore ha rilasciato un aggiornamento software e gli esperti hanno fornito linee guida per *sanitizzare* i dati pubblicati, ma l'episodio conferma che anche la privacy dei voti è a rischio se le implementazioni non sono impeccabili.

Ulteriori minacce alla confidenzialità riguardano la fuga di dati personali dagli archivi elettorali. I database degli elettori contengono informazioni sensibili (nominativi, indirizzi, eventualmente orientamenti di partito se l'elettore li ha dichiarati per le primarie, ecc.) che possono essere oggetto di furto da parte di attaccanti informatici. Negli ultimi anni si sono verificati diversi *data breach*: ad esempio, nel 2017 i dati di oltre 198 milioni di elettori statunitensi furono esposti online da una società di analisi politica, mostrando come la superficie di rischio includa non solo i sistemi ufficiali ma anche attori terzi coinvolti nel processo elettorale. Sebbene tali incidenti non alterino i voti, possono avere effetti indiretti sulla democraticità – ad esempio facilitando campagne mirate di soppressione del voto o disinformazione calibrata sui profili demografici rubati.

Infine, attacchi alla confidenzialità possono consistere in sorveglianza illegale del processo di voto elettronico. Se un malware infetta una macchina DRE o un dispositivo di voto personale, potrebbe teoricamente registrare schermate o segnare le scelte di ogni elettore, inviandole all'attaccante. Ciò violerebbe la segretezza dell'urna e aprirebbe la porta a coercizione e voto di scambio (perché l'attaccante potrebbe poi dimostrare come ha votato l'elettore e punirlo o ricompensarlo di conseguenza). Anche senza immaginare scenari così estremi, il solo dubbio che la segretezza possa essere compromessa può minare la fiducia dei cittadini nel sistema elettronico, dissuadendoli dall'uso. Pertanto, normative e standard richiedono espressamente che i sistemi di e-voting garantiscano il segreto del voto "con lo stesso livello di sicurezza delle votazioni tradizionali". Strumenti come le schede di recupero (che consentono all'elettore di controllare che il suo voto cifrato corrisponda effettivamente alla sua scelta, senza rivelarla a terzi) e le misure organizzative (vietare qualsiasi dispositivo di ripresa nel seggio elettronico, ecc.) sono tutti volti a salvaguardare questo principio.

7.3.4 Il ruolo crescente dell'Intelligenza Artificiale negli attacchi informatici elettorali

Come accennato, l'Intelligenza Artificiale sta diventando un fattore moltiplicatore di minacce. Pur non creando ex novo nuove categorie di attacco, l'IA ne amplifica portata e velocità. Oltre agli esempi già fatti (malware generati da algoritmi e DDoS potenziati), l'IA offre strumenti avanzati per il social engineering:

reti neurali di sintesi vocale possono produrre *deepfake audio* con la voce di persone di fiducia, da usare in attacchi di phishing altamente mirati. Immagini e video deepfake possono simulare identità o eventi inesistenti, ingannando funzionari elettorali. CISA ha avvertito che malintenzionati potrebbero utilizzare la clonazione vocale per impersonare telefonicamente un tecnico di supporto e farsi rivelare password o dettagli di configurazione, o generare video falsi di presidenti di seggio che commettono brogli per seminare caos e sfiducia. Inoltre, i grandi modelli linguistici (LLM) permettono di automatizzare la produzione di email e documenti dall'apparenza credibile: un attaccante potrebbe generare valanghe di richieste FOIA pretestuose o segnalazioni di brogli tutte diverse ma plausibili, sommergendo gli uffici elettorali e distraendoli da minacce reali. Uno scenario di questo tipo è emerso negli Stati Uniti: nel 2023 alcune contee hanno ricevuto ondate coordinate di richieste di accesso agli atti e reclami identici nel contenuto ma con variazioni stilistiche, facendo sospettare l'uso di LLM per affaticare l'amministrazione (*paperwork DDoS*).

I *ransomware*, altra minaccia alla disponibilità/integrità, possono anch'essi essere resi più efficaci dall'IA: vi sono evidenze che criminali informatici stiano testando algoritmi generativi per migliorare l'offuscamento del codice malevolo e trovare più rapidamente varianti che sfuggano agli antivirus tradizionali. Un malware IA-powered potrebbe cambiare la propria firma continuamente (malware polimorfico), complicando la difesa. Infine, l'IA consente di effettuare ricognizioni automatizzate: bot intelligenti possono scandagliare siti e servizi elettorali alla ricerca di vulnerabilità note o configurazioni errate (come un database aperto su internet), fornendo agli aggressori un elenco di possibili punti deboli da sfruttare, il tutto in tempi rapidissimi rispetto a un'analisi manuale.

Riassumendo, le minacce informatiche ai sistemi di voto elettronico e online sono variegate e sempre più sofisticate. Attacchi all'integrità, disponibilità e confidenzialità possono manifestarsi singolarmente o in combinazione, spesso mirando all'effetto più dirompente: anche se l'attacco non riesce a modificare voti, può ritardare lo scrutinio o diffondere il sospetto che qualcosa sia avvenuto, con danni significativi alla credibilità del processo elettorale. La componente d' informazione e disinformazione, infatti, si sovrappone a quella tecnica: è il tema affrontato nella sezione seguente.

7.4 Disinformazione online e manipolazione dell'opinione pubblica con l'IA

Parallelamente ai rischi strettamente tecnici, le elezioni contemporanee – specialmente in scenari di voto elettronico o in situazioni di crisi – sono minacciate da campagne di disinformazione e manipolazione mediatica, spesso orchestrate sfruttando strumenti digitali avanzati. L'obiettivo di questi attacchi non è violare direttamente il sistema di voto, bensì influenzare gli elettori (nelle loro percezioni, decisioni di voto o fiducia nelle istituzioni) attraverso la diffusione massiva di contenuti falsi o fuorvianti. L'Intelligenza Artificiale gioca un ruolo di crescente importanza in tale contesto, tanto che il 2024 è stato definito da alcuni osservatori come l'anno in cui si sono verificate "le prime elezioni dell'era dell'AI" per l'impatto pervasivo che i contenuti generati da IA potrebbero aver avuto sul dibattito pubblico.

Gli esempi concreti emersi di recente sono illuminanti. Negli Stati Uniti, durante le primarie di inizio 2024, alcuni elettori del New Hampshire hanno ricevuto telefonate automatiche (robocall) generate da IA che imitavano la voce del Presidente Joe Biden, le quali li invitavano a non recarsi a votare, con il chiaro intento di diminuire l'affluenza[10]. Queste chiamate deepfake, collegate a società di telemarketing ombra, rappresentano il primo caso documentato di utilizzo di audio sintetico per interferire con un'elezione negli USA[11]. Anche se non è possibile misurare quanti elettori siano stati effettivamente ingannati, l'episodio dimostra che la tecnologia per produrre *fake audio* credibili è già nelle mani di attori ostili. In Europa, il "caso Slovacchia 2023" è divenuto emblematico di come un singolo contenuto AI fake possa alterare la narrativa elettorale: due giorni prima delle elezioni parlamentari slovacche, è circolato un file audio virale in cui il leader di un partito pro-EU discuteva di brogli elettorali con un giornalista. Si trattava di un falso generato con IA, smentito dai diretti interessati, ma uscito nel periodo di "silenzio elettorale" quando i media tradizionali non potevano efficacemente controbattere; il partito bersaglio ha subito una flessione nel consenso e ha prevalso la fazione avversaria filo-russa, alimentando la percezione (semplificata) che la *deepfake* avesse "fatto vincere le elezioni al disinformante"[12]. Studi successivi hanno evidenziato che l'effetto

10 Leingang, R. (2024). "'Disinformation on steroids': is the US prepared for AI's influence on the election?" *The Guardian*, 26 febbraio 2024. Articolo che documenta il caso delle robocall con voce sintetica attribuita a Joe Biden (New Hampshire) e inquadra il tema dei deepfake audio come vettore di interferenza informativa e di erosione della fiducia elettorale.

11 Ibidem

12 de Nadal, L., & Jančárik, P. (2024). "Beyond the deepfake hype: AI, democracy, and 'the Slovak case'". *Harvard Kennedy School Misinformation Review*, 22 agosto 2024. Analisi che problematizza il nesso causale "deepfake → esito elettorale", evidenziando fattori di contesto (polarizzazione, fiducia istituzionale, ecosistemi mediatici) che amplificano l'impatto della disinformazione.

della clip falsificata è stato amplificato da un ecosistema informativo già segnato da bassa fiducia istituzionale e forte polarizzazione, e che l'andamento elettorale non può essere spiegato in modo monocasuale attribuendolo esclusivamente a quel singolo contenuto. Resta, tuttavia, un precedente rilevante e preoccupante: dimostra quanto un artefatto sintetico plausibile, immesso nel dibattito in una finestra temporale critica, possa alterare la percezione pubblica e aumentare l'incertezza sull'integrità del processo.

In prospettiva, scenari analoghi sono replicabili in altri contesti: un deepfake credibile (ad esempio un video in cui un candidato "confessa" illeciti) diffuso a poche ore dal voto potrebbe propagarsi rapidamente attraverso social network e canali di messaggistica cifrata, rendendo difficile un'efficace attività di verifica e smentita prima che il contenuto produca effetti sul comportamento elettorale e, soprattutto, sulla fiducia collettiva nei risultati.

La disinformazione elettorale esercitata dall'IA non si limita ai candidati, ma può coinvolgere le istituzioni elettorali stesse: ad esempio, generando immagini contraffatte di operatori ai seggi che manipolano urne, o falsi comunicati ufficiali circa rinvii di voto, nel tentativo di seminare caos. CISA ha ipotizzato scenari in cui video deepfake di scontri violenti presso un seggio, creati al computer, vengano diffusi il giorno delle elezioni per spaventare gli elettori e tenerli lontani dalle urne. Un altro rischio è la moltiplicazione di contenuti di propaganda e astroturfing[13]: account falsi con foto profilo create da reti neurali (*GAN*) possono invadere le piattaforme social promuovendo narrative estreme o teorie del complotto sulle macchine di voto, alimentando movimenti negazionisti del risultato. Già il World Economic Forum nel 2023 ha indicato la disinformazione online come un rischio globale crescente, aggravato dall'IA generativa in grado di produrre quantità virtualmente illimitate di testi, immagini e video perfettamente adattati ai target prescelti.

L'IA consente anche una micro-targettizzazione più spinta: grazie agli algoritmi di raccomandazione e profilazione, i contenuti falsi possono essere confezionati e indirizzati a gruppi specifici di elettori vulnerabili a determinati

13 Con il termine *astroturfing* si indica una pratica di manipolazione dell'opinione pubblica consistente nella creazione artificiale di un'apparente mobilitazione spontanea "dal basso" (*grassroots*), in realtà orchestrata in modo centralizzato da attori politici, economici o statali. In ambito digitale, l'astroturfing si manifesta attraverso reti coordinate di account falsi o automatizzati, commenti preconfezionati, campagne di amplificazione artificiale e, sempre più frequentemente, contenuti generati o adattati tramite sistemi di intelligenza artificiale. La letteratura evidenzia come tali pratiche, soprattutto in contesti elettorali, possano alterare la percezione del consenso, rafforzare narrative polarizzanti e amplificare la disinformazione, creando l'illusione di un sostegno popolare diffuso e influenzando indirettamente il comportamento degli elettori. Cfr. Ferrara, E. et al., "The Rise of Social Bots", *Communications of the ACM*, 59(7), 2016; Woolley, S. C., & Howard, P. N., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford University Press, 2019; CISA, *Risk in Focus: Generative AI and the 2024 Election Cycle*, 2024.

messaggi. Si parla di *precision propaganda*, quando, ad esempio, un messaggio di disinformazione sui rischi del voto elettronico può essere mostrato ossessivamente a coloro che nutrono già dubbi sulla tecnologia, rinforzando la loro sfiducia (*filter bubble* potenziata da IA). Tali tecniche ricordano quelle emerse nello scandalo Cambridge Analytica, ma oggi gli strumenti sono ancor più sofisticati e accessibili.

Contrastare la disinformazione elettorale nell'era AI è una sfida complessa. Le autorità elettorali devono affiancare alle difese tecnologiche anche strategie di comunicazione proattiva: trasparenza sulle procedure, smentite rapide dei falsi virali, collaborazione con media e piattaforme online per segnalare contenuti manipolati. Alcune giurisdizioni hanno istituito "war room" contro la disinformazione durante le elezioni, coinvolgendo esperti OSINT, data scientist e comunicatori. Sul fronte normativo (come vedremo nella prossima sezione), si stanno predisponendo obblighi di *disclaimer* per i contenuti elettorali generati da IA, e divieti specifici sull'uso di deepfake ingannevoli nei periodi elettorali. Tuttavia, vi è un sottile equilibrio da mantenere per rispettare la libertà di espressione: normative troppo generiche potrebbero essere abusate per censurare legittima satira o dissenso politico. Gli studiosi avvertono di evitare approcci allarmistici unilaterali: se è vero che l'IA porta la disinformazione su scala industriale, va anche notato che spesso gli effetti di quest'ultima dipendono da vulnerabilità sociali preesistenti (polarizzazione, sfiducia istituzionale)[14]. In ogni caso, per il presente discorso è chiaro che le campagne di disinformazione basate su IA costituiscono una minaccia reale all'integrità percepita delle elezioni elettroniche, specialmente in contesti di crisi in cui la popolazione è più sensibile a paure e voci infondate.

7.5 Blockchain e voto elettronico: prospettive e rischi

Negli ultimi anni, la tecnologia *blockchain* è stata spesso proposta come panacea per risolvere i problemi di fiducia nel voto elettronico e online. La logica è intuitiva: una *blockchain* pubblica e immutabile potrebbe conservare i voti in modo tale che nessuno – né hacker malevoli né funzionari corrotti – possa alterarli senza che ciò venga immediatamente rilevato, data la natura distribuita e *trustless* di questa tecnologia. Alcune sperimentazioni hanno già avuto luogo: ad esempio, la città di Mosca ha utilizzato nel 2019 un sistema di e-voting basato su blockchain per le elezioni del consiglio comunale, mentre negli USA l'app mobile Voatz per il voto di militari all'estero affermava di registrare le preferenze su

14 de Nadal, L., & Jančárik, P. (2024). "Beyond the deepfake hype: AI, democracy, and 'the Slovak case'". *Harvard Kennedy School Misinformation Review*, 22 agosto 2024. Analisi che problematizza il nesso causale "deepfake → esito elettorale", evidenziando fattori di contesto (polarizzazione, fiducia istituzionale, ecosistemi mediatici) che amplificano l'impatto della disinformazione.

una blockchain autorizzata. Tali iniziative hanno alimentato un dibattito acceso tra sostenitori e critici dell'approccio blockchain applicato al suffragio.

I potenziali benefici che offre la blockchain sono l'*auditabilità* e l'*integrità*: una volta che un voto è scritto in un blocco e validato dalla rete, risulta estremamente difficile modificarlo retroattivamente (a meno di controllare la maggioranza della rete, scenario improbabile se la rete è sufficientemente decentralizzata). Ciò potrebbe aumentare la resistenza a brogli interni: diversamente da un database elettorale tradizionale, dove un amministratore con privilegi potrebbe alterare dati o cancellare log, in una blockchain ogni operazione è tracciata e pubblica (perlomeno agli osservatori tecnici). Inoltre, si potrebbero coinvolgere più parti terze (università, ONG, partiti) come *nodi validatori* della blockchain elettorale, creando un sistema di contro-verifica distribuito. Questo approccio richiama il concetto di *scrutinio pubblico universale* auspicato da alcuni esperti: un registro dei voti pubblicamente verificabile (ma cifrato quanto al contenuto dei voti) a cui chiunque possa applicare controlli di coerenza. In teoria, la blockchain potrebbe anche facilitare nuovi modelli di voto verificabili dall'elettore: ad esempio, ad ogni votante potrebbe essere fornito un identificativo della propria transazione di voto sulla blockchain, così da poter controllare che il proprio voto appaia (in forma anonima) nel registro globale e sia stato contato. Sistemi come *FollowMyVote* hanno esplorato questa idea per dare maggiore empowerment agli elettori, cosa difficile da ottenere con database chiusi.

Tuttavia, a fronte di queste promesse, i rischi e i limiti dell'approccio blockchain nel voto sono sostanziali. Anzitutto, la blockchain non elimina le vulnerabilità a monte e a valle del processo: se un malware compromette il dispositivo dell'elettore e cambia il voto prima che sia inviato, oppure se un coercitore costringe qualcuno a votare in un certo modo, la blockchain registrerà fedelmente un voto già falsato all'origine. Come sintetizzato in uno studio del MIT Media Lab, "passare dal voto elettronico tradizionale al voto su blockchain può significare andare *dalla padella alla brace*: si aumentano i potenziali punti di fallimento senza risolvere quelli esistenti". Gli autori di tale studio sottolineano che il voto online basato su blockchain non risolve i problemi fondamentali di sicurezza client e di autenticazione, ed in più introduce nuove problematiche. Ad esempio, la trasparenza stessa della blockchain può confliggere con la segretezza del voto: assicurare l'anonimato su un registro pubblico richiede schemi crittografici avanzati (come gli *zero-knowledge proofs*), la cui implementazione corretta è non banale e soggetta ad errori. In alcuni prototipi, è emerso il pericolo che le sequenze temporali delle transazioni potessero essere correlate agli orari di voto degli elettori, riducendo in questo modo l'anonimato.

Un altro elemento critico è la governance della blockchain. Affinché il voto elettronico abbia validità legale, deve esserci un'autorità elettorale che certifica i risultati ufficiali. Anche usando blockchain, ci sarà dunque una qualche entità (o consorzio di entità) responsabile dell'avvio della rete, della gestione

delle chiavi crittografiche di scrutinio, ecc. Questo reintroduce un certo grado di fiducia centralizzata. Se però tale autorità malintenzionata o compromessa coordinasse i nodi validatori (o detenesse la maggioranza nel caso di una *blockchain permissioned),* potrebbe manipolare comunque i dati prima che entrino in blockchain censurando determinate transazioni di voto. Ad esempio, nei test di Mosca 2019 un ricercatore francese riuscì a violare parzialmente l'algoritmo di crittografia omofonica usato, dimostrando come, con adeguate risorse, fosse possibile decifrare i voti registrati in blockchain durante la votazione (violando così la segretezza) per inserire transazioni potenzialmente malevole. Il sistema fu corretto in fretta, ma evidenziò l'elevata complessità nel coniugare senza falle blockchain e crittografia del voto.

Va anche considerata la possibilità di attacchi 51% o legati al consenso distribuito. In una blockchain pubblica tipo Bitcoin, un attaccante con oltre la metà della potenza di calcolo potrebbe riscrivere la storia delle transazioni; nel contesto di un'elezione nazionale questo scenario è remoto (sarebbe necessario un immenso dispendio di risorse in breve tempo), ma se si optasse per blockchain permissioned con pochi nodi validatori, basterebbe comprometterne la maggioranza (ad es. 3 su 5) per corrompere il registro. Inoltre, un altro difetto di blockchain è la irreversibilità completa: se venisse registrato un risultato errato (magari per un bug software), correggerlo richiederebbe il consenso di tutti i nodi in una sorta di *hard fork*, un'operazione straordinaria e delicata. Questo mal si adatta all'esigenza di flessibilità che talvolta serve nelle elezioni (si pensi a dover rimuovere dei voti dichiarati nulli dopo un ricorso, ecc.).

La comunità scientifica si mantiene dunque cauta sull'uso della blockchain nel voto. Un dettagliato rapporto del 2020 concludeva che "il voto online, incluso quello basato su blockchain, aumenterebbe drasticamente il potenziale di fallimenti catastrofici e non rilevabili su scala nazionale" e che qualunque eventuale guadagno di partecipazione elettorale grazie alla comodità verrebbe ottenuto "al costo di perdere ogni garanzia di credibilità sul fatto che i voti vengano contati come espressi". Questo giudizio, forse drastico, riflette la preoccupazione che l'introduzione di blockchain non risolve il problema fondamentale: la difficoltà di assicurare simultaneamente segretezza, integrità e verificabilità in un ambiente insicuro come Internet. Viceversa, alcuni ricercatori e startup continuano a esplorare soluzioni ibride: ad esempio, sistemi di voto elettronico E2E-V (end-to-end verifiable) che usano blockchain solo come audit trail pubblico di ricevute crittografate (non decifrabili): quindi la blockchain funge da registro di immodificabilità, mentre la verifica del voto avviene separatamente mediante protocolli crittografici[15]. Questo potrebbe mitigare alcuni rischi, ma rimane un campo sperimentale.

15 European Partnership for Democracy (EPD) & Election-Watch.EU. (2024). *The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach*. Policy paper (settembre 2024). Documento di analisi sull'AI Act con focus su integrità elettorale,

In termini critici, va anche sottolineato che la fiducia che i cittadini ripongono in una tecnologia non è automatica. La blockchain, pur essendo una parola di moda, è poco compresa nei dettagli dal grande pubblico. In assenza di una comprensione diffusa, rischia di diventare un *buzzword* usata per dare un'illusione di sicurezza ("c'è la blockchain, quindi è sicuro") mentre i veri problemi avvengono altrove. Un approccio scientificamente solido richiede invece trasparenza su ciò che la blockchain può e non può garantire. Per ora, nessuna nazione ha adottato il voto basato su blockchain su scala vincolante nazionale, limitandosi a progetti pilota. Il consenso tra molti esperti di cybersecurity elettorale è che la soluzione più robusta resti un sistema cartaceo tradizionale con scrutinio pubblico, oppure sistemi elettronici con supporto cartaceo verificabile, integrati da procedure di audit, piuttosto che soluzioni interamente digitali, blockchain incluse.

In conclusione, la blockchain presenta caratteristiche interessanti (immutabilità, trasparenza distribuita) che ben si adattano ad alcune esigenze del voto, e futuri sviluppi potrebbero renderla parte di sistemi di voto più sicuri. Ma al 2025, un atteggiamento prudente e bilanciato è d'obbligo: l'uso della blockchain nel voto non è una panacea e comporta sfide tecniche e di principio non ancora risolte. Qualsiasi implementazione dovrebbe essere attentamente valutata in contesti ristretti e a basso rischio prima di un'eventuale estensione generalizzata.

7.6 Quadro normativo e standard di sicurezza

Di fronte alle minacce e vulnerabilità descritte, il quadro normativo e regolamentare sta evolvendo sia a livello internazionale che nazionale per fissare requisiti di sicurezza e salvaguardie democratiche nel contesto del voto elettronico e dell'uso di IA nei processi elettorali.

A livello internazionale, uno dei riferimenti principali è la già menzionata Raccomandazione CM/Rec(2017)5 del Consiglio d'Europa sugli standard per e-voting. Questo documento, adottato dal Comitato dei Ministri nel 2017, aggiorna una precedente raccomandazione del 2004 e stabilisce principi giuridici e tecnici che gli Stati membri dovrebbero rispettare se intendono introdurre il voto elettronico. Tra i punti chiave: i sistemi di voto elettronico devono garantire gli stessi principi del voto tradizionale (libertà di voto, uguaglianza, segretezza, personalità, universalità); devono inoltre essere affidabili e sicuri, soggetti a certificazione da parte di organismi indipendenti, e fornire verificabilità end-to-end (ossia sia individuale che universale). La raccomandazione incoraggia fortemente l'utilizzo di meccanismi di verifica indipendenti (come registri cartacei o prove crittografiche) e la trasparenza (codice ispezionabile, pubblicazione di documentazione tecnica, osservazione elettorale anche sul software). Pur non

rischi da microtargeting e disinformazione, obblighi per sistemi ad alto rischio e interazione con DSA e regolazione della pubblicità politica.

vincolante, questo standard influenza le legislazioni nazionali europee e ha ispirato anche linee guida tecniche, come il Compendio di buone pratiche sull'e-voting pubblicato nel 2020. Inoltre, l'OSCE/ODIHR ha incluso controlli specifici sulla sicurezza cibernetica delle elezioni nelle sue osservazioni elettorali, segno che la comunità internazionale considera queste tematiche parte integrante della valutazione di regolarità di un'elezione.

Negli Stati Uniti, la regolamentazione del voto elettronico è frammentata a livello statale, ma esistono standard federali volontari di fatto: le Voluntary Voting System Guidelines (VVSG) emanate dall'Election Assistance Commission (EAC). L'ultima versione, VVSG 2.0 (adottata nel 2021), rappresenta un notevole avanzamento nell'incorporare requisiti di sicurezza robusti[16]. Come già accennato, essa impone il principio della software independence, richiedendo cioè che ogni sistema di voto produca una traccia permanente verificabile (tipicamente cartacea). Introduce inoltre criteri stringenti su *cybersecurity*: autenticazione a più fattori per accessi di amministratori, cifratura dei dati a riposo e in transito, registri di audit inalterabili, protezione fisica delle porte di comunicazione e capacità di rilevare manomissioni (tamper-evident design). Le VVSG 2.0 incorporano anche linee guida per l'usabilità e l'accessibilità, riconoscendo l'importanza che i sistemi siano fruibili da tutti gli elettori senza errori indotti – poiché un'interfaccia mal progettata può generare errori sistematici (voti non intenzionali) divenendo essa stessa una "vulnerabilità" per la correttezza del voto. Gli stati americani che adottano le VVSG 2.0 (direttamente o come base) obbligano i fornitori di macchine per il voto a sottoporsi a test federali di conformità. Ciò ha portato nel 2022-2023 a un'ondata di ricertificazioni e aggiornamenti dei sistemi in uso, soprattutto per integrare la stampa del voto laddove mancava. Parallelamente, a seguito di polemiche e cause legali sulla sicurezza del voto 2020, alcuni stati hanno rafforzato leggi locali: per esempio, la California ha vietato l'uso di sistemi di voto remoto online per elezioni ufficiali statali, mentre altri stati hanno introdotto l'obbligo di audit post-elettorali su campioni casuali.

Sul fronte normativo specifico per l'Intelligenza Artificiale, l'Unione Europea si è mossa con il Regolamento (UE) 2024/1689 noto come AI Act, il primo quadro organico per l'IA al mondo. Approvato definitivamente nel 2024 e con piena applicazione prevista entro il 2025-2026, l'AI Act adotta un approccio basato sul rischio: classifica alcune applicazioni di IA come "ad alto rischio" e impone requisiti severi di qualità, trasparenza e sorveglianza. I sistemi di IA

16 U.S. Election Assistance Commission (EAC). (2021). *Voluntary Voting System Guidelines (VVSG) Version 2.0* (10 febbraio 2021) e materiali ufficiali EAC sulla certificazione; NIST. (2025). *Implementation Guidance for the VVSG 2.0* (VTS series). Le VVSG 2.0 formalizzano requisiti di sicurezza, accessibilità e verificabilità (incluso il principio di *software independence* e controlli di integrità/audit), fornendo la base per test e certificazione dei sistemi in numerose giurisdizioni.

utilizzati in contesti elettorali rientrano esplicitamente nell'Allegato III tra gli *high-risk*: in particolare, vengono citati i sistemi destinati a influenzare gli elettori in campagne elettorali o referendum e quelli usati per attività di microtargeting politico. Ciò significa che, ad esempio, una piattaforma che utilizzi algoritmi di IA per profilare gli utenti e fornire messaggi politici personalizzati dovrà rispettare gli obblighi del regolamento (tra cui: valutazione del rischio ex ante, registrazione nel database UE dei sistemi ad alto rischio, documentazione tecnica, gestione del ciclo di vita, ecc.). Anche soluzioni di IA eventualmente integrate in procedure elettorali ufficiali (si pensi ad esempio a strumenti per scrutinare schede contestate o per supportare la gestione logistica del voto) dovranno essere sottoposte a rigorose verifiche di conformità riguardanti i criteri di accuratezza, robustezza, sicurezza e rispetto dei diritti fondamentali. Inoltre, l'AI Act vieta alcune pratiche di IA ritenute inaccettabili, come i sistemi di social scoring generale o la manipolazione subliminale su larga scala: seppure non indirizzati specificamente alle elezioni, questi divieti creano un contesto in cui certe applicazioni di IA, che potrebbero minacciare la democrazia (ad es. manipolazione cognitiva occulta degli elettori), sarebbero fuori legge.

Accanto all'AI Act, l'UE ha emanato normative complementari rilevanti. Il Digital Services Act (DSA) del 2022 obbliga le grandi piattaforme online ad adottare misure contro la diffusione di disinformazione e a garantire maggiore trasparenza sugli algoritmi di raccomandazione, specialmente in periodi sensibili come le elezioni. Inoltre, è in fase avanzata di approvazione un Regolamento sulla trasparenza della pubblicità politica che imporrà la segnalazione chiara di contenuti politici sponsorizzati e vieterà tecniche di targeting online che utilizzino dati personali sensibili (come opinioni politiche o etnia). Questo sforzo normativo complessivo riflette la consapevolezza europea dell'impatto che l'IA e le piattaforme digitali hanno sull'ecosistema elettorale: si cerca di preservare un dibattito informato e libero da interferenze occulte, intervenendo sia sul versante degli strumenti (AI Act per chi sviluppa modelli) sia su quello dei servizi digitali (DSA e norme sui social media).

Negli Stati Uniti, al contrario, non esiste ancora una legislazione federale onnicomprensiva sull'IA o sulla disinformazione politica online. Si è assistito però a iniziative puntuali: la Federal Election Commission (FEC) nel 2023 ha avviato un procedimento per aggiornare, eventualmente, le proprie regole sulle comunicazioni manipolatorie, valutando di equiparare certi deepfake politici a violazioni delle norme già esistenti contro le "false rappresentazioni" nei materiali di campagna. Al Congresso sono stati introdotti disegni di legge come il *DEEP FAKES Accountability Act* (che avrebbe imposto watermark e avvertenze sui media sintetici, con sanzioni penali per l'uso improprio in contesto elettorale), ma finora tali proposte non hanno raggiunto l'approvazione. Nel vuoto federale, sono stati gli Stati federati a legiferare: 28 Stati USA ad oggi hanno promulgato leggi relative ai deepfake in ambito politico o elettorale. La California

è stata apripista con l'Assembly Bill 730 del 2019, che proibiva la distribuzione intenzionale, entro 60 giorni dalle elezioni, di media audiovisivi "materialmente ingannevoli" manipolati per danneggiare un candidato, a meno che fossero chiaramente etichettati come parodia o artificio. Questa norma (temporanea, poi sostituita da nuove leggi nel 2023-24) ha ispirato altri: il Texas, ad esempio, con la Senate Bill 751 (2019) ha reso reato la pubblicazione di deepfake di candidati entro 30 giorni dal voto con intento diffamatorio o di influenzare gli elettori. Nel 2024 la California ha ulteriormente rafforzato il quadro con nuovi provvedimenti che impongono alle piattaforme online di rimuovere o segnalare i deepfake elettorali non etichettati e richiedono disclaimers obbligatori quando i contenuti politici sono generati da IA. Queste leggi statali, pur sollevando talvolta dubbi di compatibilità col Primo Emendamento (tanto che alcune sono oggetto di ricorsi in tribunale per possibile violazione della libertà di parola), rappresentano tentativi concreti di arginare l'ondata di disinformazione tecnologicamente potenziata.

Per quanto riguarda gli standard tecnici, negli USA è rilevante citare i lavori del National Institute of Standards and Technology (NIST), che ha pubblicato linee guida per la sicurezza informatica delle infrastrutture elettorali (es. NISTIR 8310) e più di recente un AI Risk Management Framework (2023) per guidare l'implementazione responsabile di sistemi di Intelligenza Artificiale, che può essere applicato anche in ambito elettorale per valutare e mitigare i rischi specifici. Anche l'Institute of Electrical and Electronics Engineers (IEEE) ha attivato gruppi di lavoro sul voto elettronico e su principi etici dell'IA: ad esempio, il progetto IEEE 3295 mira a standardizzare i requisiti di sicurezza e integrità per i sistemi di votazione elettronica, includendo aspetti di crittografia end-to-end. Sul piano europeo, la normativa eIDAS (Electonic Identification, Authentication and Trust Services) fornisce un quadro per l'identità digitale e le firme elettroniche che può supportare parti del processo di voto online (autenticazione sicura degli elettori, firme digitali delle schede), contribuendo alla resilienza del sistema.

In ambito nazionale italiano, il voto elettronico è disciplinato finora solo in forma sperimentale: varie leggi e decreti (dal D.L. 1/2006 all'art. 36 del D.L. 77/2021) hanno autorizzato sperimentazioni di voto elettronico in alcune consultazioni locali o per gli elettori all'estero, ma sempre subordinandole al rispetto dei principi costituzionali di segretezza e personalità del voto e sotto il controllo del Ministero dell'Interno. L'Italia, come molti altri paesi, ha adottato un approccio cauto proprio per i rischi legati alla sicurezza: le poche sperimentazioni effettuate (es. in Regione Lombardia e Veneto nel 2017 con voting machine, o il recente progetto di voto elettronico per cittadini temporaneamente all'estero) sono state accompagnate da verifiche parallele cartacee e non hanno ancora portato a un utilizzo su vasta scala. Sul versante della disinformazione e dei deepfake, in Italia valgono le norme penali generali (es. reati di diffusione

di notizie false idonee a turbare l'ordine pubblico, articolo 656 c.p.) e il Codice di Autoregolamentazione elettorale sui media, ma non esiste una legislazione specifica sui deepfake politici al 2025. Proprio per colmare tale lacuna normativa, nella XIX Legislatura è stata avanzata una proposta di legge ad hoc: l'Atto Camera 2212 (d'iniziativa On. Ascani ed altri), presentato il 23 gennaio 2025. Questo progetto mira a modificare la legge 4 aprile 1956, n. 212 (Disciplina della propaganda elettorale), introducendo disposizioni volte a prevenire e sanzionare le alterazioni delle campagne elettorali e referendarie tramite contenuti ingannevoli generati da sistemi di intelligenza artificiale. L'obiettivo dichiarato è garantire il libero e consapevole esercizio del diritto di voto: in tal senso la proposta vieta espressamente la creazione e diffusione, durante la campagna elettorale, di contenuti falsificati o manipolati (come i *deepfake*) prodotti con l'IA, imponendo al contempo un obbligo di etichettatura chiara per qualsiasi materiale di propaganda generato con sistemi di IA.

Il meccanismo di enforcement delineato affida la vigilanza all'Autorità per le Garanzie nelle Comunicazioni (AGCOM), con poteri di rimozione immediata dei contenuti illeciti e, nei casi più gravi, di blocco dei siti o indirizzi online che li diffondono. Sono previste sanzioni amministrative pecuniarie significative (multe fino a 250.000 euro) e perfino una nuova fattispecie penale: la diffusione intenzionale di deepfake o altri media artefatti allo scopo di manipolare il voto verrebbe punita con la reclusione da 1 a 4 anni. Non mancano cautele a tutela della libertà di espressione: il divieto non si applicherebbe ai contenuti a fini didattici, informativi o di satira politica, purché tali materiali risultino chiaramente riconoscibili come non autentici. Il testo di A.C. 2212 richiama inoltre espressamente il quadro normativo europeo vigente, dal Regolamento (UE) 2024/900 sulla trasparenza della pubblicità politica al GDPR e al Digital Services Act, e coinvolge il Garante Privacy per gli aspetti attinenti al trattamento dei dati personali e alle tecniche di microtargeting online.

Al 5 novembre 2025, lo stato dell'iter parlamentare della proposta risulta ancora fermo alla prima lettura in Commissione: l'esame in I Commissione Affari Costituzionali, avviato il 18 giugno 2025, è tuttora in corso. Ciò testimonia l'attenzione crescente del legislatore verso la necessità di contrastare le nuove forme di manipolazione digitale del consenso elettorale, dotando l'ordinamento di strumenti mirati per preservare l'integrità delle campagne democratiche dall'impatto delle IA generative.

Tuttavia, come Stato membro UE, l'Italia beneficerà direttamente dell'applicazione del DSA e del futuro AI Act, e ha organismi come l'AGCOM attivi nel monitorare la disinformazione online durante le campagne (con poteri di intervento contro le piattaforme, rafforzati di recente).

In sintesi, il quadro normativo e standard sta rafforzando i bastioni a tutela delle elezioni digitalizzate: da un lato fissando criteri tecnici più stringenti per i sistemi (certificazione, audit, requisiti di sicurezza e veridicità algoritmica),

dall'altro aggiornando le leggi per sanzionare gli abusi emergenti (deepfake, propaganda micro-mirata illecita). Malgrado ciò, le normative inseguono una minaccia in evoluzione continua, e l'effettiva implementazione di standard elevati dipende anche dalla volontà politica e dalle risorse. Ad esempio, negli USA l'adozione di VVSG 2.0 richiede finanziamenti agli stati per sostituire le vecchie macchine; in UE l'AI Act dovrà essere applicato e fatto rispettare dai singoli stati con autorità nazionali competenti ancora da rodare. Rimane cruciale la cooperazione internazionale e lo scambio di *best practice*, dato che le minacce informatiche alle elezioni travalicano i confini (si pensi alle interferenze russe in vari processi elettorali occidentali). Un auspicio condiviso da esperti e istituzioni è che la sicurezza elettorale diventi parte integrante della cultura della cybersecurity nazionale, riconoscendo le elezioni come infrastruttura critica (cosa avvenuta formalmente negli USA dal 2017 e in vari paesi UE più di recente). Ciò implica test di penetrazione regolari, piani di risposta a incidenti informatici durante il periodo elettorale, formazione specifica per il personale elettorale, e campagne di alfabetizzazione digitale per gli elettori stessi.

7.7 Conclusioni

L'analisi svolta evidenzia che i sistemi di voto elettronico e online, pur rappresentando un'importante innovazione per la partecipazione democratica tanto in situazioni di stabilità quanto e soprattutto in contesti di crisi globale, presentano sempre un ampio ventaglio di minacce e vulnerabilità che non possono essere ignorate. Dal punto di vista tecnico, ogni componente, dall'hardware al software, dalla rete alle procedure umane, deve essere considerato un potenziale punto debole da proteggere con misure di sicurezza multilivello. Gli attacchi informatici possono colpire l'integrità dei risultati, la disponibilità del servizio di voto e la confidenzialità delle scelte degli elettori; l'avvento di strumenti di Intelligenza Artificiale rende tali attacchi più efficaci, automatici e difficili da contrastare con i soli metodi tradizionali. Parallelamente, l'IA ha aperto nuovi fronti di scontro sull'"opinione pubblica digitale", con la disinformazione algoritmica che può mettere in crisi la fiducia nelle elezioni almeno quanto un attacco informatico diretto. Di fronte a questo scenario, non esiste una soluzione semplice o puramente tecnologica. Ad esempio, l'adozione della blockchain nel voto – da alcuni indicata come panacea miracolosa – si è rivelata un'arma a doppio taglio, con benefici limitati e rischi aggiuntivi secondo gran parte degli studi scientifici attuali. Più che confidare in tecnologie risolutive, occorre un approccio sistemico improntato alla sicurezza, alla trasparenza e alla resilienza. Ciò include: progettare i sistemi di e-voting seguendo standard rigorosi (come VVSG 2.0 e Rec(2017)5 CoE), prevedere sempre meccanismi di verifica indipendente (audit trail cartaceo o prove crittografiche solide), sottoporre ogni componente a verifiche e test pubblici, e predisporre piani di emergenza per scenari avversi

(cyberattacchi il giorno del voto, malfunzionamenti diffusi, campagne di fake news virali, ecc.). Le istituzioni devono inoltre aggiornare continuamente il quadro normativo per colmare le lacune mano a mano che le nuove minacce emergono: l'esperienza recente con i deepfake e le normative di contrasto in UE e USA ne è un esempio, ma altri fronti potrebbero aprirsi (si pensi a futuri utilizzi di IA per influenzare referendum tramite chatbot interattivi, o a rischi quantistici per la crittografia del voto online).

In definitiva, l'uso dell'IA nel contesto elettorale, tanto da parte dei difensori dell'integrità del voto quanto da parte di chi volesse sovvertirla, è un fattore destinato a crescere. Mentre l'IA può aiutare a potenziare la sicurezza (ad esempio nei sistemi di *intrusion detection*, nel monitoraggio in tempo reale di anomalie di affluenza o nel debunking rapido di notizie false), il suo impiego malevolo può creare minacce senza precedenti. L'equilibrio tra innovazione tecnologica e tutela dei princìpi democratici richiede dunque uno sforzo interdisciplinare: informatici, giuristi, politologi e decisori pubblici devono lavorare insieme per assicurare che l'introduzione di tecnologia nel voto avvenga in modo graduale, controllato e sostenibile. Gli errori o le falle in questo campo hanno un costo elevatissimo, perché incidono sul cuore della legittimità democratica.

Come parte della presente monografia sull'impatto dell'IA sul voto elettronico nelle crisi globali, questo capitolo ha messo in luce con sguardo critico i pericoli da affrontare. Nei capitoli successivi si discuteranno possibili soluzioni e *best practice* per mitigare questi rischi, dalla progettazione di sistemi di voto più sicuri sin dall'inizio, alle strategie di *cyber diplomacy* per prevenire interferenze straniere, fino alle campagne di educazione civica digitale per creare una resilienza sociale alla disinformazione. Solo con un approccio olistico e proattivo sarà possibile cogliere i benefici dell'innovazione nel voto senza comprometterne l'integrità, anche nelle situazioni straordinarie imposte dalle crisi globali.

Capitolo 8
Implicazioni legali ed etiche

8.1 Introduzione

Se è vero che le consultazioni elettorali rappresentano il momento in cui si manifesta in forma diretta la sovranità popolare e si rinnova la legittimazione democratica delle istituzioni e che dunque nel voto si esprime l'atto costitutivo della democrazia, attraverso cui il corpo elettorale conferisce legittimità al potere pubblico secondo regole condivise, altrettanto indubbio è che negli ultimi anni sono emerse sfide senza precedenti dovute a crisi globali come pandemie sanitarie, conflitti armati e disastri climatici. Tali situazioni di emergenza hanno richiesto l'adozione rapida di strumenti di voto elettronico e altre soluzioni tecnologiche per garantire la continuità dei processi elettorali. Le tecnologie digitali hanno offerto nuove opportunità di partecipazione consentendo il voto a distanza quando le tradizionali operazioni di voto in presenza risultavano impraticabili, ma al contempo hanno introdotto rischi e incognite legali ed etiche di grande rilievo. In particolare, l'impiego sempre più diffuso dell'intelligenza artificiale (IA) in ambito elettorale ha amplificato la portata di fenomeni come la disinformazione automatizzata, la manipolazione dell'opinione pubblica tramite social bot e contenuti sintetici, nonché il trattamento massivo di dati personali sensibili. Come evidenziato anche in contesti internazionali, se da un lato le tecnologie di informazione e comunicazione promettono modalità innovative di espressione del voto, dall'altro l'IA e gli strumenti cibernetici estendono il perimetro di possibili interferenze e manipolazioni nel periodo elettorale. In una fase storica segnata da crisi successive, le istituzioni democratiche si trovano a dover bilanciare con attenzione l'adozione di misure eccezionali con il rispetto dei principi fondamentali del diritto elettorale, primo fra tutti quello di elezioni libere ed eque anche nelle circostanze più avverse.

Questo capitolo, pertanto, intende esaminare in maniera organica le principali implicazioni legali ed etiche derivanti dall'impatto dell'IA sul voto elettronico in tempi di crisi globale. Verranno analizzati il quadro normativo emergente e le responsabilità giuridiche (Sez. 8.2), le sfide etiche per la tutela dei valori democratici (Sez. 8.3) e tre sviluppi innovativi di grande attualità: l'IA generativa applicata ai deepfake politici (Sez. 8.4), la questione della sovranità digitale nelle odierne *guerre ibride* (Sez. 8.5) e il nascente ambito del diritto computazionale elettorale (Sez. 8.6). Si conclude con una sintesi delle considerazioni emerse (Sez. 8.7). L'analisi, rivolta a un pubblico esperto di diritto, cybersecurity, I.A. e governance elettorale, punta a fornire una visione complessiva e aggiornata a

luglio 2025 di come l'I.A. stia ridefinendo i confini della materia elettorale sotto il duplice profilo normativo ed etico.

8.2 Implicazioni legali e adeguamenti normativi

L'introduzione dell'I.A. nel ciclo elettorale solleva importanti questioni giuridiche, che richiedono l'adeguamento dei quadri normativi esistenti e l'elaborazione di nuove regole a tutela dell'integrità del voto. In primo luogo, l'impiego di sistemi automatizzati nel voto elettronico deve conformarsi ai princìpi costituzionali e internazionali in materia elettorale, come quelli di uguaglianza, segretezza e libertà del voto, che conservano valore vincolante anche durante situazioni di emergenza.

La base di tali principi, nel contesto italiano, è l'art. 48 della Costituzione, il quale sancisce che «il voto è personale ed eguale, libero e segreto. Il suo esercizio è dovere civico». Ne discende che qualsiasi introduzione di tecnologie nel processo elettorale (ivi compresi il voto elettronico e l'uso di sistemi di IA), deve rispettare rigorosamente questi requisiti costituzionali, garantendo in particolare la personalità e la segretezza del voto nonché l'uguaglianza di ogni suffragio. In altri termini, l'innovazione tecnica non può mai derogare ai princìpi fondamentali del diritto di voto, ma deve piuttosto servire a renderne più efficace l'attuazione pratica (ad esempio ampliando l'accessibilità del voto senza compromettere libertà e segretezza).

Parallelamente, a livello sovranazionale, si registra un chiaro indirizzo politico verso la trasformazione digitale della democrazia. Nella Comunicazione «2030 Digital Compass: the European way for the Digital Decade» del 9 marzo 2021, la Commissione europea ha delineato la visione di un'Europa digitalmente inclusiva entro il 2030. Tra gli obiettivi figurano il pieno accesso di tutti i cittadini alla vita democratica online, anche attraverso il ricorso al voto elettronico sicuro e affidabile, ritenuto uno strumento capace di favorire una maggiore partecipazione civica. Questo significa che l'UE auspica piattaforme di e-voting che, sfruttando anche tecnologie avanzate (come l'IA per migliorare usabilità e sicurezza), permettano a chiunque – comprese le persone con disabilità – di esercitare facilmente i propri diritti politici da remoto. Tale spinta verso la digitalizzazione del voto, tuttavia, deve armonizzarsi con i vincoli costituzionali interni: l'adozione di sistemi elettronici e di soluzioni basate sull'IA dovrà infatti avvenire nel rispetto dei principi di libertà, uguaglianza e segretezza sanciti dall'art. 48 Cost., così da coniugare innovazione tecnologica ed effettiva tutela dei diritti democratici fondamentali.

Le norme eccezionali adottate per consentire il voto in pandemia o in contesti bellici non possono derogare a tali principi cardine: ad esempio, soluzioni di voto online o postale implementate in tempi di crisi devono garantire che ogni elettore possa esprimersi senza coercizioni, che il voto resti segreto e che nessun

voto valga più di un altro, pena la violazione del diritto a libere elezioni sancito anche dall'art. 3 del Protocollo I CEDU[1]. Ne discende la necessità di una responsabilizzazione giuridica chiara per i soggetti che progettano, forniscono e gestiscono sistemi di e-voting basati su IA: qualora un malfunzionamento algoritmico o un attacco informatico comprometta il risultato elettorale, occorre stabilire chi ne risponde legalmente e con quali rimedi per gli elettori lesi. Attualmente, molti ordinamenti si trovano sprovvisti di disposizioni specifiche sulla responsabilità civile o penale legata a errori o abusi di sistemi di voto automatizzati, imponendo un aggiornamento legislativo in tale direzione, senza mai trascurare gli aspetti di Digital forensics[2].

Un secondo profilo cruciale attiene alla protezione dei dati personali nel contesto elettorale. L'uso di IA può comportare la raccolta e l'elaborazione massiva di dati sensibili degli elettori, ad esempio nelle tecniche di autenticazione biometrica del votante, nei sistemi di registrazione elettronica o nelle piattaforme di voto online. Tali trattamenti devono rispettare rigorosamente la normativa vigente in materia di privacy (in Europa, il Regolamento Generale UE 2016/679 – GDPR) e i princìpi di minimizzazione e finalità dei dati. Studi recenti hanno evidenziato possibili contrasti tra l'uso intensivo di big data per scopi politico-elettorali e alcuni obblighi del GDPR, come il principio di limitazione della conservazione e il divieto di profilazione su larga scala senza adeguate basi giuridiche. Ad esempio, la pratica del *microtargeting* politico, ossia l'invio di messaggi personalizzati agli elettori tramite algoritmi che profilano gusti e opinioni politiche, è messa in discussione in quanto potenzialmente lesiva del diritto degli interessati a non essere sottoposti a decisioni automatizzate totalmente opache e a ottenere spiegazioni sulle logiche di tali sistemi[3]. A tutela della trasparenza, l'Unione Europea ha di recente adottato il Regolamento (UE) 2024/900 sulla trasparenza e targeting della pubblicità politica, che impone obblighi stringenti di disclosure sugli sponsor, sui criteri di targeting utilizzati e vieta l'uso di dati personali sensibili (come opinioni politiche o appartenenza etnica) per il

1 Consiglio d'Europa – Assemblea parlamentare, *Elections in times of crisis: challenges and opportunities* (Rapporto e Dichiarazione di Berna, 9–10 maggio 2023); Convenzione europea dei diritti dell'uomo, Protocollo addizionale n. 1, art. 3 (*Right to free elections*) e relativa giurisprudenza della Corte EDU. I riferimenti richiamano l'obbligo di garantire elezioni libere ed eque anche in situazioni eccezionali, nel rispetto dei principi di suffragio e delle garanzie sostanziali di libertà e segretezza del voto.

2 Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press, 2011; Consiglio d'Europa, iniziative e documenti sul rapporto tra interferenze cyber e processi democratici. Le fonti supportano l'esigenza di responsabilizzazione giuridica e tracciabilità forense nei sistemi elettorali digitali, soprattutto quando decisioni o malfunzionamenti algoritmici incidono su diritti fondamentali.

3 Coniglione, C., "L'utilizzo dei big data in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa", *Nomos – Le attualità nel diritto*, 1/2023; Regolamento (UE) 2016/679 (GDPR), artt. 5, 6, 9, 22 e 35. Le fonti inquadrano le tensioni tra profilazione/microtargeting e principi di trasparenza, proporzionalità e tutela degli interessati.

microtargeting elettorale senza il consenso esplicito dell'interessato[4]. Questa normativa, prima nel suo genere, mira a prevenire forme di manipolazione occulta dell'elettorato rese possibili dall'IA, assicurando che gli elettori siano consapevoli quando vengono bersagliati da messaggi politici personalizzati e potenzialmente divisivi.

In parallelo, diverse giurisdizioni stanno sperimentando requisiti di trasparenza algoritmica applicati al contesto elettorale: ad esempio, proposte di legge negli Stati Uniti mirano a imporre *impact assessment* e audit indipendenti sugli algoritmi utilizzati nelle campagne politiche e nell'amministrazione del voto, affinché eventuali bias o rischi siano identificati e corretti prima di incidere sui diritti degli elettori.

Un ulteriore ambito normativo in evoluzione riguarda il contrasto alle interferenze straniere e alla disinformazione online mediate dall'IA. Le campagne di manipolazione informativa orchestrate da attori statali o gruppi organizzati, spesso sono indicate come forme di *ibridazione bellica*, hanno spinto molti ordinamenti a rafforzare gli strumenti legali per proteggere la sovranità dei processi elettorali. A livello internazionale, si registra una tendenza a classificare i sistemi di IA orientati a influenzare l'esito di elezioni o referendum come sistemi ad alto rischio, soggetti a regolazione speciale. Emblematico è il nuovo Regolamento europeo sull'IA (AI Act), il quale include tra gli *high-risk AI* proprio quei sistemi destinati a influire sull'opinione politica o sulle scelte di voto dei cittadini[5]. In base al testo approvato dal Parlamento europeo, tali applicazioni dovranno rispettare requisiti rigorosi di trasparenza, documentazione e controllo umano, e saranno vietate se comportano manipolazioni cognitive indebite degli elettori[6]. Contestualmente, già nel marzo 2023 il Consiglio d'Europa emanava le Linee guida sulla manipolazione dell'informazione che invitano gli Stati membri a criminalizzare le forme più gravi di interferenza digitale nei processi democratici e a cooperare nello scambio di intelligence su cyberattacchi a infrastrutture elettorali[7]. In sintesi, il panorama normativo si sta rapidamente adattando: accanto ai tradizionali principi del diritto elettorale, emergono nuove normative settoriali su IA ed elezioni che intendono preservare la regolarità del voto elettronico e

4 Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio sulla trasparenza e il targeting della pubblicità politica. La disciplina rafforza gli obblighi di disclosure su sponsor e criteri di targeting e limita l'uso di categorie particolari di dati personali in contesto elettorale.

5 Regolamento (UE) 2024/1689 (*Artificial Intelligence Act*), con particolare riferimento ai sistemi ad alto rischio, agli obblighi di gestione del rischio, trasparenza, controllo umano e alle pratiche vietate per manipolazione indebita dei diritti fondamentali.

6 Ibidem

7 Consiglio d'Europa – Steering Committee on Media and Information Society (CDMSI), *Guidance Note on countering the spread of online mis- and disinformation in a human rights compliant manner*, 2023; Dichiarazione di Berna 2023. I documenti delineano raccomandazioni operative per contrastare la manipolazione informativa nei processi democratici nel rispetto dei diritti umani.

la fiducia pubblica nelle procedure democratiche, anche in scenari di crisi. Il fine ultimo è assicurare che l'innovazione tecnologica non vanifichi le garanzie giuridiche conquistate nel corso di decenni, ma venga incanalata entro limiti e responsabilità ben definite a tutela della sovranità popolare.

8.3 Sfide etiche e tutela dei principi democratici

Oltre ai profili giuridici, l'adozione dell'IA nel voto elettronico innesca una serie di dilemmi etici che le autorità e la società civile devono affrontare per preservare i valori democratici. Uno dei nodi principali è quello della giustizia e dell'inclusività del processo elettorale. Gli algoritmi di IA possono introdurre o amplificare bìas sistemici: ad esempio, sistemi di verifica automatica dell'identità o di conteggio dei voti potrebbero funzionare in modo meno accurato per determinate minoranze etniche o categorie sociali, se addestrati su dati non rappresentativi. Ciò creerebbe discriminazioni de facto nel diritto di voto, minando il principio di eguaglianza politica. Diversi studi hanno evidenziato come i bìas nei dataset di addestramento possano perpetuare pregiudizi razziali o di genere anche nelle applicazioni elettorali, così come errori algoritmici apparentemente neutri possano tradursi in esclusione di elettori legittimati (ad esempio, cancellazioni improprie da liste elettorali). Equità algoritmica significa dunque garantire che gli strumenti di IA impiegati in qualsiasi fase – dalla registrazione dei votanti fino allo spoglio elettronico – non operino differenze ingiustificate tra cittadini. Ciò richiede un'attenta fase di progettazione etica: selezione di dati equilibrati, monitoraggio continuo degli output e presenza di meccanismi di ricorso per correggere eventuali decisioni automatizzate errate. In mancanza di tali accorgimenti, l'IA rischia di amplificare le disuguaglianze esistenti, con i gruppi già emarginati più esposti a errori e abusi. Proprio per questo, organizzazioni internazionali come International IDEA sostengono la necessità di porre etica e diritti umani al centro di ogni applicazione di IA in ambito elettorale, sviluppando linee guida che si richiamino ai valori democratici e alla responsabilizzazione degli sviluppatori sin dalla fase di design.

Il tema della trasparenza è un ulteriore caposaldo etico. Nei processi democratici è essenziale che gli attori e gli elettori possano comprendere, almeno nelle linee generali, come funzionano gli strumenti che incidono sull'espressione del voto o sull'informazione politica. I sistemi di IA spesso operano come *scatole nere*, con logiche decisionali opache persino per i tecnici che li hanno creati. Ciò contrasta con l'esigenza etica (e giuridica) di spiegabilità: in un contesto elettorale, ad esempio, un elettore escluso da un sistema automatico di autenticazione ha il diritto morale (oltre che potenzialmente legale) di sapere perché la macchina ha rifiutato il suo riconoscimento. Il *diritto alla spiegazione* dei processi algoritmici, benché non ancora definito compiutamente a livello normativo, è invocato dalla dottrina come corollario del principio democratico di

trasparenza. Oltre che per i cittadini, la trasparenza dei sistemi è fondamentale per consentire audit indipendenti da parte di osservatori elettorali, accademici e organizzazioni non governative: solo aprendo all'esame pubblico gli algoritmi di conteggio o di gestione del voto è possibile verificare che rispettino i requisiti di accuratezza e imparzialità. L'etica dell'IA applicata al voto impone dunque di mitigare l'opacità tipica dei modelli di machine learning, tramite documentazione accessibile, pubblicazione di codici sorgente critici e confronto interdisciplinare tra informatici, giuristi ed esperti di etica. Iniziative come le *Ethical AI Guidelines* della Commissione Europea incoraggiano proprio questa cultura della trasparenza e dell'accountability, affermando che l'IA "affidabile" deve tra l'altro garantire la tracciabilità delle decisioni e la supervisione umana continua. Nel contesto elettorale, ciò potrebbe tradursi nell'istituzione di comitati etici presso le autorità elettorali, incaricati di sovrintendere all'implementazione dei sistemi automatizzati e riferire pubblicamente sul loro operato.

Un'altra sfida etica rilevante è la tutela sia dell'autonomia decisionale dell'elettore sia della genuinità del dibattito democratico nell'era dell'IA. La crescente pervasività di algoritmi di raccomandazione e di content curation nei social media fa sì che gran parte degli elettori riceva informazioni politiche in forme personalizzate e potenzialmente distorte. L'IA consente di costruire *filter bubble* informative su misura per ciascun utente, mostrando solo contenuti coerenti con le sue convinzioni o manipolando l'ordine delle notizie per influenzarne le reazioni emotive. Ciò pone un problema etico di pluralismo informativo: se ogni elettore vive in una bolla algoritmica, il confronto democratico può divenire frammentato e polarizzato. Inoltre, tecniche di persuasione algoritmica avanzata, come il *neuromarketing* politico che sfrutta big data e psicometria, possono ridurre lo spazio per un libero formarsi dell'opinione, avvicinandosi a forme di manipolazione mentale di massa. Diviene eticamente imprescindibile chiedersi dove tracciare il confine tra lecito convincimento politico e influenza indebita perpetrata tramite IA. In questo senso, documenti come la Dichiarazione di Berna 2023 del Consiglio d'Europa hanno ribadito che, anche in tempi di crisi, occorre resistere a derive autoritarie e preservare un ecosistema informativo sano, contrastando la manipolazione e garantendo ai cittadini la possibilità di formarsi opinioni autonome su basi fattuali. Le strategie etiche raccomandate includono programmi diffusi di alfabetizzazione mediatica e digitale - per aiutare gli elettori a riconoscere contenuti falsi o generati dall'IA, come vedremo meglio in seguito -, e l'istituzione di organismi di vigilanza indipendenti che monitorino l'impatto dell'IA sul discorso pubblico, segnalando in tempo reale campagne di disinformazione o incitamento all'odio orchestrate via algoritmi. Sul versante opposto, va riconosciuto che la stessa IA potrebbe essere impiegata con finalità etiche: ad esempio, strumenti automatizzati di *fact-checking* e rilevazione di fake news possono aiutare a contenere la diffusione virale di notizie false durante le campagne elettorali. L'etica dell'IA nel voto elettronico

deve pertanto bilanciare un approccio precauzionale, che mitighi i rischi per i diritti e i valori democratici, con la valorizzazione delle opportunità benefiche dell'IA, assicurando sempre che al centro resti la dignità e l'autodeterminazione dell'essere umano. Come suggerito in un rapporto dell'OSCE, l'adozione di un approccio basato sui diritti umani fin dalla fase di progettazione delle politiche è cruciale: l'IA elettorale deve essere human-centric, potenziando la partecipazione informata anziché comprometterla.

8.4 IA generativa e *deepfake* politici

Uno degli sviluppi tecnologici più insidiosi emersi di recente è l'uso di IA generativa per produrre *deepfake* nel contesto politico-elettorale. I *deepfake* sono contenuti audio-visivi sintetici, generati da algoritmi di apprendimento profondo, capaci di simulare in modo estremamente realistico l'aspetto e la voce di personaggi esistenti. In ambito elettorale, essi possono essere usati per creare falsi video o audio di candidati e leader politici mentre compiono azioni o pronunciano dichiarazioni mai avvenute nella realtà. Questa tecnologia pone sfide legali ed etiche di prim'ordine, in quanto può ingannare massivamente gli elettori, minare la reputazione dei candidati e inquinare il dibattito pubblico nei momenti decisivi prima del voto. Gli esempi concreti non mancano: alla vigilia delle elezioni slovacche dell'ottobre 2023, sono circolate tracce audio deepfake attribuite falsamente al leader progressista Michal Šimečka, in cui sembrava ammettere brogli elettorali e altre affermazioni scandalose; questi falsi, diffusi pochi giorni prima del voto, sono stati ascoltati da migliaia di cittadini e alcuni osservatori hanno ipotizzato che abbiano potuto influenzare l'esito finale, molto risicato, a favore della parte avversaria. Allo stesso modo, negli Stati Uniti, già durante le primarie del 2024 si sono visti i primi spot elettorali contenenti immagini generate da IA: celebre il caso del video diffuso dal team del governatore Ron DeSantis con fotomontaggi deepfake che raffiguravano l'ex Presidente Trump in atteggiamenti mai tenuti realmente, come abbracciare l'immunologo Anthony Fauci, il tutto al fine di solleticare specifiche sensibilità dell'elettorato conservatore.

Questi episodi illustrano il potenziale destabilizzante dei deepfake: diffusi in prossimità delle urne, quando i tempi per le smentite sono ridottissimi, possono seminare confusione, alimentare teorie cospirative e minare la fiducia nell'informazione proprio nel momento cruciale in cui gli elettori formano la loro scelta. Dal punto di vista etico, i deepfake politici violano l'aspettativa di veridicità del discorso pubblico, sfruttando l'IA per creare menzogne difficili da discernere. Possono costituire una forma di inganno deliberato degli elettori, incompatibile con il principio democratico secondo cui il voto deve basarsi su un consenso informato. Inoltre, spesso tali falsi colpiscono con particolare virulenza categorie vulnerabili: si pensi ai deepfake a sfondo sessuale usati per

screditare candidate donne – una moderna arma di violenza di genere digitale che mira a estrometterle dalla vita pubblica tramite la vergogna e le minacce. Il rischio etico è dunque duplice: da un lato la manipolazione cognitiva di massa, dall'altro la violazione della dignità individuale delle vittime ritratte nei deepfake.

Di fronte a questi pericoli, le implicazioni legali stanno rapidamente evolvendo. Numerosi ordinamenti hanno avviato interventi normativi per arginare l'uso malevolo dei deepfake in contesto elettorale. Negli Stati Uniti, in assenza (finora) di una normativa federale, sono stati gli Stati membri a prendere l'iniziativa: a metà 2025, ben 25 Stati federati avevano già emanato leggi specifiche che vietano o regolano la diffusione di media falsificati da IA durante le campagne elettorali[8]. Tali leggi spesso proibiscono la pubblicazione di video o audio falsi che rappresentino candidati a fini di denigrazione, almeno in prossimità delle elezioni (tipicamente nelle due, tre settimane precedenti il voto), salvo che siano chiaramente etichettati come contenuto artificiale. Si tratta di misure pensate per tutelare gli elettori da inganni su larga scala: il fatto che solo 5 Stati USA avessero leggi simili prima del 2024, e altri 20 le abbiano introdotte sull'onda della crescente consapevolezza del fenomeno, dimostra quanto sia diventato urgente predisporre safeguards normativi contro i deepfake politici.

Anche altrove si registrano sviluppi analoghi: la Cina, già nel 2022, ha imposto l'obbligo di indicare con appositi watermark ogni contenuto generato da IA, e l'Unione Europea nel negoziato sull'AI Act ha incluso disposizioni che impongono ai generatori di media sintetici di segnalare chiaramente la natura artificiale dei contenuti, salvo eccezioni per satira o arte[9]. Tuttavia, queste risposte normative sollevano a loro volta interrogativi: come garantire l'applicazione effettiva di tali divieti nell'ecosistema globale di Internet, dove un deepfake prodotto all'estero può diffondersi viralmente ovunque? E come bilanciare il divieto di deepfake con la libertà di espressione, specialmente quando si tratta di parodie politiche? Ad esempio, alcune leggi statali americane esentano dal divieto i contenuti satirici o palesemente ironici, per non incorrere in censure eccessive. Il confine tra tutela della verità e censura politica può farsi sottile. In ambito etico-legale, una soluzione equilibrata sembra essere quella di privilegiare la trasparenza: obbligare per legge all'inserimento di avvertenze visibili (come filigrane o disclaimer audio) nei contenuti generati da IA, anziché bandirli totalmente, in modo da informare lo spettatore senza sopprimere la creatività o la satira. Alcune piattaforme online hanno già adottato politiche del genere: ad

8 Rassegne legislative statunitensi aggiornate al 2025 documentano l'adozione, da parte di numerosi Stati, di norme specifiche sui deepfake in ambito elettorale, con divieti temporali, obblighi di etichettatura ed eccezioni per satira e parodia, nel bilanciamento con la libertà di espressione.

9 Regolamento (UE) 2024/1689 (*Artificial Intelligence Act*), con particolare riferimento ai sistemi ad alto rischio, agli obblighi di gestione del rischio, trasparenza, controllo umano e alle pratiche vietate per manipolazione indebita dei diritti fondamentali.

esempio, Twitter e Facebook dichiarano di rimuovere o segnalare con etichette i media manipolati suscettibili di fuorviare il pubblico sulle questioni politiche. L'efficacia di queste misure resta però incerta, specie se i deepfake vengono diffusi attraverso canali privati (chat crittografate, piccoli forum) sfuggendo al radar delle grandi piattaforme.

Dal punto di vista delle autorità elettorali e dei governi, fronteggiare i deepfake richiede un insieme di azioni coordinate. Oltre agli interventi normativi repressivi (sanzioni penali o amministrative per chi crea e diffonde deepfake dannosi), è indispensabile investire in tecnologie anti-deepfake: sistemi di rilevazione automatica basati su IA stessa, capaci di analizzare video e audio e identificare tracce di artificiosità (ad esempio imperfezioni pixel o incongruenze nel timbro vocale). La ricerca in questo campo è una rincorsa continua tra lancia e scudo: a ogni avanzamento nella generazione di falsi corrisponde uno sforzo per potenziare gli algoritmi di detection. Purtroppo, al momento molti deepfake sofisticati riescono ancora a eludere i rilevatori automatici, specie se questi ultimi non dispongono di accesso all'originale con cui fare un confronto. Ecco perché è fondamentale anche il ruolo di un'informazione tempestiva e qualificata. Diversi osservatori suggeriscono di istituire task force elettorali composte da esperti di comunicazione, fact-checker e tecnologi, pronte a reagire rapidamente durante la campagna elettorale per smentire ufficialmente eventuali deepfake virali prima che producano effetti irreversibili sulle opinioni degli elettori. In prospettiva, l'avvento dell'IA generativa impone alle democrazie una presa di coscienza: entrare nell'era in cui "vedere non è più credere" e in cui la fiducia nelle fonti informative deve basarsi su nuove forme di garanzia. La collaborazione internazionale sarà determinante, poiché i deepfake non conoscono confini nazionali. Organismi sovranazionali come la NATO e l'Unione Europea stanno studiando contromisure comuni, riconoscendo i *deepfake* come potenziali armi di disinformazione di massa nell'arsenale della guerra ibrida[10]. Complessivamente, l'uso di IA generativa per creare falsi politici è destinato a crescere ed evolvere, ma anche la consapevolezza pubblica e le difese normative-tecnologiche si stanno rafforzando. La sfida per il prossimo futuro sarà mantenere un dibattito democratico autentico, evitando che l'"inquinamento informativo" da deepfake eroda ulteriormente la fiducia dei cittadini nelle istituzioni e nei media in un circolo vizioso di cinismo e disillusione.

10 European Partnership for Democracy & Election-Watch.EU, *The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach*, 2024; studi parlamentari europei sulla resilienza democratica. I documenti trattano deepfake e manipolazione informativa come rischi sistemici e propongono misure di governance e tutela dei diritti.

8.5 Sovranità digitale e guerre ibride

Nell'odierno contesto geopolitico, segnato da tensioni internazionali e conflitti non convenzionali, il concetto di sovranità digitale è emerso come elemento chiave per la protezione dei processi elettorali nelle cosiddette *guerre ibride*. Con questa espressione ci si riferisce a strategie ostili che combinano strumenti convenzionali e non convenzionali, includendo attacchi cibernetici, disinformazione online, coercizione economica e altre tattiche volte a destabilizzare dall'interno le democrazie rivali senza ricorrere a un'invasione militare palese, fisica. Le elezioni rappresentano un obiettivo privilegiato di tali strategie, in quanto momento culminante della vita democratica: interferire in un'elezione significa minare la coesione nazionale e la legittimità del governo che ne risulterà. Negli ultimi anni numerosi rapporti di intelligence e indagini indipendenti hanno documentato operazioni di interferenza elettorale condotte da potenze straniere tramite strumenti digitali. Questi vanno dal semplice hackeraggio di sistemi di voto o registri elettronici, alla manipolazione dei flussi informativi sui social media per influenzare l'orientamento degli elettori, sino all'uso di IA per creare contenuti polarizzanti o fomentare divisioni sociali preesistenti.

In tale scenario, per sovranità digitale s' intende la capacità di uno Stato di controllare e proteggere le proprie infrastrutture informatiche, i propri dati e il proprio ecosistema digitale da interferenze esterne, garantendo che le decisioni critiche – come appunto le elezioni – non siano vulnerabili a ingerenze o condizionamenti altrui. Sul piano elettorale, ciò implica diverse azioni. Anzitutto, assicurarsi che le piattaforme tecnologiche utilizzate nel processo di voto (dalle macchine per il voto elettronico ai server che raccolgono i risultati, fino ai social network dove si svolge la campagna) siano soggette alla giurisdizione nazionale o comunque rispettino le regole locali. Un tema dibattuto è la dipendenza da fornitori stranieri: se un paese affida a una società estera la fornitura del sistema di e-voting o la gestione in cloud dei dati elettorali, la sua sovranità potrebbe essere a rischio, soprattutto se il paese di origine di tale società ha interessi ostili o potrebbe esercitare pressioni. Autonomia tecnologica significa quindi investire in soluzioni nazionali o quantomeno avere accesso al codice sorgente e pieno controllo operativo sui sistemi critici. L'Unione Europea, nell'ambito della sua agenda di sovranità digitale, incoraggia gli Stati membri a ridurre la dipendenza da tecnologie extra-UE, promuovendo ad esempio iniziative di cloud europeo per dati sensibili e standard aperti per il software elettorale[11]. Alcuni governi hanno già iniziato a scrutinare attentamente l'origine delle componenti digitali: ad esempio, diversi paesi hanno escluso fornitori cinesi o russi dalla realizzazione di infrastrutture chiave (come le reti 5G) temendo possibili

11 Letteratura recente su sovranità digitale e resilienza democratica in UE evidenzia il nesso tra controllo delle infrastrutture critiche, governance delle piattaforme e protezione dei processi elettorali da interferenze esterne e disinformazione.

backdoor e usi malevoli. Analogamente, software e hardware impiegati nelle elezioni dovrebbero essere certificati per la sicurezza e preferibilmente prodotti in contesti fidati.

Un secondo pilastro della sovranità digitale in chiave elettorale è il controllo dei dati. I dati degli elettori (liste elettorali, dati personali, registri dei votanti ecc.) rappresentano un asset strategico: se trafugati o alterati, possono consentire furti d'identità, coercizioni (si pensi alla divulgazione di preferenze politiche) o delegittimazione del voto. Garantire la sovranità significa custodire questi dati all'interno di infrastrutture nazionali sicure, soggette alle leggi locali sulla protezione dati, e impedire accessi non autorizzati da parte di soggetti esterni. Nei contesti di guerra ibrida, attacchi cibernetici mirati agli archivi elettorali sono stati documentati come tentativi di compromettere l'esito del voto o almeno di diffondere il dubbio sulla sua validità. Ad esempio, durante il conflitto in Ucraina iniziato nel 2022, le autorità europee hanno segnalato un aumento di attacchi hacker a enti pubblici, incluse commissioni elettorali, attribuiti a gruppi sponsorizzati dalla Russia, nel tentativo di destabilizzare i paesi che supportavano Kiev. La risposta sta in solide misure di cybersecurity elettorale: crittografia avanzata, sistemi di backup isolati, piani di emergenza per passare a modalità analogiche di voto se necessario, cooperazione con team di cyberdifesa (talora militari) per presidiare gli eventi elettorali come veri e propri "obiettivi sensibili" della sicurezza nazionale. Inoltre, per fronteggiare campagne di disinformazione orchestrate da attori esterni, la sovranità digitale richiede anche resilienza informativa: ciò comprende la già citata alfabetizzazione mediatica dei cittadini, ma anche meccanismi di risposta rapida da parte delle istituzioni (debunking di notizie false, comunicazioni ufficiali tempestive per smentire rumors sul corretto svolgimento del voto). In questo contesto, concetti come la *democratic sovereignty* o *electoral sovereignty* evocati da alcuni analisti indicano proprio la necessità di recuperare la capacità, da parte delle democrazie, di difendere autonomamente il proprio spazio informativo e decisionale. Non a caso si parla di "riconquistare la sovranità democratica": dopo anni in cui le società aperte hanno subito campagne di influenza segrete, vi è consenso sul fatto che la risposta non possa essere meramente reattiva. Serve un approccio sistemico e proattivo, che unisca governi, settore privato tecnologico e società civile per mettere in sicurezza l'ecosistema digitale prima che le minacce prendano forma.

Nel contesto europeo, gli sforzi per la sovranità digitale si sono tradotti in vari atti legislativi come il Digital Services Act (DSA) e il Digital Markets Act (DMA), entrati in vigore nel 2022-23, che impongono regole più stringenti alle grandi piattaforme online (spesso non europee) in termini di moderazione dei contenuti, trasparenza degli algoritmi e responsabilità verso le autorità nazionali. Anche la futura European Media Freedom Act e lo stesso AI Act rientrano in una strategia per garantire che la UE e i suoi Stati membri possano fissare standard propri anziché subire passivamente le dinamiche tecnologiche globali.

Si tratta in definitiva di affermare un principio: così come uno Stato sovrano difende i propri confini territoriali, oggi deve difendere i propri "confini digitali", specialmente durante le consultazioni elettorali, momento in cui è più esposto a interferenze. Naturalmente, questa difesa non può tradursi in isolazionismo tecnologico o censura di Stato. La sfida è piuttosto creare un ecosistema digitale sicuro ma aperto, in cui le informazioni circolino liberamente ma senza lasciare spazio ad intrusioni illecite. Ciò comporta anche una riflessione etica: fino a che punto le democrazie liberali possono spingersi per controllare l'ambiente digitale in nome della sicurezza? Alcune misure, come il blocco totale dei social network durante periodi elettorali turbolenti (attuato ad esempio in paesi extraeuropei), sarebbero impensabili in una democrazia matura poiché comprimono i diritti civili. La sovranità digitale in ambito elettorale deve allora fondarsi su legalità e proporzionalità: ad esempio, oscurare account specificamente legati a operazioni di propaganda straniera può essere giustificato se provato che quelli agiscono su mandato di governi ostili, ma un oscuramento massivo di Internet sarebbe contrario ai nostri princìpi. In conclusione, la protezione delle elezioni nelle guerre ibride richiede Stati tecnologicamente sovrani e che lo siano realmente, capaci di decidere con chi e come innovare (strategicità delle partnership tecnologiche), e al contempo resilienti rispetto a minacce transnazionali. L'IA è al centro di questo equilibrio: può essere un'arma nelle mani degli aggressori, ma anche uno scudo se usata per difendere i sistemi (come nell'identificazione di attacchi informatici in tempo reale). L'Europa e altri attori democratici dovranno continuare su questa strada, affermando nei fatti che la sovranità digitale è parte integrante della sovranità popolare nell'era digitale.

8.6 Diritto computazionale elettorale

L'ultimo aspetto innovativo da considerare riguarda la convergenza tra diritto elettorale e informatica, che potremmo definire diritto computazionale elettorale. Con questa espressione si intende l'insieme di metodologie e strumenti che consentono di tradurre norme e procedure elettorali in linguaggio formale o algoritmico, così da poterle implementare e verificare in sistemi digitali. L'avvento del voto elettronico e di sistemi software per la gestione dei complessi calcoli elettorali (dai quorum alle ripartizioni proporzionali dei seggi) ha infatti evidenziato come le tradizionali norme scritte talora non bastino a garantire un'interpretazione univoca e corretta: occorre che la legge "dialoghi" con la macchina. Un caso emblematico è quello della legislazione elettorale italiana sui sistemi proporzionali di allocazione dei seggi, che prevede calcoli su più livelli territoriali e una combinazione di metodo dei quozienti e dei resti. Studi recenti hanno mostrato che il testo normativo lasciava margini di ambiguità su *quale algoritmo specifico* adottare per effettuare certe ripartizioni, al punto che diverse implementazioni informatiche (tutte formalmente compatibili col testo di

legge) potevano condurre a risultati divergenti in termini di seggi assegnati. Solo un'analisi algoritmica dettagliata ha permesso di individuare queste ambiguità normative e proporre una formulazione più chiara, evitando esiti indesiderati come possibili indeterminazioni del risultato elettorale[12]. Questo esempio evidenzia l'importanza del diritto computazionale: formalizzare le regole elettorali in modo preciso (tramite formule matematiche, diagrammi di flusso o codice) può rivelare incoerenze o lacune del linguaggio naturale, consentendo al legislatore di correggerle prima che si manifestino nelle urne.

Il diritto computazionale elettorale si muove su due binari complementari. Da un lato, mira a rendere le leggi *machine-readable,* ossia direttamente utilizzabili dai sistemi di e-voting o di scrutinio elettronico. Ciò implica sviluppare standard e linguaggi ad hoc per codificare procedure come la registrazione di un elettore, la votazione, il conteggio e l'assegnazione dei seggi. Idealmente, la norma giuridica potrebbe un giorno essere affiancata dal suo *algoritmo ufficiale* di riferimento: per esempio, un'appendice normativa potrebbe contenere lo pseudo-codice certificato del metodo di calcolo dei seggi, scritto e approvato dal legislatore stesso, eliminando così ogni incertezza interpretativa. Si tratterebbe di un cambio di paradigma nel modo di scrivere le leggi, che alcuni autori intravedono già come possibile evoluzione nel campo del *computational law*[13]. Dall'altro lato, il diritto computazionale applicato alle elezioni fornisce strumenti per la verifica e il rispetto della legalità nei sistemi elettronici. Un sistema di voto digitale non è altro che un insieme di regole codificate in software, risulta quindi fondamentale assicurarsi che tali regole rispettino in toto la legge elettorale vigente. A tal fine, tecniche di verifica formale e testing possono essere impiegate per provare che, ad esempio, un programma di scrutinio preserva sempre il principio "una testa, un voto", che non permette mai di risalire dall'esito al singolo votante (rispettando la segretezza) e che assegna i seggi con esattezza matematica secondo la formula stabilita. In alcuni paesi, come la Norvegia e la Svizzera durante le sperimentazioni di e-voting, sono stati utilizzati metodi crittografici avanzati (prove a conoscenza zero, protocolli di *end-to-end verifiability*) per dare garanzia sia agli elettori sia agli osservatori che ogni voto elettronico fosse contato senza alterazioni e che eventuali brogli fossero rilevabili[14]. Qui il diritto computazionale sconfina nella cybersecurity legale: le regole tecniche di sicurezza (cifratura, firme digitali, audit trail) diventano di fatto estensioni delle norme giuridiche

12 Crafa, S., "Algorithmic Thinking for the Legal Writing: The Case of Italian Election Law", *Digital Society*, 2024. Il contributo mostra come la formalizzazione algoritmica delle procedure elettorali evidenzi ambiguità normative e migliori controllabilità, trasparenza e certezza del risultato.

13 Ibidem, p. 119

14 Documentazione accademica e istituzionale sulle sperimentazioni di e-voting in Norvegia e Svizzera descrive l'uso di schemi crittografici avanzati e di verificabilità end-to-end come garanzie tecniche di integrità e auditabilità del voto elettronico, a condizione di audit indipendenti e controllo umano continuo.

sulla validità del voto. È compito del legislatore e delle autorità di regolamentazione definire standard tecnologici minimi che i sistemi di voto elettronico debbono possedere (ad esempio requisiti di disponibilità offline, di interoperabilità, di accessibilità per disabili), così che il software incaricato di gestire l'elezione sia costruito *by design* per rispettare diritti e princìpi.

Un altro ambito emergente è l'uso dell'IA stessa per *supportare* il diritto elettorale: ad esempio, gli algoritmi potrebbero analizzare precedenti sentenze o reclami elettorali per identificare schemi e suggerire modifiche normative atte a prevenire contenziosi. In USA alcune contee hanno sperimentato sistemi esperti per il *redistricting* (ridisegno dei collegi elettorali) volti a minimizzare il gerrymandering[15], seguendo criteri di neutralità impartiti dalla legge. Se questi algoritmi fossero riconosciuti come affidabili, potrebbero essere integrati nelle procedure ufficiali, con lo statuto quasi di "ausiliari digitali" del giudice o dell'amministratore elettorale. Ciò però solleva interrogativi: fino a che punto possiamo delegare a un'IA decisioni che hanno natura giuridica e politica (come la conformità di una circoscrizione ai requisiti di equa rappresentanza)? Il diritto computazionale dovrà tracciare confini netti, prevedendo sempre una supervisione umana e meccanismi di appello contro decisioni automatizzate.

Infine, va menzionato come il diritto computazionale elettorale possa contribuire alla trasparenza e comprensibilità delle regole del gioco democratico. Rappresentare visivamente o algoritmicamente un complesso sistema elettorale può aiutare cittadini e media a comprenderne il funzionamento. Alcuni paesi hanno iniziato a pubblicare simulazioni online che mostrano, ad esempio, come i voti si traducano in seggi col proprio sistema proporzionale, passo dopo passo. Questo approccio *didattico* è stato auspicato anche per l'Italia, dove la notevole complicazione delle leggi elettorali degli ultimi anni ha creato disorientamento nell'elettorato: si potrebbe affiancare al testo di legge una sorta di "calcolatore ufficiale" che, inserendo voti ipotetici, restituisca la distribuzione dei seggi secondo la formula prevista, in modo neutrale e pubblico. Si realizzerebbe così il principio per cui la conoscibilità delle regole è parte della sovranità popolare: l'elettore capirebbe meglio come il suo voto concorre al risultato finale.

15 Con il termine *gerrymandering* si indica la pratica di manipolare i confini delle circoscrizioni elettorali al fine di favorire sistematicamente un partito politico, un gruppo o un interesse specifico, alterando la rappresentatività del voto pur nel rispetto formale delle procedure elettorali. Il fenomeno si realizza tipicamente attraverso tecniche di *packing* (concentrazione degli elettori avversi in poche circoscrizioni) e *cracking* (dispersione degli elettori avversi in molte circoscrizioni), con l'effetto di distorcere la proporzionalità tra voti ottenuti e seggi assegnati. In ambito giuridico e comparato, il *gerrymandering* è considerato una violazione del principio di equa rappresentanza e dell'uguaglianza del voto, poiché consente di influenzare l'esito elettorale non attraverso il consenso, ma mediante il disegno strategico delle regole territoriali del voto. Nel contesto dell'uso di sistemi esperti e algoritmi per il *redistricting*, il riferimento al *gerrymandering* evidenzia l'obiettivo di ridurre discrezionalità politica e arbitrarietà, pur sollevando interrogativi sulla legittimità democratica e sul controllo giurisdizionale delle decisioni automatizzate.

In conclusione, il diritto computazionale elettorale rappresenta un campo di frontiera in cui giuristi e informatici collaborano per garantire che la "traduzione" digitale della democrazia sia fedele ai suoi princìpi di base. In un futuro di elezioni sempre più digitalizzate, solo formalizzando accuratamente le norme e verificandone la corretta implementazione nelle macchine si potrà evitare che scarti interpretativi o bug informatici compromettano il volere degli elettori. L'auspicio è che vengano sviluppati standard internazionali condivisi (ad esempio sotto l'egida di enti come l'IEEE o lo stesso Consiglio d'Europa) per il coding delle procedure elettorali, assicurando interoperabilità, sicurezza e rispetto delle tradizioni costituzionali di ciascun paese. Il diritto elettorale, lungi dall'essere statico, dovrà così evolvere abbracciando il paradigma computazionale, per continuare a svolgere la sua funzione garantista nell'era dell'IA e dell'automazione.

8.7 Sintesi conclusiva

Le analisi svolte in questo capitolo hanno evidenziato come l'impatto dell'intelligenza artificiale sul voto elettronico durante crisi globali ponga sfide complesse ma non insormontabili, a patto di affrontarle con un approccio multidisciplinare e proattivo. Dal punto di vista legale, è emersa l'urgenza di aggiornare i quadri normativi introducendo regole specifiche per l'IA in ambito elettorale: ciò include sia misure di contrasto agli abusi (come il divieto di deepfake e la trasparenza sul microtargeting politico) sia requisiti positivi per chi adotta tali tecnologie (trasparenza, controlli indipendenti, rispetto dei principi elettorali fondamentali). Molte democrazie occidentali hanno già avviato questo percorso normativo, come attestano il nuovo Regolamento UE sui messaggi politici online e le leggi anti-deepfake approvate in numerosi Stati, ma il diritto dovrà continuare a evolvere al passo con l'innovazione, mantenendo al centro la tutela della sovranità popolare. Sul versante etico, l'IA impone di ribadire con forza i valori di equità, trasparenza e responsabilità: gli algoritmi devono servire l'interesse pubblico senza introdurre discriminazioni o opacità incompatibili con la fiducia democratica. La gestione etica comprende tanto la progettazione *a monte* di sistemi elettorali tecnologici inclusivi e spiegabili, quanto la formazione *a valle* di cittadini ed operatori, affinché sviluppino la consapevolezza critica necessaria nell'ecosistema informativo attuale. I fenomeni esaminati, dalla minaccia dei deepfake politici alla necessità di garantire la sovranità digitale contro interferenze ibride, fino alla formalizzazione computazionale delle norme, delineano un orizzonte elettorale in rapido mutamento, dove rischi ed opportunità coesistono. Da un lato, attacchi cibernetici, disinformazione automatizzata e manipolazioni algoritmiche rappresentano pericoli concreti per l'integrità elettorale e richiedono robuste contromisure tecniche, legali e diplomatiche. Dall'altro, le stesse tecnologie IA possono essere sfruttate positivamente: ad esempio per

migliorare l'accessibilità al voto (con interfacce intelligenti per disabili), ottimizzare la gestione logistica delle elezioni, o potenziare gli strumenti di monitoraggio delle irregolarità (rilevando schemi anomali nei dati di affluenza o scrutinio).

In definitiva, la resilienza dei processi democratici in tempi di pandemia, guerra o crisi climatica dipenderà dalla capacità delle istituzioni di governare l'innovazione: non subirla passivamente, né demonizzarla, ma integrarla in modo sicuro e rispettoso dei diritti. Come sottolineato in sede europea, anche durante emergenze straordinarie rimane inderogabile il dovere di garantire elezioni "in conformità con i princìpi cardinali dell'eredità elettorale europea, ossia suffragio universale, libero, eguale, segreto e diretto"[16]. L'IA dovrà dunque essere imbrigliata entro schemi che ne esaltino i vantaggi (efficienza, rapidità di elaborazione, analisi predittiva) senza permettere che ne sovverta i presupposti democratici (libertà di scelta, correttezza, trasparenza). Fondamentale sarà lo scambio di *best practice* a livello internazionale: forum come il Consiglio d'Europa, l'OSCE e organizzazioni specializzate (IDEA, IFES) stanno facilitando la condivisione di esperienze e linee guida tra paesi, affinché nessuno resti indietro nell'affrontare la sfida dell'IA applicata alle elezioni. In parallelo, il coinvolgimento degli stakeholder (partiti, media, aziende tech, accademia e società civile) costituirà un pilastro per soluzioni efficaci e legittimate. Un esempio virtuoso è rappresentato dagli accordi volontari con le grandi piattaforme digitali per contrastare la disinformazione algoritmica durante le campagne: tali codici di condotta, sebbene non vincolanti, indicano la strada verso una corresponsabilità di tutti gli attori nella salvaguardia dell'integrità elettorale.

Per concludere, l'impatto dell'IA sul voto elettronico in situazioni di crisi globale può essere governato con successo solo adottando un approccio olistico che combini rigore normativo, riflessione etica, innovazione tecnica e cooperazione istituzionale. La storia insegna che la democrazia ha saputo adattarsi a grandi mutamenti sociali, economici, tecnologici traendone nuovo vigore. All'alba dell'era digitale avanzata plasmata dall'intelligenza artificiale, le democrazie sono chiamate ancora una volta ad adattarsi e innovarsi: l'IA potrà divenire un alleato potente per sistemi elettorali più resilienti e inclusivi, purché sia disciplinata e incanalata da solide strutture di diritto e di principio. In questo equilibrio dinamico tra tecnologia e valori risiede la sfida, ma anche la promessa, della governance elettorale del XXI secolo.

16 L'espressione richiama i princìpi fondamentali dell'eredità elettorale europea come codificati dalla Commissione europea per la democrazia attraverso il diritto (Commissione di Venezia) nel *Code of Good Practice in Electoral Matters*, adottato dal Consiglio d'Europa nel 2002 e successivamente ribadito in numerosi pareri e documenti interpretativi. Il Codice individua cinque principi cardine inderogabili delle elezioni democratiche: suffragio universale, libero, eguale, segreto e diretto, affermando che essi devono essere garantiti anche in contesti eccezionali o di crisi, e che ogni innovazione procedurale o tecnologica – incluso il voto elettronico – deve essere valutata alla luce della loro piena salvaguardia. Tali principi costituiscono lo standard di riferimento europeo per la legittimità dei processi elettorali e vincolano l'azione normativa e amministrativa degli Stati membri del Consiglio d'Europa.

PARTE V
SCENARI DI CRISI GLOBALI E IMPATTI DELL'I.A. SUL VOTO ELETTRONICO

Capitolo 9
Intelligenza artificiale, pandemie e voto elettronico

La pandemia di COVID-19 ha imposto sfide senza precedenti allo svolgimento delle elezioni, obbligando molti paesi ad adottare con urgenza strumenti di voto elettronico e altre soluzioni tecnologiche per garantire la continuità dei processi elettorali durante lockdown e restrizioni sanitarie.

Fin dalle prime fasi dell'emergenza, organizzazioni internazionali come il Consiglio d'Europa hanno sottolineato che, anche in situazioni di crisi, devono essere rispettati i principi fondamentali di elezioni libere ed eque sanciti dal diritto internazionale (ad esempio l'art. 3 del Protocollo I della CEDU). Di conseguenza, ogni sperimentazione di voto online o remoto in pandemia ha richiesto misure atte a salvaguardare i diritti democratici di uguaglianza, segretezza e libertà del voto, evitando coercizioni e garantendo che ogni voto avesse lo stesso peso. Tali preoccupazioni sono state ribadite in un rapporto dell'Assemblea Parlamentare del Consiglio d'Europa, che ha evidenziato le opportunità ma anche i rischi delle elezioni in tempi di crisi, indicando come le norme eccezionali non possano derogare ai principi cardine della democrazia[1]. In parallelo, si è assistito a una rapida evoluzione dei quadri normativi: governi e parlamenti hanno dovuto bilanciare l'urgenza di assicurare il voto con soluzioni tecnologiche innovative – incluse quelle basate sull'I.A. per la gestione elettorale – con la tutela dei diritti elettorali e della privacy degli elettori.

Durante il biennio 2020-2021, oltre 80 paesi in tutto il mondo hanno deciso di posporre elezioni nazionali o subnazionali a causa dell'emergenza pandemica, mentre almeno 160 paesi hanno comunque tenuto votazioni nonostante le preoccupazioni sanitarie[2]. Molte democrazie hanno optato per rinvii di consultazioni, ad esempio posticipando referendum ed elezioni locali, ritenendo impossibile garantire un voto in presenza in sicurezza nei momenti più acuti dei

1 McGee, D., & Santolaya, P. (2021). *Elections in times of crisis: challenges and opportunities*. Assemblea Parlamentare del Consiglio d'Europa. Gli autori analizzano l'impatto delle emergenze globali sui processi elettorali, ribadendo che anche in situazioni straordinarie gli Stati restano vincolati al rispetto dei principi fondamentali delle elezioni libere ed eque, sanciti dal diritto internazionale dei diritti umani, e che le misure eccezionali non possono incidere sul nucleo essenziale del diritto di voto.

2 Garnett, H. A., James, T. S., & Plesner, J. (2020–2022). *Elections, COVID-19 and emergency preparedness*. International IDEA. Le ricerche comparative documentano come, durante la pandemia, oltre ottanta paesi abbiano rinviato consultazioni elettorali mentre molti altri abbiano introdotto adattamenti procedurali (voto anticipato, voto postale, misure sanitarie rafforzate), offrendo una mappatura globale delle risposte istituzionali alla crisi.

contagi[3]. In altri casi si è preferito procedere con le elezioni previste introducendo rigidi protocolli sanitari e strumenti alternativi di voto.

Un caso emblematico è quello della Corea del Sud, che il 15 aprile 2020 è divenuto il primo paese ad organizzare elezioni nazionali in piena pandemia. Le autorità sudcoreane hanno allestito circa 14.000 seggi con misure straordinarie: sanificazioni frequenti, obbligo per gli elettori di indossare mascherine e guanti monouso, controllo della temperatura all'ingresso e cabine separate per votanti con sintomi[4]. Nonostante i timori iniziali di bassa affluenza, l'affluenza finale ha raggiunto il 61,2%, la più alta per le elezioni legislative sudcoreane dal 1996, segnando un successo attribuito all'efficace gestione sanitaria e alla fiducia dei cittadini[5].

Anche in altri contesti si sono sperimentate soluzioni per consentire il voto in sicurezza: in vari Stati degli USA le elezioni si sono svolte estendendo massicciamente il voto per corrispondenza per ridurre gli assembramenti ai seggi, mentre in Europa si è fatto maggiore ricorso al voto anticipato e al voto domiciliare per elettori fragili.

Gli studi giuridici comparati condotti nel 2020 evidenziano inoltre come la pandemia abbia prodotto risposte differenti nei vari ordinamenti. La Polonia tentò di organizzare un'elezione presidenziale completamente postale nel maggio 2020, salvo poi annullarla all'ultimo minuto per difficoltà logistiche e controversie politiche; la Francia svolse il primo turno delle elezioni comunali a marzo 2020 con bassa affluenza, rinviando il secondo turno di alcuni mesi; in Italia vari appuntamenti elettorali furono accorpati o posticipati per decreto, incluso il referendum costituzionale sul taglio dei parlamentari, poi celebrato in settembre 2020 anziché a marzo. Tali esperienze hanno messo in luce l'importanza di predisporre in anticipo basi normative flessibili per affrontare emergenze sanitarie, ad esempio prevedendo nel diritto interno clausole per il rinvio del voto in caso di calamità o per l'ampliamento delle modalità di voto (posta, delega, voto elettronico) in situazioni eccezionali.

---

3 Spano, G. (2020); Faraguna, P. (2021). Studi di diritto costituzionale comparato sull'impatto della pandemia da COVID-19 sulle elezioni in Europa. Le analisi evidenziano come gli ordinamenti abbiano adottato soluzioni eterogenee – rinvii, accorpamenti, modifiche temporanee delle modalità di voto – e sottolineano l'importanza di predisporre in via preventiva clausole normative di emergenza per salvaguardare certezza del diritto e legittimità democratica.

4 Kim, Y., & Kim, S. (2020). "Elections during a pandemic: South Korea's legislative elections of April 2020". *Asian Journal of Comparative Politics*. Il caso sudcoreano viene descritto come un esempio emblematico di gestione elettorale in emergenza sanitaria, basata su rigorose misure di sicurezza ai seggi e su un'organizzazione amministrativa efficiente, senza ricorso generalizzato al voto elettronico remoto.

5 Moon, C., & Park, C. (2021). "Voter turnout and trust during COVID-19: Evidence from South Korea". *Electoral Studies*. Gli autori mostrano come l'elevata affluenza alle elezioni legislative del 2020 sia stata favorita dalla fiducia dei cittadini nelle istituzioni e nelle misure sanitarie adottate, confermando che la percezione di sicurezza e legittimità è un fattore chiave della partecipazione elettorale in tempi di crisi.

Dal punto di vista tecnologico, la pandemia ha accelerato la sperimentazione di sistemi di voto elettronico e soluzioni digitali innovative, anche basate su IA, per facilitare la partecipazione elettorale a distanza. Ad esempio, in alcuni contesti sono stati studiati sistemi di identificazione degli elettori mediante riconoscimento facciale o altre tecniche *AI-driven* per evitare contatti fisici, suscitando però interrogativi in tema di privacy e sicurezza. In generale, l'adozione affrettata di nuove tecnologie durante l'emergenza ha riproposto il dilemma tra innovazione e affidabilità: da un lato l'IA e i sistemi digitali possono aiutare a gestire grandi moli di dati sanitari e logistici (ad esempio per monitorare l'affluenza in tempo reale o ottimizzare la distribuzione dei seggi), dall'altro la fretta nell'implementazione senza adeguati collaudi può esporre a malfunzionamenti e vulnerabilità informatiche. I legislatori si sono trovati quindi a dover aggiornare le normative elettorali per regolare questi nuovi strumenti. Particolare attenzione è stata dedicata alla protezione dei dati personali dei votanti: l'uso di applicazioni di tracciamento dei contatti o di certificazioni verdi (green pass) integrato nei processi di voto ha richiesto rigidi protocolli di conformità al GDPR in Europa e alle leggi privacy negli altri paesi. Permane il rischio che l'impiego massivo di dati sanitari o di profilazione algoritmica degli elettori – ad esempio per scaglionare gli accessi ai seggi o inviare comunicazioni personalizzate relative al voto – possa confliggere con i principi di minimizzazione e finalità dei dati.

Alcune analisi hanno segnalato possibili abusi, come l'uso di strumenti di micro-targeting politico durante la pandemia, facilitato dall'aumento della dipendenza dai social media in isolamento: ciò potrebbe aver esposto fasce di elettorato a messaggi disinformativi generati da bot o da algoritmi di IA, richiedendo interventi normativi per garantire trasparenza e correttezza dell'informazione elettorale[6].

In sintesi, l'esperienza pandemica ha rappresentato un banco di prova cruciale per i sistemi di voto elettronico e l'impiego dell'IA nelle elezioni. Da essa sono emersi insegnamenti importanti: la necessità di predisporre per tempo protocolli di emergenza e infrastrutture tecniche resilienti; l'urgenza di aggiornare il quadro legale per prevedere modalità di voto alternative rispettose dei principi democratici; l'importanza di valutare con rigore l'impatto delle tecnologie – soprattutto quelle di IA – sui diritti degli elettori, bilanciando innovazione e tutela. Organizzazioni come International IDEA hanno raccolto in un volume del 2023 ben 26 casi di studio da tutto il mondo per trarre lezioni sul

6 Woolley, S. C., & Howard, P. N. (2020). *Computational Propaganda, Political Communication, and COVID-19*. Oxford University Press; Persily, N., & Tucker, J. A. (2021). Studi sulla disinformazione durante la pandemia evidenziano come l'isolamento sociale e l'intensificazione dell'uso delle piattaforme digitali abbiano favorito pratiche di micro-targeting politico e la diffusione di contenuti automatizzati, talvolta generati o amplificati tramite sistemi di intelligenza artificiale, con potenziali effetti distorsivi sul dibattito elettorale.

mantenimento dell'integrità elettorale durante la pandemia[7], formulando una serie di raccomandazioni su come rendere i processi di voto più sicuri e inclusivi in future situazioni di emergenza sanitaria[8].

Il ricorso all'IA, dunque, se opportunamente regolato, potrà contribuire a migliorare la gestione elettorale (ad esempio con sistemi di supporto decisionale per gli enti elettorali in situazioni critiche), ma solo a condizione di non sacrificare i principi di trasparenza, responsabilità e rispetto della volontà popolare che costituiscono il fondamento di ogni democrazia anche nei momenti di maggior crisi come l'esperienza dell'emergenza sanitaria del 2020 ci ha insegnato.

7 Garnett, H. A., James, T. S., & Plesner, J. (eds.) (2023). *Elections and COVID-19: Building Resilience in Electoral Processes*. International IDEA. Il volume raccoglie 26 casi di studio internazionali e formula raccomandazioni operative per rafforzare la resilienza dei processi elettorali in future emergenze sanitarie, sottolineando il ruolo potenziale delle tecnologie digitali e dell'IA come strumenti di supporto, a condizione che siano adottati nel rispetto dei principi democratici e dei diritti fondamentali.

8 Ibidem.

Capitolo 10
Contesti di guerra e voto elettronico

10.1 Introduzione

Le consultazioni elettorali in contesti di conflitto armato presentano sfide senza precedenti per la salvaguardia della democrazia. Crisi come guerre ed emergenze hanno imposto pressioni drammatiche sui processi elettorali, rendendo arduo garantire elezioni libere e regolari secondo gli standard internazionali. In particolare, il ritorno di una guerra su larga scala in Europa ha sollevato nuovi rischi: le tecnologie digitali avanzate – dall'intelligenza artificiale alle cyber-armi – espandono il perimetro di possibili manipolazioni, disinformazione e attacchi cibernetici legati alle elezioni.

Organismi internazionali sottolineano come le elezioni non sono minacciate solo dalla guerra "fisica" sul campo, ma anche da *guerre ibride* condotte sul piano informativo e cibernetico. Questo capitolo esamina dunque l'impatto dell'IA nei contesti bellici in relazione al voto elettronico, attraverso casi di studio recenti (Ucraina, Lituania, Israele) e analisi dei fenomeni di disinformazione automatizzata, attacchi cyber-elettorali e strumenti forensi impiegati in zone di conflitto. Vengono inoltre discussi gli aggiornamenti giuridici sino al momento in cui si termina il presente volume, ovvero luglio 2025 – dal nuovo diritto europeo sulla cibersicurezza (direttiva NIS2) alla cooperazione internazionale (Convenzione di Budapest) sino alle norme di diritto internazionale umanitario – per inquadrare le responsabilità e le contromisure legali di fronte a queste sfide emergenti. L'obiettivo è fornire una visione organica e aggiornata di come l'IA, quando impiegata in scenari bellici, possa influire sull'integrità dei processi elettorali e quali risposte normative e tecnologiche risultino necessarie per tutelare il principio di elezioni libere e regolari anche nelle circostanze più avverse.

10.2 IA e guerra ibrida: interferenze elettorali come arma di conflitto

Nel moderno paradigma della *guerra ibrida*, strumenti cibernetici e informativi vengono integrati con le tattiche militari convenzionali per colpire le istituzioni democratiche del nemico. In particolare, l'integrità dei processi elettorali è divenuta un bersaglio esplicito di operazioni ostili condotte da attori statali e non-statali durante i conflitti. Studi recenti evidenziano che la guerra ibrida *"ora*

prende di mira di routine l'integrità elettorale"[1], combinando operazioni psicologiche, cyber-attacchi e campagne di disinformazione alimentate dall'IA. Democrazie un tempo considerate resilienti si scoprono vulnerabili in uno scenario in cui si confondono i confini tra minacce esterne ed interne, tra dimensione digitale e fisica, e tra realtà e manipolazione[2]. Regimi autoritari come la Russia e l'Iran hanno affinato strategie sofisticate per interferire nelle elezioni altrui, impiegando *hacker* militari, propaganda online e contenuti sintetici generati dall'IA per destabilizzare i governi avversari. Tali operazioni perseguono finalità belliche mediante mezzi subdoli: ad esempio, simulando dissenso interno tramite reti di bot e propagandisti locali, gli aggressori possono polarizzare l'elettorato di un paese bersaglio e minarne la coesione dall'interno[3]. Un rapporto del 2023 ha rivelato come queste tattiche possano influenzare anche democrazie consolidate, esercitando pressioni persistenti e difficili da attribuire sugli iter elettorali. In sintesi, l'IA e le tecniche di *machine learning* amplificano l'efficacia della guerra informativa, consentendo operazioni di influenza su larga scala che un tempo richiedevano ingenti risorse umane. Nel contesto bellico attuale, l'interferenza elettorale orchestrata tramite strumenti digitali avanzati è diventata un vero e proprio "secondo fronte" di conflitto, mirato a conseguire obiettivi strategici (come l'erosione del sostegno popolare alla guerra o l'insediamento di governi più compiacenti) senza ricorrere esclusivamente alla forza militare.

---

1 Rodenas, I., *Election Interference in the Age of Hybrid Warfare*, Centre for Youth and International Studies (CYIS), luglio 2025. L'autore osserva che la guerra ibrida "ora prende di mira di routine l'integrità elettorale", descrivendo un continuum tra operazioni psicologiche, attività cyber e campagne di disinformazione che mirano a erodere fiducia e coesione democratica.

2 Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), *Countering hybrid threats to elections: From updating legislation to securing digital infrastructure*, Research Report, 2024; Consiglio dell'Unione europea, *Guiding framework and progress reporting on countering hybrid threats / Foreign Information Manipulation and Interference (FIMI)*, 2024. La letteratura e i documenti strategici europei inquadrano l'interferenza elettorale come obiettivo ricorrente delle minacce ibride, in cui campagne di influenza, cyber-operazioni e sfruttamento di vulnerabilità sociali e istituzionali mirano a degradare fiducia pubblica, coesione interna e legittimità democratica, spesso con tecniche di attribuzione complessa e "plausible deniability".

3 Woolley, S. C., & Howard, P. N. (eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford University Press, 2019; de Nadal, L., & Jančárik, P., "Beyond the deepfake hype: AI, democracy, and 'the Slovak case'", *Harvard Kennedy School Misinformation Review*, 2024. Le fonti descrivono come reti di account coordinati (bot e profili inautentici) e contenuti sintetici possano simulare consenso o dissenso "dal basso" (*astroturfing / coordinated inauthentic behavior*), amplificando polarizzazione e sfiducia; i casi recenti mostrano che l'impatto di singoli contenuti manipolati dipende fortemente dal contesto (bassa fiducia, frammentazione informativa, dinamiche di piattaforma), rendendo l'operazione di influenza un fenomeno socio-tecnico più che un semplice "falso" isolato.

Casi di studio: Europa orientale

La guerra russo-ucraina illustra in modo emblematico l'uso bellico dell'interferenza elettorale. Già nel 2014, durante il conflitto nel Donbass, la rete informatica della Commissione Elettorale ucraina subì un grave attacco informatico da parte di hacker filo-russi volto ad alterare i risultati ufficiali delle presidenziali. Il piano prevedeva di proclamare vincitore un candidato ultranazionalista estraneo alla volontà popolare, così da delegittimare il nuovo governo di Kiev. Il malware infiltrato nel sistema centrale di conteggio avrebbe visualizzato sul sito elettorale un dato falso, ovvero la vittoria del leader dell'estrema destra Dmytro Yarosh con il 37% dei voti, per poi essere rilanciato immediatamente dai media russi come "notizia" dell'esito del voto. In effetti, il primo canale televisivo di Mosca annunciò quella sera la clamorosa (e inesistente) vittoria di Yarosh, nell'evidente tentativo di seminare caos politico in Ucraina e confermare la narrativa propagandistica che descrive il governo post-rivoluzionario come preda dei "fascisti". Fortunatamente, i tecnici ucraini riuscirono a neutralizzare il virus pochi minuti prima della chiusura delle urne, impedendo la manipolazione dei dati reali. L'episodio, definito dagli esperti *"uno dei tentativi più audaci e su larga scala di manipolare un'elezione nazionale"*[4] fino ad allora, rientrava in una strategia più ampia di *guerra informativa* condotta dalla Russia parallelamente alla campagna militare sul terreno. Esso dimostra dunque come, in un contesto bellico, un attacco cibernetico ai sistemi elettorali possa divenire una vera "arma" per delegittimare le istituzioni nemiche e compromettere la fiducia dei cittadini nella democrazia. È significativo notare che, dal 2014 ad oggi, l'aggressione russa contro l'Ucraina ha incluso un ventaglio di operazioni cyber e di disinformazione sempre più sofisticate, volte sia a colpire infrastrutture civili critiche sia a influenzare l'opinione pubblica. Nel 2022, allo scoppio dell'invasione su vasta scala, le autorità ucraine hanno dovuto sospendere a tempo indeterminato lo svolgimento di elezioni sotto la legge marziale. Ciò ha prevenuto interferenze dirette nei processi di voto durante il conflitto in corso, ma non ha impedito alla macchina propagandistica russa di cercare altri bersagli: Mosca ha intensificato gli sforzi per condizionare le elezioni nei paesi occidentali alleati di Kiev, diffondendo narrazioni ostili e sfruttando strumenti di IA generativa per amplificare i messaggi sovversivi. Ad esempio, fonti di intelligence statunitensi hanno affermato che la Russia – insieme ad altri regimi autoritari – già utilizza sistemi di IA per provare a influenzare gli elettori americani in vista delle elezioni presidenziali del 2024, propagando disinformazione mirata sui social media. Allo stesso tempo, l'Ucraina stessa si è trovata costretta a sviluppare contromisure

4 Greenberg, A., *Hackers Tried to Rig Ukraine's Election*, Wired, 3 giugno 2014. L'autore, sulla base di fonti tecniche e governative ucraine, definisce l'attacco informatico alle elezioni presidenziali del 2014 come uno dei tentativi più audaci e sistemici di manipolazione di un'elezione nazionale mai osservati fino ad allora, inserendolo nel contesto più ampio delle operazioni di guerra informativa condotte dalla Russia.

basate su IA: funzionari di Kiev riferiscono di utilizzare algoritmi generativi per monitorare e contrastare in tempo reale le campagne di fake news orchestrate dal nemico. Ne emerge un quadro in cui l'IA è divenuta al contempo strumento di offesa e di difesa nell'arena dell'informazione bellica, mentre le elezioni, anche quando rimandate o svolte altrove, restano un campo di battaglia conteso tra narrative e attacchi invisibili.

Un altro esempio significativo proviene dalla regione baltica. La Lituania, pur non essendo direttamente coinvolta in un conflitto armato, si considera sulla linea del fronte della guerra ibrida russa a causa del suo fermo sostegno all'Ucraina. Nel 2023-2024 i servizi di sicurezza lituani hanno documentato un'intensa campagna del Cremlino volta a screditare il paese attraverso la manipolazione storica e le accuse propagandistiche (diffondendo un'immagine "russofoba" e "neo-nazista"). In parallelo a queste narrazioni ostili, Mosca ha potenziato l'uso di strumenti di IA generativa per creare contenuti falsi in lingua lituana destinati ai social media locali. Le autorità di Vilnius avvertono che *"gli strumenti di IA, inclusi i deepfake video, audio e immagini, consentono di generare contenuti ingannevoli in modo molto più veloce ed economico"*[5], aumentando l'efficacia e la portata della disinformazione.

Fino al 2024 l'impatto di tali contenuti sintetici è stato limitato, ma con il rapido avanzare della tecnologia si valuta che la disinformazione prodotta dall'IA diventerà *"altamente più efficace e dannosa"*[6] in breve tempo. Un episodio occorso nel maggio 2024 illustra bene la minaccia: su Telegram e siti filorussi circolò la notizia (completamente falsa) dell'arresto in Lituania di due attivisti anti-NATO, notizia accompagnata da immagini e video apparentemente credibili ma generati ad arte. La *fake news* fu poi rilanciata da portali russi e perfino su alcuni media lituani filo-moscoviti, prima di essere smentita dalle autorità. Episodi come questo, insieme all'uso crescente di *bot* e profili falsi per diffondere propaganda, confermano che la Lituania è oggetto di un'aggressione informativa continua. In vista delle proprie elezioni parlamentari, Vilnius ha quindi rafforzato le difese cibernetiche ed elevato l'allerta sulle interferenze straniere: i funzionari prevedono che la Russia potrebbe sfruttare l'IA sia per veicolare *fake news* polarizzanti nel dibattito elettorale, sia per attacchi hacker alle infrastrutture di voto elettronico, nell'eventualità (oggi remota) che tali sistemi vengano adottati.

---

5 State Security Department of the Republic of Lithuania (VSD), *National Threat Assessment 2024*, Vilnius, 2024. Il rapporto evidenzia come l'uso di strumenti di intelligenza artificiale generativa, inclusi deepfake audio, video e immagini, consenta agli attori ostili di produrre e diffondere contenuti ingannevoli in modo significativamente più rapido ed economico, aumentando l'efficacia delle campagne di disinformazione contro la Lituania.

6 European External Action Service (EEAS), *Foreign Information Manipulation and Interference (FIMI) Report 2024*, Bruxelles, 2024. Il rapporto valuta che la disinformazione potenziata dall'intelligenza artificiale è destinata a diventare altamente più efficace e dannosa nel breve periodo, in particolare nei confronti degli Stati membri dell'UE esposti a campagne di influenza ostile, come i Paesi baltici.

Casi di studio: il Medio Oriente

Fuori dal teatro europeo, anche il conflitto cronico arabo-israeliano offre esempi rilevanti di minacce IA alle dinamiche elettorali e all'opinione pubblica. Israele, circondato da ostilità e spesso coinvolto in operazioni militari, è al contempo uno dei paesi leader nelle tecnologie di IA e cyber-defense. Ciò non ha impedito che nel 2023-2025 il paese subisse campagne di disinformazione avanzate orchestrate dai suoi nemici regionali (in primis l'Iran) sfruttando contenuti creati artificialmente. Ad esempio, durante l'escalation militari del 2024, dopo scambi di attacchi tra Israele e Iran, sui social network sono comparsi video e immagini scioccanti, fra cui la foto di un bombardiere americano B-2 precipitato in Iran o anche un filmato sulle devastazioni a Tel Aviv: questi contenuti hanno rapidamente catturato l'attenzione pubblica. In realtà, si trattava di materiale artificiosamente generato dall'IA: la foto del presunto B-2 abbattuto era un'elaborazione, così come il video di Tel Aviv distrutta era stato creato con strumenti di *deep learning* ancor prima che gli attacchi missilistici avvenissero realmente. Questi falsi contenuti miravano evidentemente a seminare panico e influenzare la percezione del conflitto sia all'interno della popolazione israeliana sia a livello internazionale. Le autorità israeliane hanno dovuto attivarsi per smentire rapidamente tali *fake news*, mentre aziende specializzate in cybersecurity forense – come la startup locale *GetReal* – sono state coinvolte per analizzare la veridicità dei media circolanti. Secondo Hany Farid, esperto di analisi forensi digitali, siamo di fronte a *"un trend allarmante di contenuti falsi che circolano online durante i grandi eventi mondiali"*[7], la cui individuazione risulta sempre più complessa. Significativamente, gli analisti notano che sia Israele sia l'Iran possiedono capacità avanzate in ambito IA e non hanno remore a impiegare *deepfake* e reti di *bot* per sostenere le rispettive narrative belliche. In un certo senso, gli strumenti di disinformazione automatizzata diventano essi stessi armi strategiche, dal momento che possono creare l'illusione di un consenso o di una rivolta popolare là dove non esistono, orientare l'opinione pubblica contro i leader avversari e indebolire la coesione sociale del nemico. Ciò ha implicazioni anche per i processi elettorali: in Iran, ad esempio, propaganda con video falsi potrebbe essere usata per delegittimare candidati moderati accusandoli di legami segreti con Israele; viceversa, in Israele, campagne di *fake news* orchestrate da attori esterni potrebbero puntare a influenzare l'elettorato su temi di sicurezza nazionale, favorendo fazioni politiche più aggressive o più arrendevoli a seconda degli interessi di chi diffonde la disinformazione. Durante le ultime elezioni israeliane del 2022, si registrarono già tentativi di ingerenza cibernetica attribuiti a Iran e

7 Farid, H., interventi e analisi pubbliche sull'uso di deepfake e contenuti sintetici nei conflitti contemporanei (2023–2024). L'autore osserva come la diffusione di media falsificati durante grandi eventi geopolitici rappresenti una tendenza allarmante, reso più difficile da contrastare dall'elevata qualità dei contenuti generati dall'intelligenza artificiale e dalla rapidità con cui essi circolano negli ecosistemi digitali globali.

altri gruppi, sebbene senza un impatto determinante. Tuttavia, l'avvento di IA sempre più potenti rende verosimile un salto di qualità: nel prossimo futuro, campagne elettorali condotte in parallelo a conflitti militari potrebbero essere "inquinate" da ondate di contenuti falsificati (discorsi attribuiti fraudolentemente a leader, scandali inventati, appelli alla resa falsi) generati e diffusi con pochi clic. Tale prospettiva desta forti preoccupazioni nella comunità internazionale, poiché minaccia di compromettere ulteriormente la possibilità di avere processi democratici legittimi in regioni già instabili.

10.3 Disinformazione automatizzata e *deepfake* in scenari bellici

Una delle manifestazioni più insidiose dell'IA nei contesti di guerra è il suo impiego in operazioni di *disinformazione su larga scala*, in particolare tramite la creazione di contenuti multimediali *deepfake*. Con questo termine si indicano video, audio o immagini generati dall'intelligenza artificiale che riproducono in maniera iper-realistica volti e voci di persone reali, alterandone però i messaggi e le azioni. In situazioni di conflitto, i deepfake diventano armi psicologiche potenti: possono diffondere notizie false mirate a demoralizzare le truppe, ingannare la popolazione civile o influenzare l'andamento politico di una nazione nemica senza sparare un colpo. Un caso divenuto emblematico è quello già citato del falso video del Presidente ucraino Zelensky diffuso nel marzo 2022, poche settimane dopo l'invasione russa dell'Ucraina. In quel breve filmato artefatto, realizzato con un grossolano *face swap* digitale, Zelensky appariva con espressione affranta nell'ufficio presidenziale mentre invitava i suoi concittadini a deporre le armi e ad arrendersi alle forze russe. Il deepfake, benché tecnicamente imperfetto (l'intonazione e la colorazione del volto tradivano anomalie evidenti), fu presumibilmente concepito per seminare il panico e la resa tra le fila ucraine. La reazione immediata del governo di Kiev – che tramite i social ufficiali e una pronta smentita video dello stesso Zelensky definì la clip una *"provocazione infantile"*[8] e ribadì *"non deporremo le armi"*[9] – riuscì a ridurre l'impatto dell'inganno. Tuttavia, gli esperti hanno messo in guardia che quell'episodio potrebbe rappresentare *"solo la punta dell'iceberg"*[10] delle future manipolazioni

8 Zelensky, V., dichiarazione pubblica della Presidenza dell'Ucraina (marzo 2022), in cui il Presidente definisce il video deepfake che lo ritrae mentre invita alla resa come una "provocazione infantile", respingendo ogni ipotesi di cessazione della resistenza armata.

9 Zelensky, V., messaggio video ufficiale diffuso sui canali istituzionali ucraini (marzo 2022), nel quale il Presidente ribadisce che l'Ucraina "non deporrà le armi", smentendo il contenuto del deepfake circolato online.

10 Analisi successive al caso del deepfake attribuito al Presidente ucraino Zelensky (2022–2023) da parte di esperti di disinformazione e digital forensics (tra cui **Hany Farid** (University of California, Berkeley), **Nina Jankowicz** (disinformation studies, già Executive Director del

belliche basate sull'IA. Col prolungarsi della guerra, infatti, le autorità ucraine avevano già avvisato della possibilità che Mosca utilizzasse deepfake sempre più sofisticati per confondere la popolazione e i militari.

Questa previsione si è in parte avverata: negli anni seguenti, la propaganda russa ha effettivamente iniziato a incorporare anche elementi sintetici (come falsi video di presunte atrocità ucraine, o discorsi manipolati di leader occidentali) all'interno della sua campagna di disinformazione volta a giustificare l'aggressione. Parallelamente, altri scenari di conflitto hanno visto proliferare l'uso malevolo di deepfake. Nella guerra civile siriana, ad esempio, si sono segnalati audio falsificati di comandanti ribelli diffusi per minarne la credibilità; nel contesto delle tensioni Cina-Taiwan, circolano periodicamente video contraffatti riguardanti mosse militari o dichiarazioni di resa di Taipei, volti a dissuadere l'isola dalla resistenza.

Un tratto peculiare della disinformazione basata sull'IA è la sua velocità e diffusività. Strumenti come generatori di testo e immagini (ad es. reti neurali tipo GPT o GAN) permettono di creare in pochi secondi centinaia di varianti di uno stesso messaggio falso, adattandolo a pubblici diversi e disseminandolo contemporaneamente su più piattaforme. In pratica, l'IA consente campagne di *propaganda automatizzata* di portata senza precedenti, difficili da contrastare con i mezzi tradizionali. Durante il 2024, definito da alcuni *"l'anno delle elezioni"*[11] per l'elevato numero di tornate elettorali a livello globale, questo fenomeno ha destato allarme: si teme infatti che i deepfake e altri contenuti generati dall'IA possano essere usati per influenzare subdolamente l'esito di elezioni cruciali, amplificando teorie cospirative, diffamando candidati tramite falsi video o creando il caos informativo in prossimità del voto. Organizzazioni come la NATO e l'Unione Europea hanno indicato la disinformazione come parte integrante delle minacce ibride alla sicurezza, avvertendo che *"le campagne di manipolazione mediate dall'IA"*[12] mirano a destabilizzare le democrazie dall'interno. Un esempio

Disinformation Governance Board del DHS), Ben Nimmo (Principal Investigator for Open Source Intelligence, Meta/Facebook) e Clint Watts (ex FBI, analista di information warfare)) hanno qualificato l'episodio come "solo la punta dell'iceberg". Tali analisi hanno avvertito che la rapida evoluzione dell'intelligenza artificiale generativa avrebbe reso future operazioni di manipolazione bellica e psicologica significativamente più sofisticate, credibili e difficili da rilevare e contrastare, soprattutto in contesti di conflitto armato e crisi geopolitica.

11 L'espressione "l'anno delle elezioni" è stata utilizzata, tra gli altri, da Juhan Lepassaar, Executive Director dell'ENISA, e ripresa da funzionari dell'Unione Europea e da International IDEA per indicare il 2024 come anno eccezionale per numero e rilevanza delle consultazioni elettorali globali, con un conseguente aumento sistemico dei rischi di interferenza informativa e cibernetica potenziata dall'intelligenza artificiale.

12 L'espressione "campagne di manipolazione mediate dall'IA" è utilizzata da Ilkka Salmi (European External Action Service) e ripresa nelle analisi del NATO Strategic Communications Centre of Excellence, nonché da Ben Nimmo, per descrivere operazioni di disinformazione e influenza che sfruttano intelligenza artificiale generativa, bot e tecniche automatizzate al fine di destabilizzare le democrazie dall'interno, soprattutto in contesti elettorali.

concreto è avvenuto nelle elezioni parlamentari slovacche del 2023, quando furono diffusi su Internet video *deepfake* che pretendevano di mostrare brogli elettorali compiuti dal governo uscente, alimentando sfiducia e tensione sociale. Anche se poi smascherati, quei falsi contribuirono a creare un clima di sospetto tale che una parte dell'elettorato rifiutò di accettare il risultato elettorale, già condizionato da narrative cospirative e polarizzanti propagate online[13]. Questo episodio illustra come i deepfake possano essere sfruttati non solo da attori esterni (come Stati ostili) ma anche da forze politiche interne senza scrupoli, che ne amplificano i contenuti per proprio tornaconto. Il rischio sistemico è la frammentazione della realtà condivisa: segmenti di popolazione finiscono per credere ciascuno alla "propria" versione dei fatti, rendendo impossibile un dibattito pubblico basato su fatti oggettivi e minando alla base la legittimità del processo democratico.

Di fronte a tali minacce, emergono diverse linee di difesa. Da un lato, si stanno sviluppando tecnologie di *deepfake detection*, spesso esse stesse basate su algoritmi di IA addestrati a riconoscere artefatti digitali impercettibili all'occhio umano (incongruenze di pixel, riflessi di luce innaturali, asincronie labiali, ecc.). Aziende specializzate in *forensic tech* stanno affiancando governi e media nella verifica dei contenuti virali: il caso citato di *GetReal* in Israele, che ha analizzato i filmati sospetti del conflitto con l'Iran, ne è un esempio. Allo stesso tempo, piattaforme e *social network* sono sotto pressione affinché implementino sistemi di tracciamento dell'origine dei media (come filigrane digitali, certificati di autenticità o metadati verificati) per ogni video o immagine condivisa. La risposta normativa sta muovendo i primi passi: ad esempio, negli Stati Uniti ben 25 stati hanno approvato leggi che vietano o regolano la diffusione di deepfake a scopo di interferenza elettorale, prevedendo sanzioni per chi pubblica video/audio falsificati di candidati nei periodi immediatamente precedenti al voto[14]. Tali leggi mirano a prevenire la *manipolazione occulta dell'elettorato* resa possibile dall'IA, imponendo obblighi di trasparenza e divieti mirati (come l'uso di

13 Woolley, S. C., & Howard, P. N. (eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford University Press, 2019; de Nadal, L., & Jančárik, P., "Beyond the deepfake hype: AI, democracy, and 'the Slovak case'", *Harvard Kennedy School Misinformation Review*, 2024. Le fonti descrivono come reti di account coordinati (bot e profili inautentici) e contenuti sintetici possano simulare consenso o dissenso "dal basso" (*astroturfing / coordinated inauthentic behavior*), amplificando polarizzazione e sfiducia; i casi recenti mostrano che l'impatto di singoli contenuti manipolati dipende fortemente dal contesto (bassa fiducia, frammentazione informativa, dinamiche di piattaforma), rendendo l'operazione di influenza un fenomeno socio-tecnico più che un semplice "falso" isolato.

14 Public Citizen, *25 States Enact Laws to Regulate Election Deepfakes*, 13 maggio 2025; Public Citizen, *Tracker: State Legislation on Deepfakes in Elections*, aggiornamenti 2025. Le fonti documentano la rapida proliferazione di normative statali USA sui deepfake elettorali (divieti temporali pre-elezione, obblighi di disclosure/etichettatura, eccezioni per satira e parodia), evidenziando la tensione strutturale tra tutela dell'integrità informativa e salvaguardia della libertà di espressione.

deepfake denigratori durante la campagna) per tutelare il diritto degli elettori a una corretta informazione. Analoghi provvedimenti sono allo studio in Europa: la Commissione Europea, ad esempio, ha emanato nel 2022 un Codice rafforzato di buone pratiche sulla disinformazione, che impegna le grandi piattaforme online a identificare e segnalare i contenuti manipolati con IA. Inoltre, il Regolamento UE 2024/900 sulla trasparenza della pubblicità politica prevede l'obbligo di indicare chiaramente l'uso di tecniche automatizzate e di dati personali nelle inserzioni elettorali online, per contrastare la microtargettizzazione occulta degli elettori. Nonostante ciò, resta aperta la questione dell'effettiva applicazione di tali misure: identificare e rimuovere in tempo reale contenuti falsi in un ecosistema informativo globalizzato è impresa ardua, e vi è il rischio che gli strumenti di moderazione automatica si rivelino insufficienti o tardivi rispetto alla rapidità virale delle *fake news*. Per questo molti esperti sottolineano l'importanza di agire anche sul lato della resilienza sociale: programmi diffusi di educazione ai media e al digitale, campagne di *awareness* sui pericoli dei deepfake e sul funzionamento delle tecnologie di IA, nonché il coinvolgimento attivo dei media tradizionali nel *fact-checking*, sono tutti elementi essenziali per creare un elettorato più consapevole e meno facilmente manipolabile[15]. In ultima analisi, la sfida dei deepfake in tempo di guerra (e di elezioni) è destinata a crescere nel prossimo futuro, ma una combinazione di innovazioni tecniche, normative efficaci e aumento della coscienza critica del pubblico potrà arginarne gli effetti più deleteri sul processo democratico.

10.4 Attacchi cibernetici a infrastrutture elettorali in contesti bellici

Accanto alla disinformazione, un altro rischio concreto nei contesti di guerra è rappresentato dagli attacchi informatici diretti contro le infrastrutture del processo elettorale, specialmente laddove si impiegano sistemi di voto elettronico o di gestione digitale delle elezioni. In tempo di pace, la cybersecurity elettorale è già una questione critica; ma in scenari bellici questi sistemi possono diventare bersagli prioritari di operazioni ostili tese a sabotare il funzionamento della democrazia dall'interno. Gli attacchi possono assumere forme diverse: intrusioni nelle liste elettorali per cancellare o modificare dati di registrazione degli elettori; manomissione dei sistemi di voto a distanza o delle macchine di

15 Patel, A. (2025), *Freedom of Expression, Artificial Intelligence, and Elections* (issue brief UNESCO/UNDP); UNDP, *Strengthening Information Integrity in Elections*, 2025; UNESCO, *Deepfakes and the crisis of knowing*, 2025. La letteratura più recente sottolinea che, oltre a detection e rimozione, la resilienza democratica richiede interventi "a monte" di alfabetizzazione mediatica e digitale (prebunking, educazione alla verifica delle fonti, comprensione delle tecniche generative e dei limiti cognitivi), per ridurre la vulnerabilità della popolazione a manipolazioni rapide e scalabili, soprattutto in contesti di crisi e conflitto.

voto elettronico per alterare voti o conteggi; blocco dei server di pubblicazione dei risultati tramite attacchi *DDoS* (Distributed Denial of Service) per ritardare o impedire l'annuncio degli esiti; fino a operazioni più subdole come l'inoculazione di malware nei software elettorali al fine di creare malfunzionamenti e mettere in dubbio l'affidabilità del voto. È evidente che in un contesto di conflitto queste azioni possono essere coordinate con le operazioni militari sul campo: ad esempio, un attacco hacker potrebbe cercare di far saltare un'elezione in una zona contesa immediatamente prima o dopo un'offensiva militare, così da delegittimare le autorità locali e facilitarne la caduta. Oppure, un attore ostile potrebbe sfruttare la distrazione dell'opinione pubblica durante una crisi di sicurezza per penetrare nei sistemi elettorali di un paese vicino e preparare future manipolazioni.

Abbiamo già esaminato il caso ucraino del 2014, in cui un attacco cibernetico su scala nazionale fu condotto come parte integrante dell'azione bellica russa. Da allora, vari altri episodi hanno confermato il nesso fra guerra e cyber-attacchi elettorali. Nel 2015, durante il conflitto in corso in Ucraina, gruppi hacker sponsorizzati da Mosca (es. *CyberBerkut*) attaccarono ripetutamente i siti governativi e i sistemi del Parlamento ucraino, minacciando di colpire anche future consultazioni elettorali. Nel 2020, secondo fonti USA, l'Iran prese di mira l'infrastruttura elettorale israeliana con tentativi di intrusione nei registri degli elettori, nel quadro delle tensioni seguite alle operazioni militari tra i due paesi (anche se Israele negò impatti significativi). Ancora, nel 2022, pochi giorni prima dell'invasione russa dell'Ucraina, si registrò un massiccio attacco DDoS che colpì i siti del Ministero della Difesa e di due grandi banche ucraine; contestualmente furono diffusi falsi allarmi di chiusura di bancomat via SMS ai cittadini, probabilmente per generare panico e sfiducia verso le autorità. Si tratta di uno schema che, se applicato al giorno di un'ipotetica elezione, potrebbe causare il caos. In prospettiva, qualora una nazione sotto attacco bellico tentasse di organizzare elezioni (ad esempio per riaffermare la propria legittimità democratica), dovrebbe affrontare non solo le difficoltà logistiche e di sicurezza fisica, ma anche la quasi certa aggressione cibernetica ai sistemi elettorali da parte dell'avversario. Non a caso, la dichiarazione congiunta della conferenza di Berna 2023 (Consiglio d'Europa) riconosce che *"è quasi impossibile soddisfare gli standard democratici internazionali durante conflitti armati in corso"*, sottolineando la necessità di definire condizioni minime e misure straordinarie per poter tenere elezioni libere subito dopo la fine delle ostilità. Tra queste misure rientra certamente la messa in sicurezza delle infrastrutture elettorali critiche. Viene raccomandato di predisporre *roadmap* post-belliche che assicurino il ripristino di registri elettorali affidabili, l'aggiornamento dei sistemi di voto e la verifica integrale di eventuali componenti hardware/software utilizzate, al fine di accertare che il nemico non vi abbia inserito *backdoor* o malware durante il conflitto. Questo perché un avversario potrebbe sfruttare l'occupazione di territori o l'accesso clandestino

alle reti per compromettere i sistemi elettorali e poi, a guerra finita, innescare disservizi o manipolazioni dall'interno.

In ambito internazionale cresce dunque l'attenzione sulla *cyber resilience* dei processi democratici in tempo di crisi. L'Unione Europea ha dichiarato le elezioni una possibile *infrastruttura critica* da proteggere e, pur lasciando agli Stati membri la scelta degli strumenti (alcuni paesi UE hanno sperimentato il voto elettronico, altri lo rifiutano), promuove lo scambio di informazioni sulle minacce e sulle migliori pratiche di difesa. Strumenti come la direttiva NIS2, adottata a fine 2022, impongono standard minimi di sicurezza informatica a un ventaglio ampliato di settori essenziali, che ora includono anche la *pubblica amministrazione* centrale e regionale. Ciò significa che, indirettamente, anche le autorità elettorali rientrano tra i soggetti che dovranno adeguarsi a rigorose misure di gestione del rischio cyber e notifica degli incidenti[16]. In pratica, un Ministero dell'Interno o un Ufficio elettorale centrale di uno Stato UE, essendo parte dell'amministrazione pubblica, dovrà dotarsi di piani di sicurezza avanzati (cifratura dei dati, sistemi di *intrusion detection*, audit periodici del codice dei software elettorali, ecc.) e sarà soggetto a sanzioni in caso di inadempienza sulla cybersecurity. L'obiettivo è elevare il livello di protezione contro attacchi statuali o terroristici che possano compromettere servizi cruciali come le elezioni. Inoltre, la cooperazione a livello europeo e NATO offre ulteriori garanzie: EU ed ENISA (Agenzia UE per la cybersecurity) hanno istituito task force e gruppi di risposta rapida (come la rete *EU-CyCLONe*) per gestire incidenti cyber su larga scala e specifiche simulazioni di crisi (war games) sono state condotte includendo scenari di attacchi informatici durante processi elettorali, così da testare la prontezza delle contromisure. In ambito NATO, il Centro di eccellenza per la cybersecurity (CCDCOE) di Tallinn ha sviluppato il *Cyber Law Toolkit* e guide per la protezione delle elezioni in operazioni di difesa collettiva, riconoscendo che un attacco cibernetico su infrastrutture elettorali di un paese membro potrebbe, in certe circostanze, attivare l'art. 5 del Trattato NATO se equiparato a un attacco contro la sua sicurezza nazionale. Siamo dunque in presenza di una crescente *militarizzazione* della sicurezza elettorale: ciò che un tempo era dominio esclusivo di giuristi e tecnici elettorali oggi coinvolge anche esperti militari, intelligence e organismi di difesa, a testimonianza che proteggere le urne equivale a proteggere la sovranità nazionale.

16 Direttiva (UE) 2022/2555 (*NIS2*), 14 dicembre 2022; Commissione europea, documentazione di policy sulla NIS2 e sui settori/obblighi di gestione del rischio e notifica incidenti (2023–2025). La NIS2 amplia il perimetro degli obblighi di sicurezza e resilienza per enti essenziali e importanti, includendo la pubblica amministrazione in molti casi e imponendo misure organizzative e tecniche, reporting e governance del rischio; ciò incide indirettamente anche sulle autorità elettorali digitalizzate e sulle infrastrutture pubbliche che supportano il ciclo elettorale.

In quest'ottica, l'IA gioca un ruolo ambivalente. Da un lato, gli aggressori possono usarla per potenziare i loro attacchi: ad esempio, algoritmi di *machine learning* possono scansionare automaticamente il codice di un software di voto alla ricerca di vulnerabilità sconosciute (*zero-day exploits*), oppure generare milioni di tentativi di *phishing* altamente personalizzati per ingannare gli operatori elettorali e ottenere credenziali di accesso. D'altro canto, l'IA è anche un potente alleato per i difensori: sistemi di *cyber threat intelligence* basati su AI possono analizzare in tempo reale enormi flussi di dati di rete, rilevando pattern anomali che segnalino un attacco in corso, o prevedendo con algoritmi predittivi quali asset sono più a rischio e quando. Già oggi alcuni Paesi impiegano strumenti di IA per *stress-testare* le proprie piattaforme di e-voting. In pratica vengono lanciati attacchi simulati generati da computer per identificare punti deboli e per monitorare i social media in cerca di segni premonitori di intrusioni (ad esempio, gruppi hacker che rivendicano in anticipo di avere accesso ai sistemi elettorali di un dato paese). Nonostante questi progressi, la natura asimmetrica del conflitto cibernetico resta preoccupante, poiché basta una singola falla trascurata perché un attacco abbia successo, mentre i difensori devono proteggere ogni anello della catena. Per questa ragione, insieme alla prevenzione tecnologica si prevedono piani di *emergency backup* con molti Stati che stanno predisponendo protocolli per tornare al voto tradizionale cartaceo nel caso in cui i sistemi elettronici risultassero compromessi da attacchi, assicurando così la continuità del processo democratico anche sotto pressione nemica. Ad esempio, è noto che l'Estonia – pioniera del voto online – mantiene comunque la possibilità di disattivare l'e-voting e utilizzare schede fisiche qualora l'intelligence rilevi un imminente cyber-attacco su vasta scala durante le elezioni. Misure analoghe di *ridondanza analogica* sono raccomandate nelle linee guida internazionali, affinché la tecnologia rimanga un mezzo e non un punto di vulnerabilità fatale per la democrazia.

10.5 Digital Forensics e attribuzione in zone di conflitto

Quando si verificano incidenti di sicurezza informatica o campagne di disinformazione in contesti elettorali, soprattutto durante conflitti, diventa fondamentale poter condurre *indagini informatico-forensi* efficaci per attribuire le responsabilità e raccogliere prove utilizzabili in sede legale.

La *digital forensics* applicata alle interferenze elettorali comprende una serie di tecniche: dall'analisi dei log di sistema per ricostruire accessi non autorizzati, all'estrazione di metadati da video e immagini sospette per risalire al dispositivo o software che le ha generate, fino all'utilizzo di database OSINT (Open Source INTelligence) e metodi di *tracciamento blockchain* per seguire la diffusione di criptovalute che finanziano operazioni occulte. Nei teatri di guerra, queste attività investigative incontrano ostacoli aggiuntivi, quali ad esempio infrastrutture degradate, mancanza di personale addestrato sul campo, ostilità attiva

dell'avversario. Tuttavia esse assumono un ruolo cruciale: come riconosciuto dal Consiglio d'Europa, *"le prove dei crimini di guerra sono spesso in formato digitale"* e ciò vale anche per gli attacchi cibernetici o le operazioni informative condotte durante i conflitti.

Un importante sviluppo in questo ambito è il crescente coinvolgimento di organi di giustizia internazionale nelle indagini cyber. Nel giugno 2023 fonti Reuters hanno rivelato che la Corte Penale Internazionale (CPI) stava investigando su sospetti attacchi hacker russi contro infrastrutture civili ucraine considerandoli alla stregua di possibili *crimini di guerra*, in quanto violazioni deliberate della legge umanitaria. Si tratta di un precedente significativo: se un cyber-attacco (ad esempio contro la rete elettrica di una città, o ipoteticamente contro il sistema elettorale di un paese in guerra) causa gravi conseguenze per la popolazione civile, esso può essere assimilato a un attacco convenzionale vietato dal diritto bellico e dunque perseguibile penalmente. Nel caso specifico, l'Ucraina ha cooperato strettamente con la CPI fornendo tracciamenti digitali e altri elementi probatori per individuare i responsabili degli attacchi informatici ai danni dei suoi civili. In futuro, questo approccio potrebbe estendersi: se durante un conflitto un attore statale manipolasse pesantemente un'elezione (per esempio nei territori occupati, imponendo con la forza un "referendum" farsa mediante sistemi elettronici compromessi), ciò potrebbe essere presentato in sede internazionale come violazione dei diritti politici della popolazione, se non addirittura come atto di persecuzione politica. Al di là del diritto penale internazionale, anche a livello di cooperazione transnazionale di polizia si registrano novità: l'Interpol e le forze di diversi paesi hanno istituito task force congiunte per tracciare gruppi hacker attivi in operazioni di interferenza elettorale. Un esempio è la collaborazione tra FBI statunitense e omologhi europei per smantellare, nel 2024, una rete di *troll farm* basata a San Pietroburgo (notoriamente legata all'Internet Research Agency) che utilizzava anche contenuti deepfake per influenzare opinioni su elezioni estere. L'operazione ha comportato il sequestro di server in vari paesi e l'analisi di terabyte di dati per collegare le attività a individui specifici, dimostrando l'importanza di condividere intelligence e capacità forensi fra nazioni alleate.

In questo contesto, la Convenzione di Budapest sul cybercrime (2001) e i suoi protocolli aggiuntivi forniscono un quadro giuridico prezioso per abilitare la cooperazione investigativa. La Conferenza di Berna 2023 ha ribadito *"l'importanza della Convenzione di Budapest e in particolare del Secondo Protocollo Addizionale sulla cooperazione potenziata"* proprio come strumenti per assicurare la raccolta e condivisione rapida di prove elettroniche nelle indagini sulle interferenze elettorali transfrontaliere[17]. Il Secondo Protocollo, aperto alla firma nel maggio 2022,

17 Consiglio d'Europa, *Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) on enhanced co-operation and disclosure of electronic evidence*, aperto alla firma il 12 maggio 2022; Assemblea Parlamentare del Consiglio d'Europa, *Final Declaration – Bern Conference "Elections in*

introduce meccanismi innovativi come la possibilità per le autorità di un paese di richiedere direttamente ai fornitori di servizi esteri i dati degli utenti (ad es. registri di provider internet, informazioni su account social) o di ottenere in tempi estremamente rapidi conservazioni di dati e cooperazione *urgentissima* in caso di attacchi gravi. Questi strumenti, corredati da garanzie di tutela dei diritti umani, sono pensati per superare le lente burocrazie delle rogatorie tradizionali, riconoscendo che nel dominio digitale – specialmente durante una crisi – le tracce possono svanire in poche ore se non acquisite prontamente. Ad esempio, se durante un conflitto si sospetta un attacco hacker a un sistema elettorale partito da server in un altro paese, tramite il Protocollo Budapest le forze di polizia possono chiedere immediatamente ai provider di hosting i log e i dati relativi a quell'attacco, senza dover attendere mesi di procedure diplomatiche. Ciò aumenta significativamente le chance di attribuzione degli attacchi e quindi di deterrenza. La Segretaria Generale del Consiglio d'Europa ha sottolineato che grazie a questi nuovi strumenti *"la Convenzione di Budapest resterà il quadro internazionale più rilevante ed efficace per combattere il cybercrime negli anni a venire"*, anche alla luce delle sfide poste dalla guerra in Ucraina e da altre crisi.

Un aspetto peculiare delle indagini digitali in tempo di guerra è che spesso coinvolgono una molteplicità di attori, civili inclusi. Nel conflitto russo-ucraino, ad esempio, è emerso il fenomeno dei *patriotic hackers*, cioè di esperti informatici volontari, spesso privati cittadini, che conducono attacchi contro il nemico o aiutano la difesa nazionale in modo non ufficialmente inquadrato. L'ICRC (Comitato Internazionale della Croce Rossa) ha emanato nel 2022 delle linee guida in cui invita gli hacker civili a rispettare il diritto bellico, ricordando che, sebbene essi non siano combattenti legittimi, le loro azioni (ad esempio sabotare sistemi civili avversari) possono comunque mettere a rischio vite umane e quindi violare i principi umanitari[18]. Inoltre, la presenza di hacker civili complica l'attribuzione: un attacco a un'infrastruttura elettorale potrebbe provenire da un individuo autonomo o da un gruppo non direttamente controllato da uno Stato, sollevando interrogativi su come qualificare legalmente tale condotta (crimine

times of crisis", 9–10 maggio 2023. Le fonti collegano la cooperazione rafforzata per l'acquisizione e la conservazione rapida di evidenze elettroniche (incluse richieste dirette e procedure d'urgenza verso service provider, con garanzie sui diritti) alla necessità di investigare interferenze transfrontaliere, incluse quelle che colpiscono infrastrutture democratiche e processi elettorali.

18 Comitato Internazionale della Croce Rossa (ICRC), *Eight rules for "civilian hackers" during war, and four obligations for states to restrain them*, 2022; ICRC, *International Humanitarian Law and the growing involvement of civilians in cyber operations and other digital activities during armed conflict*, report, 2025. I documenti chiariscono che il coinvolgimento di "patriotic hackers" e civili in operazioni cyber in contesto di conflitto può integrare partecipazione diretta alle ostilità e aumentare rischi per civili e infrastrutture; inoltre complica attribuzione e qualificazione giuridica delle condotte, rafforzando l'esigenza di regole di contenimento statale, due diligence e raccolta probatoria solida.

comune, atto di terrorismo, o comunque atto imputabile allo Stato che lo tollera?). Il dibattito è aperto, ma nella prassi gli Stati tendono a ritenere responsabile anche lo Stato avversario se non impedisce che il proprio territorio (o il proprio ciberspazio) sia utilizzato per lanciare attacchi informatici devastanti durante un conflitto. In ogni caso, raccogliere prove solide diviene fondamentale per sostenere eventuali accuse sul piano internazionale. Tecniche di *attribution* come l'analisi del malware (per rintracciare similitudini con codici noti di gruppi hacker sponsorizzati), l'identificazione di fusi orari, lingua e altre *fingerprints* nei software usati, rimangono strumenti chiave per risalire ai mandanti. L'IA può certamente dare un contributo anche in questo caso: algoritmi di clustering e correlazione possono setacciare enormi quantità di dati di attacco, individuando pattern ricorrenti che suggeriscono un'unica regia dietro atti apparentemente scollegati. In sintesi, la guerra nel ciberspazio elettorale è anche una guerra di investigazione e contro-investigazione informatico-forense, in cui ogni parte cerca di risalire alle tracce digitali del nemico e, al contempo, di occultare le proprie. La capacità forense di far luce su queste operazioni è dunque non solo uno strumento di giustizia *ex post*, ma anche un elemento deterrente *ex ante*: se un attore sa che le sue azioni nel dominio digitale potranno essere provate e attribuite, sarà meno incline a violare impunemente le regole.

10.6 Evoluzione del quadro giuridico e normativo (agg. Luglio 2025)

Le trasformazioni tecnologiche e strategiche descritte hanno posto con urgenza la questione di come adeguare il quadro giuridico, sia nazionale che internazionale, per fronteggiare efficacemente le interferenze elettorali mediate dall'IA in situazioni di conflitto. Al luglio 2025 si possono registrare progressi su vari fronti, sebbene permangano zone grigie e sfide interpretative significative.

In ambito di *diritto internazionale umanitario* (DIU), il principio cardine è che le norme delle Convenzioni di Ginevra e del diritto bellico si applicano anche alle operazioni condotte nel ciberspazio durante i conflitti armati, così come a qualsiasi altro mezzo o metodo di guerra. Gli Stati e comitati di esperti (si veda il *Tallinn Manual 2.0* del NATO CCDCOE) hanno in gran parte concordato su questo punto: l'IA e gli attacchi cyber non creano un vuoto giuridico, ma rientrano nelle regole esistenti, prime fra tutte il divieto di attacchi diretti a civili o a oggetti civili, il principio di distinzione e quello di proporzionalità. Tuttavia, permangono aree di incertezza rilevanti per le interferenze elettorali. Un cyber-attacco che *disturbi o impedisca un'elezione* senza causare distruzioni fisiche (ad esempio bloccando i sistemi elettronici di voto o manipolando i dati elettorali) può essere considerato un "attacco" ai sensi del DIU? Secondo alcuni esperti, se l'effetto è quello di privare i civili del loro diritto fondamentale di partecipare

alla vita politica, potrebbe configurarsi come una forma di violenza intellettuale comunque vietata, specie se mirata a esercitare controllo sulla popolazione nemica. La posizione del CICR è cauta e ritiene che sia necessario un ulteriore chiarimento vòlto a determinare se *"operazioni cyber che perturbano i sistemi senza arrecare danni fisici costituiscano attacchi ai sensi del diritto umanitario"*. Finora nessun trattato lo definisce esplicitamente. Tuttavia, c'è consenso che, se tali operazioni causano *effetti equiparabili* a quelli di un attacco cinetico (ad esempio il collasso di infrastrutture civili vitali), allora i principi del DIU scattano. Nel caso delle elezioni, si può ipotizzare che sabotare deliberatamente un'elezione in corso in territorio nemico, specie se parte di un'occupazione, vìoli anche l'obbligo di potenza occupante di garantire l'ordine pubblico e i diritti civili fondamentali (IV Convenzione di Ginevra).

Un altro tema aperto è la protezione dei dati civili: il DIU protegge le persone e gli oggetti civili, ma i dati personali (come liste di elettori) sono essi stessi considerabili "oggetti" protetti? La digitalizzazione delle società pone questa nuova domanda. Il CICR ha auspicato che *"il diritto umanitario sia interpretato in modo da proteggere non solo gli oggetti fisici ma anche le infrastrutture digitali essenziali nella vita delle persone"*. Ciò implicherebbe che attacchi informatici contro, ad esempio, il registro elettorale nazionale (parte della *infrastruttura digitale critica*) dovrebbero essere proibiti al pari di un attacco fisico contro gli uffici elettorali. Nel 2021, in un'importante dichiarazione alle Nazioni Unite, il CICR ha proposto che i dati personali dei civili siano assimilati a *beni civili* protetti, specialmente se il loro sabotaggio può arrecare un danno umanitario (si pensi ai dati sanitari, ma anche ai dati elettorali che garantiscono diritti politici). Tale proposta non è ancora diritto cogente, ma indica la direzione di un possibile sviluppo normativo.

Un'altra area cruciale è la normativa sulla cibersicurezza e la resilienza elettorale in tempo di pace, che getta le basi per resistere meglio anche in tempo di guerra. A livello regionale, l'Unione Europea ha adottato negli ultimi anni una serie di atti rilevanti. Si è citata la Direttiva (UE) 2022/2555 (*NIS2*), entrata in vigore nel 2023, che obbliga gli Stati membri a definire strategie di cybersecurity e ad applicare misure rigorose a numerosi settori critici, inclusa la pubblica amministrazione e potenzialmente gli organismi elettorali. Parallelamente, il Regolamento 2022/2065 (*Digital Services Act*) impone ai grandi fornitori di servizi online obblighi di gestione dei rischi sistemici, tra cui la disinformazione. Ciò potrebbe tradursi, ad esempio, in una maggiore trasparenza algoritmica su piattaforme come Facebook o YouTube durante periodi elettorali sensibili. Nel 2023 l'UE ha inoltre emanato il Regolamento (UE) 2024/904 sulla trasparenza del *targeting* della pubblicità politica, primo nel suo genere, che vieta l'uso di dati sensibili (come opinioni politiche, orientamento religioso o etnico) per micro-mirare messaggi politici senza il consenso esplicito. Tale norma mira a prevenire manipolazioni occulte dell'elettorato rese possibili dall'IA, come quelle emerse nello scandalo *Cambridge Analytica*. Anche il Regolamento europeo

sull'Intelligenza Artificiale (AI Act) contiene disposizioni rilevanti, tra cui il divieto di sistemi di IA che manipolano in modo ingannevole o coercitivo il comportamento umano, compromettendo la libertà decisionale degli individui, inclusi gli elettori. In questo contesto, strumenti come i deepfake politici potrebbero rientrare tra le pratiche vietate nell'Unione, soprattutto se utilizzati per influenzare fraudolentemente l'esito delle elezioni o sopprimere il libero arbitrio degli elettori. Inoltre, l'AI Act vieta espressamente i sistemi di social scoring da parte delle autorità pubbliche e impone forti restrizioni sui sistemi di sorveglianza biometrica in tempo reale in spazi pubblici. Tali divieti e limitazioni contribuiscono indirettamente a tutelare gli elettori, in particolare nei contesti autoritari, impedendo che imprese europee forniscano tecnologie di intelligenza artificiale utilizzabili per profilare, monitorare o intimidire i votanti, ad esempio in situazioni di occupazione militare o di legge marziale.

Sul piano della cooperazione internazionale, oltre alla menzionata Convenzione di Budapest (aperta globalmente all'adesione) si segnala un dibattito in sede ONU su un nuovo trattato sul cybercrime. Tuttavia, stati come la Russia spingono per convenzioni alternative che rischiano di essere meno garantiste sui diritti umani e di non includere clausole robuste sulla cooperazione investigativa. L'UE e altri paesi insistono che il *gold standard* resti la Budapest, che ad oggi (2025) conta oltre 65 Stati parte e, con il Secondo Protocollo, fornisce un quadro aggiornato. Un punto menzionato nella dichiarazione di Berna è l'apprezzamento per il ruolo guida del Consiglio d'Europa nello sviluppo di standard nel digitale per i diritti umani, inclusa la dimensione elettorale. Vengono richiamati i documenti come le *Guidelines on the use of ICT in elections* (Linee guida 2022 sull'uso delle tecnologie digitali nei processi elettorali) e i *Principi 2020 per un uso conforme ai diritti fondamentali delle tecnologie digitali nelle elezioni*, elaborati dalla Commissione di Venezia. Questi testi non vincolanti offrono raccomandazioni dettagliate agli Stati su come introdurre l'IA e l'automazione nel ciclo elettorale in modo etico e rispettoso della democrazia (ad esempio richiedendo trasparenza sugli algoritmi di conteggio elettronico, audit indipendenti sulle piattaforme di voto online e misure contro la propaganda computazionale). Sebbene non giuridicamente obbligatori, tali standard influenzano le riforme nazionali: ad esempio, l'Italia nel 2023 ha modificato la propria legge elettorale per esplicitare che è reato la diffusione di *media sintetici falsi* atti a influenzare il voto, ispirandosi ai principi emersi in sede europea.

Infine, va citato il diritto internazionale generale, in particolare il principio di non ingerenza negli affari interni degli Stati e il divieto di uso della forza. Interferire deliberatamente nelle elezioni di un altro Stato, specie mediante campagne di destabilizzazione digitale coordinate da un governo, può costituire una violazione della sovranità e del principio di non intervento. Nel 2022 la *International Law Commission* dell'ONU ha avviato studi sull'applicabilità di questi principi alle operazioni informatiche: diversi Stati occidentali hanno dichiarato

che la manipolazione intenzionale dei processi democratici altrui dovrebbe considerarsi un atto illecito internazionale, potenzialmente sanzionabile con contromisure. Alcuni casi estremi potrebbero perfino configurare *uso della forza*: se un attacco cibernetico distruggesse infrastrutture elettorali critiche causando caos e vittime (si immagini un malware che faccia esplodere i macchinari di voto o scateni violenze civili), potrebbe essere equiparato a un attacco armato. In tali scenari limite, la vittima potrebbe invocare la legittima difesa anche sul piano informatico. Finora nessun caso simile è avvenuto, ma la semplice possibilità spinge gli Stati a chiarire *ex ante* le regole: nel 2021 e 2022, due *Open-Ended Working Group* delle Nazioni Unite sul cyberspazio hanno ribadito che il diritto internazionale, compreso il diritto umanitario e la Carta ONU, *"si applica alle tecnologie dell'informazione e comunicazione"*, invitando gli Stati a comportarsi nel ciberspazio in maniera responsabile e conforme ai loro obblighi internazionali. Sebbene queste affermazioni non dettaglino i casi specifici (come le elezioni), esse gettano un ombrello giuridico: attaccare deliberatamente le strutture democratiche di un paese tramite mezzi cibernetici viola i principi fondamentali della convivenza internazionale e può dar luogo a responsabilità dello stato autore, incluso l'obbligo di cessare l'attività e di riparare i danni.

10.7 Conclusioni

L'analisi svolta in questo capitolo mette in luce come l'intelligenza artificiale, integrata nelle dinamiche della guerra moderna, stia ridefinendo i confini della sicurezza elettorale e della sovranità democratica. Abbiamo osservato l'impiego o la minaccia di strumenti basati su IA per interferire nei processi elettorali e nelle percezioni dell'elettorato in teatri di conflitto come l'Ucraina, la Lituania sul fronte informativo o il Medio Oriente: dalle campagne di disinformazione automatizzata con *deepfake* alla manipolazione cibernetica delle infrastrutture di voto, fino alle operazioni di influenza psicologica di massa condotte tramite *bot* e algoritmi sui social media. Queste nuove forme di attacco ibrido rappresentano un'estensione delle tradizionali tattiche belliche nella sfera digitale e cognitiva, dove vincere "cuori e menti" può essere tanto decisivo quanto conquistare territori. La comunità internazionale si trova pertanto di fronte alla necessità di bilanciare l'innovazione tecnologica con robuste salvaguardie democratiche: da un lato sfruttando l'IA stessa come risorsa per migliorare la resilienza (si pensi ai sistemi di allerta precoce per fake news, o agli audit automatizzati di sicurezza nei software elettorali); dall'altro sviluppando un quadro normativo ed etico che impedisca gli abusi più perniciosi.

Gli aggiornamenti giuridici attuali a metà 2025 delineano un percorso promettente ma ancora in evoluzione. A livello interno, molti stati hanno rafforzato le proprie leggi penali e di cybersecurity per sanzionare l'ingerenza informatica nelle elezioni e regolare l'uso dell'IA in ambito politico (come le

leggi anti-deepfake in diversi ordinamenti). A livello regionale e internazionale, strumenti innovativi come la direttiva NIS2 e il Secondo Protocollo di Budapest potenziano rispettivamente la prevenzione e la repressione degli attacchi cyber-elettorali, mentre il diritto internazionale umanitario, pur con gradualità, sta affrontando le sfide poste dalle operazioni digitali ostili, riaffermando principi senza tempo (distinzione, proporzionalità, protezione dei civili) anche di fronte a *weaponization* dell'informazione. Organizzazioni come il Consiglio d'Europa, l'OSCE e l'ONU hanno assunto un ruolo guida nel definire linee guida e promuovere la cooperazione: dalla conferenza di Berna 2023 è emerso chiaramente l'appello a *"prendere tutte le misure per contrastare le interferenze indebite e garantire elezioni libere e corrette anche in situazioni di emergenza, crisi e conflitto armato"*. Ciò implica un approccio *whole-of-society*: non solo misure governative, ma coinvolgimento di media, società civile, settore tecnologico ed elettori stessi nell'opera di tutela della democrazia.

In conclusione, l'IA nei contesti di guerra si rivela un'arma a doppio taglio per i processi elettorali: può essere usata per colpire al cuore le democrazie, ma anche per fortificarle se impiegata responsabilmente. La lezione fornita dai casi esaminati è che la resilienza elettorale in epoca digitale richiede vigilanza continua, adattamento normativo e innovazione tecnica.

Le guerre del XXI secolo non risparmiano dunque le urne: anzi, le *urne* stesse – simbolo della sovranità popolare – diventano bersaglio strategico. Difenderle significa difendere i valori fondanti di libertà e autodeterminazione su cui si basano le società democratiche. In un mondo dove i conflitti sono sempre più combattuti anche con linee di codice e flussi di informazione, garantire elezioni libere ed eque sarà parte integrante della sicurezza nazionale e internazionale. Le norme giuridiche e gli strumenti tecnici dovranno dunque evolvere di pari passo, per assicurare che nemmeno la più feroce delle guerre possa annientare la voce degli elettori.

Capitolo 11
Cambiamenti climatici estremi e voto elettronico

11.1 Introduzione

L'intelligenza artificiale (IA), i fenomeni climatici estremi e il voto elettronico potrebbero sembrare ambiti molto distanti fra loro. In realtà, convergono nelle sfide e nelle opportunità che pongono alle società contemporanee. Da un lato l'IA offre strumenti senza precedenti per affrontare problemi complessi, inclusa la mitigazione del cambiamento climatico, ma dall'altro il suo impiego su larga scala solleva nuove preoccupazioni etiche e ambientali. Allo stesso modo, l'intensificarsi di eventi climatici estremi (inondazioni, ondate di calore, uragani) rischia di destabilizzare i processi democratici tradizionali, rendendo necessarie nuove forme di resilienza istituzionale.

In questo contesto, il voto elettronico emerge sia come potenziale soluzione per garantire la continuità dei meccanismi elettorali in situazioni di crisi, sia come terreno di dibattito sulla sicurezza, l'affidabilità e l'inclusività delle tecnologie civiche. Questo capitolo esamina come l'IA possa contribuire (o talvolta ostacolare) la lotta al cambiamento climatico, in che modo gli eventi climatici estremi incidano sui sistemi democratici e come l'adozione di sistemi di voto elettronico possa rappresentare una risposta efficace e al tempo stesso democratica a tali sfide.

11.2 IA e cambiamenti climatici: opportunità e dilemmi

Lo sviluppo dell'IA offre nuove opportunità per contrastare il cambiamento climatico. Applicazioni avanzate di *machine learning* e analisi dei dati aiutano già oggi a ottimizzare l'uso dell'energia, a migliorare le previsioni meteo-climatiche e a progettare materiali innovativi per l'energia pulita. Ad esempio, sistemi di IA vengono impiegati nella gestione delle reti elettriche intelligenti, nell'ottimizzazione del traffico urbano per ridurre le emissioni e persino nella ricerca di nuovi catalizzatori per batterie più efficienti. Uno studio di Rolnick del 2022 ha evidenziato il potenziale del *machine learning* nell'affrontare numerosi aspetti della crisi climatica, dalla modellazione del clima all'agricoltura di precisione, fornendo soluzioni basate sui dati su larga scala[1]. Tali strumenti possono quindi

1 Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., Ross, A. S., Milojevic-Dupont, N., Jaques, N., Waldman-Brown, A., Luccioni, A., Maharaj, T., Sherwin,

accelerare la transizione ecologica grazie a decisioni e interventi più mirati e fondati sull'evidenza scientifica[2].

Tuttavia, l'impiego dell'IA solleva anche dilemmi ambientali e sociali di rilievo. L'addestramento di modelli di *deep learning* ad alte prestazioni richiede enormi quantità di potenza computazionale, con un consumo energetico non trascurabile che contribuisce alle emissioni di carbonio[3]. Strubell, Ganesh e McCallum (2019) hanno calcolato che l'addestramento di grandi modelli di elaborazione del linguaggio naturale (Natural Language Processing, NLP) può comportare un consumo di energia talmente elevato da dover essere preso in seria considerazione nelle politiche ambientali e tecnologiche. Oltre a questi costi ambientali, emergono altre criticità: l'estrazione massiccia di dati può violare la privacy, mentre algoritmi opachi rischiano di introdurre bias nelle decisioni automatizzate. Dunque, sebbene l'IA possa fungere da alleato potente nella lotta ai cambiamenti climatici, un utilizzo indiscriminato di queste tecnologie rischia di contravvenire agli stessi obiettivi di sostenibilità che si prefigge di perseguire. Ne emerge un quadro ambivalente, in cui la tecnologia può essere al tempo stesso parte della soluzione e parte del problema.

Un ulteriore aspetto da considerare è l'impatto indiretto dell'IA sui processi politici legati al clima. La disponibilità di immense quantità di dati e di strumenti predittivi avanzati potrebbe infatti influenzare le politiche climatiche, nel bene e nel male. Da un lato l'IA può migliorare la qualità delle decisioni fornendo simulazioni estremamente accurate sugli esiti potenziali di determinate politiche ambientali; dall'altro lato si teme che l'elevata complessità tecnica accentui un divario "tecnocratico", escludendo il pubblico dal dibattito. In effetti, alcuni studiosi parlano di un dilemma tra tecnocrazia e democrazia di fronte all'emergenza climatica: da una parte l'urgenza di adottare misure rapide ed efficaci potrebbe spingere verso soluzioni tecnocratiche guidate da esperti e da algoritmi, ma dall'altra rimane imprescindibile coinvolgere democraticamente la cittadinanza nelle scelte collettive. Coeckelbergh e Sætra (2023) descrivono bene questa tensione, evidenziando che l'IA può aprire due percorsi politici divergenti: uno in cui la governance climatica viene in gran parte delegata agli strumenti e alle competenze tecniche e un altro in cui si continua ad enfatizzare

E. D., Mukkavilli, S. K., Kording, K. P., Gomes, C. P., Ng, A. Y., & Bengio, Y. (2022). *Tackling Climate Change with Machine Learning. ACM Computing Surveys*. Gli autori illustrano in modo sistematico come il machine learning possa contribuire alla mitigazione e all'adattamento climatico in settori chiave quali energia, trasporti, agricoltura e modellazione climatica, evidenziando il potenziale trasformativo delle soluzioni data-driven.

2 Ibidem.

3 Strubell, E., Ganesh, A., & McCallum, A. (2019). *Energy and Policy Considerations for Deep Learning in NLP. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*. Lo studio quantifica l'impatto energetico dell'addestramento di grandi modelli di deep learning, mostrando come i costi ambientali del calcolo intensivo debbano essere considerati nelle politiche tecnologiche e nella valutazione complessiva della sostenibilità dell'IA.

il ruolo deliberativo della cittadinanza e dell'expertise umana diffusa[4]. Trovare un equilibrio tra queste due vie è cruciale affinché l'innovazione tecnologica non eroda la legittimità democratica nel fronteggiare la crisi climatica.

11.3 Eventi climatici estremi: sfide per la democrazia e adattamenti istituzionali

Il crescente verificarsi di eventi climatici estremi pone sfide immediate e concrete alle democrazie moderne. Alluvioni, incendi boschivi, uragani e altre calamità legate al clima colpiscono comunità in ogni parte del mondo con frequenza e intensità crescenti. Secondo i dati scientifici, il numero di disastri naturali di origine climatica è quasi triplicato negli ultimi quarant'anni[5]. Inoltre, il Gruppo intergovernativo sul Cambiamento Climatico (IPCC) conferma che il riscaldamento globale in corso rende più probabili e più gravi molti fenomeni estremi, dalle ondate di calore alle precipitazioni intense, causando impatti sistemici su infrastrutture e società[6]. Queste tendenze hanno implicazioni dirette sullo svolgimento delle elezioni e sulla partecipazione politica. Ad esempio, nel solo 2024 eventi meteorologici straordinari hanno interferito con il regolare svolgimento di consultazioni elettorali nazionali o locali in almeno quindici paesi, tra cui Austria, Canada, India, Indonesia e Stati Uniti. Situazioni di emergenza, quali ad esempio uragani alla vigilia del voto o incendi diffusi durante una campagna elettorale, possono impedire a interi segmenti dell'elettorato di recarsi alle urne, causare il rinvio delle elezioni o compromettere la parità di condizioni nella competizione politica.

Di fronte a queste minacce, le istituzioni democratiche devono sviluppare strategie di resilienza per garantire comunque il corretto svolgimento dei processi elettorali. Gli organismi di amministrazione elettorale in molti paesi stanno infatti elaborando piani d'emergenza per assicurare il diritto di voto anche in condizioni avverse. Tra le misure adottate o proposte vi sono:

---

4 Coeckelbergh, M., & Sætra, H. S. (2023). *Democracy, AI and Climate Change: A Delicate Balance. Philosophy & Technology*. Gli autori analizzano la tensione tra governance tecnocratica e partecipazione democratica nella risposta alla crisi climatica, sostenendo che l'uso dell'IA può sia rafforzare sia indebolire la legittimità democratica a seconda delle modalità di implementazione e inclusione dei cittadini.

5 United Nations Office for Disaster Risk Reduction (UNDRR). (2024). *Global Assessment Report on Disaster Risk Reduction*; CRED–EM-DAT, *International Disaster Database*, aggiornamenti 2024. Le fonti mostrano che il numero di disastri climatici è quasi triplicato negli ultimi quarant'anni e documentano interferenze dirette di eventi estremi con processi elettorali in numerosi Paesi nel solo anno 2024.

6 Intergovernmental Panel on Climate Change (IPCC). (2023). *Sixth Assessment Report – Synthesis Report*. Il rapporto conferma che il riscaldamento globale antropogenico aumenta la frequenza e l'intensità degli eventi climatici estremi, con impatti sistemici su infrastrutture critiche, governance e stabilità sociale, inclusi i processi democratici.

– lo spostamento dei seggi verso aree non colpite dalle calamità;
– l'estensione del periodo di votazione;
– il ricorso al voto postale;
– l'implementazione di sistemi di voto elettronico a distanza.

L'idea di fondo è fare in modo che, anche durante calamità eccezionali, la voce degli elettori possa comunque esprimersi e la transizione dei poteri avvenga secondo le regole democratiche prestabilite. Ogni adattamento comporta però interrogativi normativi e organizzativi. Ad esempio, posporre un'elezione per motivi climatici può intaccarne la legittimità? Quali soglie stabiliscono quando un evento giustifica misure straordinarie? E come evitare che regimi autoritari sfruttino strumentalmente l'emergenza climatica per restringere gli spazi democratici?

Le calamità climatiche estreme possono anche alterare le dinamiche della partecipazione e del consenso politico. Diversi studi hanno evidenziato che i disastri naturali possono incidere sul tasso di affluenza alle urne e perfino orientare le preferenze elettorali dei cittadini colpiti. Ad esempio, un uragano devastante poco prima di un'elezione tende a ridurre l'affluenza alle urne nelle zone interessate e, in certi casi, può erodere la fiducia nell'efficacia delle istituzioni, con effetti a lungo termine sul coinvolgimento civico. D'altra parte, l'esperienza diretta di eventi estremi potrebbe galvanizzare la richiesta di una maggiore azione politica sul clima, creando nuove linee di frattura nell'arena democratica: le comunità duramente colpite dai disastri potrebbero finire per premiare alle urne i candidati che propongono programmi più incisivi di adattamento e mitigazione ambientale. In ogni caso, la crescente variabilità del clima aggiunge un ulteriore livello di complessità alla già delicata relazione tra la società civile e le istituzioni rappresentative.

Alla luce di queste sfide, alcuni esperti propongono di ripensare i meccanismi della partecipazione democratica affinché risultino più agili e inclusivi durante le emergenze climatiche. Strumenti di democrazia digitale potrebbero offrire soluzioni aggiuntive: piattaforme online per il dibattito pubblico, referendum deliberativi su scelte ambientali urgenti, oppure sistemi di voto flessibili capaci di coinvolgere gli elettori anche quando le procedure tradizionali risultano impraticabili. In questa prospettiva torna centrale anche il ruolo dell'IA: se utilizzata correttamente, l'IA potrebbe facilitare la rapida raccolta e analisi dei bisogni e delle preferenze dei cittadini in situazioni d'emergenza, fornendo dati utili a decisioni più tempestive. Alcuni autori suggeriscono, ad esempio, che piattaforme digitali potenziate dall'intelligenza artificiale possano abilitare forme di partecipazione "dal basso" ampie e continuative, offrendo quella legittimazione popolare necessaria per adottare in modo più rapido ed efficace misure

drastiche a favore della transizione ecologica[7]. Tuttavia, tali visioni, per quanto promettenti, presuppongono alcune condizioni imprescindibili: è necessario che l'accesso alle tecnologie digitali sia realmente universale, che l'alfabetizzazione digitale sia diffusa e inclusiva e che vengano adottate adeguate garanzie affinché l'introduzione di nuovi strumenti non generi ulteriori disuguaglianze né favorisca distorsioni informative. In assenza di queste tutele, l'innovazione rischierebbe di aggravare le disparità esistenti (o crearne di nuove), tradendo l'obiettivo di rafforzare la democrazia di fronte alla crisi climatica.

11.4 Conclusioni

La convergenza tra intelligenza artificiale, crisi climatica e innovazione nei processi di voto delinea uno scenario in cui tecnologia e democrazia appaiono strettamente intrecciate. Da quanto esposto emergono alcune considerazioni chiave.

In primo luogo, l'IA si conferma uno strumento indispensabile per affrontare la complessità della crisi climatica, a condizione che il suo impiego avvenga in modo responsabile e con attenzione agli effetti collaterali. Ciò significa bilanciare l'entusiasmo per le soluzioni algoritmiche con una valutazione critica della loro impronta ecologica e delle implicazioni in termini di equità sociale. Gli algoritmi possono certamente aiutare a progettare politiche climatiche più efficaci e a mobilitare la partecipazione dei cittadini, ma non devono sostituire il processo deliberativo né tradursi in una tecnocrazia calata dall'alto. Il dilemma tra rapidità d'azione e inclusività democratica può essere superato sfruttando l'IA per ampliare – anziché limitare – la sfera della partecipazione informata. Del resto, alcune iniziative di governance innovativa mostrano che è possibile congegnare strumenti digitali capaci di garantire al tempo stesso decisioni rapide e legittimazione "dal basso", a beneficio di politiche climatiche più robuste e condivise[8].

In secondo luogo, l'aggravarsi dei fenomeni climatici estremi impone alle democrazie un'evoluzione istituzionale e procedurale. La resilienza dei sistemi elettorali è ormai parte integrante della capacità di una società di fronteggiare i cambiamenti climatici. Garantire elezioni libere e regolari anche sotto la minaccia di disastri richiede investimenti in pianificazione, infrastrutture e forse persino nuovi paradigmi di voto. Il voto elettronico rappresenta, in particolare, una delle possibili risposte: esso promette maggiore flessibilità operativa in

7 Dryzek, J. S., Bächtiger, A., Chambers, S., Cohen, J., Druckman, J. N., Felicetti, A., Fishkin, J. S., Farrell, D. M., Fung, A., Gutmann, A., Landemore, H., Mansbridge, J., & Warren, M. E. (2019); aggiornamenti e applicazioni 2022–2024 sulla democrazia deliberativa digitale. Gli autori sostengono che piattaforme digitali e strumenti deliberativi, anche potenziati dall'IA, possano rafforzare la partecipazione "dal basso" e fornire legittimazione democratica a decisioni rapide in contesti di crisi, a condizione di garantire inclusività, trasparenza e accesso equo.

8 Ibidem, p. 148

situazioni di crisi, ma al contempo solleva interrogativi sulla sicurezza, la trasparenza e l'accessibilità che non possono essere ignorati. L'adozione su larga scala di sistemi di e-voting dovrà avvenire in modo graduale, testando rigorosamente sul campo l'efficacia delle soluzioni tecniche e organizzative, e coinvolgendo sia esperti indipendenti sia la cittadinanza in un dialogo aperto sulle implicazioni. Solo così sarà possibile costruire la fiducia necessaria attorno a questi strumenti, prevenendo il rischio che timori legittimi (di frodi o malfunzionamenti) degenerino in una rinnovata sfiducia verso le istituzioni.

In definitiva, le sfide epocali del XXI secolo, dalla rivoluzione digitale all'emergenza climatica, richiedono risposte integrate. L'intelligenza artificiale e il voto elettronico non sono panacee, ma costituiscono tasselli di un mosaico più ampio di innovazione socio-tecnologica che, se ben governato, può rafforzare la capacità delle democrazie di sopravvivere e prosperare in condizioni inedite. La chiave di volta sarà mantenere al centro i principi fondanti della democrazia, ovvero inclusione, trasparenza, responsabilità, mentre si sperimentano anche nuovi strumenti. Solo rispettando tali princìpi l'adozione di tecnologie avanzate potrà tradursi in un effettivo progresso civico e non in un ulteriore fattore di rischio. In questo senso, il successo non si misurerà semplicemente in base all'efficienza tecnologica, ma dalla capacità di tali innovazioni di consolidare la fiducia pubblica e di contribuire a decisioni collettive più lungimiranti, eque e sostenibili.

PARTE VI
CONCLUSIONI E RACCOMANDAZIONI PER IL FUTURO

Capitolo 12
Conclusioni, raccomandazioni operative e agenda di ricerca

12.1 Sintesi dei risultati e contributi principali

Lo studio condotto mette in luce come l'intreccio tra intelligenza artificiale (IA) e sistemi di voto elettronico rappresenti una frontiera cruciale per le democrazie contemporanee. Dall'analisi svolta emergono due facce complementari di questa convergenza tecnologica. Da un lato, l'IA offre strumenti senza precedenti per rafforzare la sicurezza, l'affidabilità e perfino l'accessibilità dei processi elettorali: algoritmi avanzati possono sorvegliare reti e dispositivi in tempo reale, rilevando irregolarità o intrusioni invisibili all'occhio umano; sistemi di machine learning possono aiutare a smascherare tentativi di frode o manomissione analizzando enormi moli di dati eterogenei più rapidamente di qualsiasi team manuale; soluzioni automatizzate possono persino supportare elettori con disabilità o barriere linguistiche, migliorando l'inclusività del voto digitale. Esperienze concrete dimostrano infatti che l'uso combinato di grandi banche dati elettorali digitali e algoritmi di IA ben progettati possono ridurre le possibilità di frodi, ad esempio eliminando elettori fittizi o registrazioni doppie e permette di identificare tempestivamente discrepanze o anomalie, così da intervenire immediatamente a tutela dell'integrità del voto. Dall'altro lato, tuttavia, l'IA introduce nuove sfide e vulnerabilità che non possono essere ignorate: strumenti di deep learning addestrati su dati di parte possono introdurre bìas nell'amministrazione elettorale; sistemi decisionali opachi rischiano di minare la trasparenza del processo di voto; soprattutto, attori ostili possono sfruttare le stesse capacità dell'IA per fini malevoli. Si pensi alla generazione automatica di deepfake e campagne di disinformazione su larga scala, alla proliferazione di bot e profili falsi per manipolare l'opinione pubblica, o ancora all'uso di algoritmi per sferrare attacchi informatici più sofisticati e mirati.

Come evidenziato anche da agenzie specializzate, l'IA generativa di nuova generazione non crea minacce del tutto inedite, ma amplifica pericolosamente i rischi esistenti, abbassando le barriere di costo e competenza richieste per diffondere contenuti falsi o lanciare cyber-attacchi[1]. In sintesi, l'impatto dell'IA sul

1 Agenzie di cybersecurity e governance del rischio hanno descritto l'intelligenza artificiale generativa come un *threat multiplier*, ossia un fattore di amplificazione delle minacce esistenti, in grado di ridurre drasticamente i costi, le competenze tecniche e i tempi necessari per condurre operazioni di disinformazione, social engineering e attacchi informatici sofisticati.

voto elettronico si delinea come un delicato equilibrio tra opportunità rivoluzionarie e rischi emergenti: un "acceleratore" che può tanto potenziare quanto compromettere i processi democratici, a seconda di come verrà gestito.

Un risultato centrale di questa ricerca è la conferma che i sistemi di e-voting potenziati dall'IA vanno considerati a tutti gli effetti infrastrutture critiche della società dell'informazione[2]. Analogamente a quanto accade per il settore energetico o finanziario, la sicurezza e resilienza delle piattaforme di voto digitali non sono più un tema meramente tecnico, bensì una componente essenziale della tenuta democratica, specialmente nell'epoca delle crisi globali. Le analisi delle best practice internazionali evidenziano infatti la necessità di un cambio di paradigma: passare da un approccio reattivo, in cui ci si limita a mitigare i singoli incidenti, a una strategia proattiva e sistemica, che integri l'IA nella governance complessiva del rischio elettorale. In quest'ottica, i risultati ottenuti supportano l'idea che ogni introduzione di IA nel processo di voto debba essere valutata alla luce dei principi fondanti della democrazia, vale a dire segretezza, integrità, trasparenza e verificabilità del voto, assicurando al contempo la neutralità tecnologica (ovvero che l'uso di nuove tecnologie non alteri i requisiti democratici sostanziali). Questo significa, ad esempio, che un algoritmo di rilevazione delle frodi non dovrebbe mai intaccare la segretezza del voto né introdurre discriminazioni o distorsioni, pena la violazione degli standard internazionali vigenti. Ugualmente, qualsiasi guadagno di efficienza apportato dall'IA non può andare a scapito del controllo umano e della responsabilità: gli strumenti algoritmici devono restare al servizio delle istituzioni elettorali e dei cittadini, e non viceversa. Solo mantenendo centrali tali princìpi sarà possibile conciliare innovazione tecnologica ed esigenze democratiche, evitando che l'adozione dell'IA si traduca in un'erosione della fiducia pubblica. A sostegno di ciò, organismi internazionali come l'OSCE e il Consiglio d'Europa hanno esplicitamente sottolineato l'urgenza di bilanciare innovazione e diritti democratici, fornendo linee guida su come implementare l'IA in modo etico nel ciclo elettorale[3]. Tali raccomanda-

---

In particolare, report di CISA, ENISA e del World Economic Forum evidenziano come l'IA consenta la scalabilità industriale di attività malevole già note, aumentando la frequenza, la personalizzazione e la difficoltà di attribuzione degli attacchi, con implicazioni dirette per la sicurezza dei processi elettorali digitali.

2 La qualificazione dei sistemi elettorali digitali come infrastrutture critiche è ormai condivisa nella letteratura sulla sicurezza nazionale e sulla resilienza democratica. Studi accademici e documenti istituzionali sottolineano che l'indisponibilità, la compromissione o la perdita di fiducia nei sistemi di voto può produrre effetti sistemici comparabili a quelli di attacchi contro settori come energia, finanza o telecomunicazioni. In tale prospettiva, la sicurezza elettorale è considerata parte integrante della sicurezza nazionale e della continuità costituzionale dello Stato, specialmente in contesti di crisi globale.

3 L'OSCE/ODIHR e il Consiglio d'Europa hanno ribadito, in numerosi documenti di soft law e linee guida tecniche, che l'introduzione di tecnologie digitali avanzate – incluse soluzioni basate su intelligenza artificiale – nel ciclo elettorale deve avvenire nel rispetto dei principi fondamentali delle elezioni democratiche, quali universalità, uguaglianza, libertà, segretezza e

zioni convergono sul fatto che i benefici dell'IA devono essere perseguiti senza compromessi sui valori democratici: l'IA può certamente potenziare la fase di "Detect" delle minacce (individuando intrusioni o anomalie prima impensabili), ma va inserita in un solido contesto di gestione del rischio e scrutinata con eguale rigore delle componenti tradizionali. In definitiva, dunque, questa ricerca conferma che "IA + voto elettronico" non è di per sé né un toccasana né un pericolo inevitabile, ma uno degli ingranaggi chiave di un più ampio mosaico socio-tecnologico che, se ben governato, potrà rafforzare la capacità delle democrazie di sopravvivere e prosperare anche nelle condizioni più critiche.

12.2 Raccomandazioni pratiche

Alla luce delle evidenze emerse, è possibile delineare alcune raccomandazioni operative per implementare in modo responsabile l'IA nei sistemi di voto elettronico, massimizzandone i benefici e minimizzandone i rischi. In primo luogo, si raccomanda di adottare un approccio di "security by design", integrando fin dall'inizio l'IA in architetture di voto progettate per essere sicure, trasparenti e verificabili. Ogni componente basata su IA dovrebbe essere sviluppata e inserita nel sistema elettorale seguendo standard rigorosi di qualità del software, testing e certificazione indipendente. In particolare, risulta fondamentale sottoporre gli algoritmi a verifiche continue e audit esterni, sia prima sia durante il loro impiego in elezioni reali, in modo da convalidarne le prestazioni e individuare tempestivamente eventuali malfunzionamenti o derive indesiderate. Benchmark periodici, esercitazioni di "red teaming" (in cui esperti simulano attacchi sia convenzionali sia basati su IA) e analisi indipendenti del codice algoritmico dovrebbero divenire prassi corrente per le autorità elettorali, così da anticipare le vulnerabilità anziché scoprirle a danno fatto. In secondo luogo, è necessario implementare misure di sicurezza multilivello che abbinino strumenti tradizionali e IA: ad esempio, affiancare ai controlli crittografici e ai protocolli di sicurezza propri del voto elettronico anche sistemi di monitoraggio AI-driven in grado di sorvegliare il ciclo elettorale end-to-end (dalla registrazione degli elettori allo spoglio elettronico), segnalando anomalie in tempo reale. Tali sistemi intelligenti di allarme precoce – già sperimentati in alcuni contesti – possono fungere da scudo attivo contro attacchi informatici e tentativi di broglio sofisticati, purché siano sviluppati con adeguate garanzie di affidabilità e precisione. A tal proposito, occorre evitare tanto i falsi negativi (cioè il mancato riconoscimento di un'intrusione reale) quanto i falsi positivi (allarmi ingiustificati che potrebbero ingenerare panico o sfiducia nel processo elettorale). Si tratta di un equilibrio

trasparenza del voto. In particolare, la Raccomandazione CM/Rec(2017)5 del Consiglio d'Europa e i manuali OSCE sull'uso delle ICT nelle elezioni insistono sulla necessità di neutralità tecnologica, verificabilità indipendente, supervisione umana e accountability istituzionale.

delicato: per mantenerlo, raccomandiamo di potenziare la cooperazione con enti di standardizzazione e sicurezza informatica (come l'ENISA a livello europeo e le analoghe agenzie nazionali), affinché vengano emanate linee guida tecniche specifiche per l'affidabilità degli algoritmi elettorali. Ciò includerà probabilmente requisiti stringenti su aspetti come la robustezza agli attacchi adversariali, la capacità di spiegare le proprie decisioni (explainability) e la tutela dei dati sensibili trattati. In terzo luogo, sul piano organizzativo e di policy, si suggerisce di aggiornare i quadri normativi esistenti tenendo conto della rapida evoluzione dell'IA. Normative generali come il regolamento europeo sull'IA (AI Act) dovranno essere declinate in standard settoriali specifici per il dominio elettorale, classificando ad esempio gli algoritmi di supporto al voto come sistemi ad alto rischio e imponendo requisiti di trasparenza, valutazione d'impatto e supervisione umana obbligatori[4]. Parallelamente, gli organismi di vigilanza elettorale potrebbero istituire comitati tecnico-etici incaricati di valutare caso per caso l'introduzione di nuove soluzioni AI nelle elezioni, assicurando che ogni innovazione sia allineata con i principi democratici e che vi sia consenso informato da parte della collettività sul suo utilizzo. Da ultimo, ma non meno importante, vanno promossi programmi di formazione specifica per tutti gli attori coinvolti nel processo elettorale – dai funzionari pubblici ai membri dei seggi, fino agli osservatori indipendenti – affinché acquisiscano competenza digitale e familiarità sia con le opportunità offerte dall'IA sia con i relativi rischi. Una migliore alfabetizzazione tecnologica del personale elettorale e dei cittadini è infatti una precondizione indispensabile per implementare soluzioni di IA in modo consapevole e condiviso, evitando misunderstanding e alimentando la fiducia pubblica nel fatto che l'innovazione sia guidata dal bene comune.

12.3 Direttrici di ricerca futura

Oltre alle raccomandazioni pratiche sopradescritte, questa ricerca evidenzia importanti lacune teoriche e apre nuove prospettive scientifiche che meritano di essere esplorate con urgenza in futuro. Un primo filone di studio riguarda la robustezza algoritmica e la resilienza agli attacchi adversariali. Come discusso, gli algoritmi di IA impiegati in ambito elettorale potrebbero diventare essi stessi bersaglio di manipolazioni: ad esempio, inserendo input artefatti, un aggressore potrebbe cercare di ingannare un sistema di monitoraggio automatico

4 Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale adotta un approccio basato sul rischio e classifica come *high-risk* i sistemi di IA suscettibili di incidere su diritti fondamentali e processi democratici. Sebbene il testo non disciplini in modo esaustivo il voto elettronico, le sue disposizioni su valutazione d'impatto, gestione del rischio, trasparenza, tracciabilità e controllo umano risultano direttamente applicabili alle tecnologie IA utilizzate in ambito elettorale. La dottrina converge sulla necessità di una declinazione settoriale dell'AI Act per le elezioni, integrata con strumenti già esistenti come la DPIA prevista dal GDPR, al fine di garantire una governance algoritmica conforme ai principi costituzionali e democratici.

affinché non rilevi una frode reale, oppure al contrario generi falsi allarmi. Al momento questi rischi restano in gran parte teorici, ma la rapida evoluzione delle tecniche di adversarial machine learning impone di non abbassare la guardia. Raccomandiamo quindi di sviluppare ulteriormente la ricerca su metodologie di difesa avanzate, quali l'adversarial training (addestramento dei modelli basato su esempi di attacco per aumentarne l'immunità) e l'implementazione di strati di calibrazione capaci di filtrare o attenuare l'effetto di input maligni. Parallelamente, sarà strategico studiare sistemi di validazione incrociata e monitoring continuo dei modelli durante il loro impiego sul campo, magari attraverso architetture meta-AI che sorveglino il comportamento dell'IA primaria e ne segnalino eventuali deviazioni.

Un secondo ambito di ricerca prioritario concerne la lotta alla disinformazione algoritmica e la tutela dell'informazione elettorale nell'era dell'IA generativa. Si rendono necessari approcci innovativi per individuare e contrastare in tempo reale la diffusione di fake news, video deepfake e altri artefatti sintetici che mirano a manipolare l'elettorato. Ciò potrà includere lo sviluppo di algoritmi di rilevazione multimediale in grado di autenticare le fonti e verificare l'integrità dei contenuti online (eventualmente facendo ricorso anche a tecnologie ausiliarie come la blockchain per tracciare la provenienza dei media digitali). Allo stesso tempo, serviranno studi interdisciplinari per definire confini e regole d'ingaggio chiari nell'uso di IA contro la disinformazione: è cruciale evitare che le contromisure algoritmiche sconfinino nella censura o ledano il pluralismo informativo.

Un terzo asse di ricerca riguarda l'ingegneria dei sistemi di voto di nuova generazione, ovvero la progettazione di piattaforme elettorali che sin dall'inizio integrino meccanismi di garanzia algoritmica. Questo implica esplorare nuove architetture in cui elementi come la trasparenza algoritmica, l'auditabilità end-to-end e la privacy differenziale siano incorporati *by-design*: ad esempio, sistemi di e-voting che rendano esplicabili (*explainable*) le decisioni prese dall'IA nel processo (come la segnalazione di un'anomalia) attraverso appositi moduli di spiegazione comprensibili agli operatori umani; oppure implementazioni che utilizzino tecniche crittografiche avanzate per consentire verifiche indipendenti dei risultati generati dall'IA senza rivelare informazioni sensibili degli elettori. Su questo fronte, un elemento chiave sarà lo sviluppo di metriche e protocolli di valutazione specifici per le performance dell'IA elettorale: non solo in termini di accuratezza tecnica, ma anche di impatto sociale, ad esempio misurando il grado di fiducia che utenti e osservatori ripongono nel sistema oppure gli eventuali bias residui. Ulteriori ricerche potranno indagare come l'IA possa promuovere la partecipazione democratica in modi nuovi, andando oltre la semplice sicurezza: si pensi a assistenti virtuali in grado di aiutare gli elettori a comprendere meglio candidati e programmi (con le dovute cautele per garantirne la neutralità), o a piattaforme deliberative online potenziate dall'IA per facilitare consultazioni pubbliche rapide in situazioni di emergenza.

Infine, ma in prospettiva non meno rilevante, occorre approfondire il rapporto tra tecnologia, contesto di crisi e diritti politici: le crisi globali (pandemie, conflitti, calamità climatiche) diventeranno con ogni probabilità sempre più frequenti, e la ricerca scientifica dovrà interrogarsi su come predisporre sistemi elettorali resilienti che sfruttino l'IA per garantire continuità istituzionale senza compromettere la legittimità del voto. Ciò potrebbe tradursi nell'elaborazione di modelli predittivi in grado di simulare diversi scenari di crisi e il loro impatto sullo svolgimento di elezioni, aiutando i decisori a pianificare le soluzioni in anticipo (ad esempio stimando l'affluenza in caso di voto online forzato da un lockdown o identificando i punti deboli di un'infrastruttura elettorale sotto attacco mirato). In sintesi, l'agenda di ricerca futura dovrà essere marcatamente interdisciplinare e innovativa, coinvolgendo informatici, esperti di sicurezza, giuristi, politologi e sociologi in uno sforzo comune per ripensare le elezioni nell'era dell'IA. Colmare questi gap teorici non sarà solo un esercizio accademico, ma avrà ricadute pratiche dirette: significherà dotare le democrazie degli strumenti concettuali e tecnologici necessari per anticipare le sfide di domani, anziché subirle passivamente.

In conclusione, l'impatto dell'intelligenza artificiale sui sistemi di voto elettronico nell'epoca delle crisi globali dipenderà in larga misura da come sapremo governare questa transizione. Le evidenze raccolte indicano che non siamo di fronte a un destino già scritto: il futuro è plasmabile tramite le scelte strategiche che verranno compiute oggi da ricercatori, policy-maker e operatori del settore. Un'implementazione oculata e responsabile dell'IA potrà rafforzare la resilienza democratica, garantendo elezioni più sicure, inclusive e adattabili anche in contesti avversi; al contrario, un'adozione frettolosa o priva di adeguate salvaguardie potrebbe acuire le vulnerabilità esistenti e alimentare nuove forme di sfiducia istituzionale. È pertanto essenziale proseguire sulla strada tracciata da questo lavoro, adottando una visione programmatica di lungo periodo: investire in ricerca e innovazione aperta, elaborare standard condivisi e regolamentazioni lungimiranti, sperimentare soluzioni pilota in ambienti controllati, diffondere consapevolezza tra gli addetti ai lavori e nel pubblico. Solo attraverso un approccio integrato sarà possibile fare in modo che l'IA e il voto elettronico – invece di rappresentare una minaccia – diventino un baluardo a tutela della democrazia nell'era delle crisi globali. Le raccomandazioni e le direttrici di ricerca delineate in questa conclusione mirano proprio a questo obiettivo: offrire spunti originali e concreti per guidare la comunità scientifica e i decisori verso soluzioni che coniughino tecnologia e valori democratici.

La sfida è di quelle che mettono alla prova la tenuta delle democrazie, ma altrettanto grandi sono le opportunità di avanzamento civile che essa dischiude. Se i principi fondanti della democrazia continueranno a fungere da stella polare nell'orientare l'innovazione tecnologica, l'intelligenza artificiale potrà davvero diventare un alleato strutturale di elezioni più solide, inclusive e lungimiranti, capaci di traghettare le nostre società attraverso le tempeste complesse e interconnesse del XXI secolo.

Bibliografia essenziale

Opere accademiche, monografie e volumi scientifici

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2008). *Electronic Voting and the Transformation of Democracy*. Cambridge University Press.

Alvarez, R. M., Levin, I., & Li, H. (2019). Election administration and the new institutionalism. *Election Law Journal*, 18(2), 122–135.

Anderson, R. (2020). *Security Engineering* (3rd ed.). Wiley.

Athiwaratkun, B., Chen, C. A., Kang, J., et al. (2023). Large language models for cybersecurity: Opportunities, challenges, and limitations. *arXiv preprint*.

Baldwin, D. A. (2016). *Power and International Relations*. Princeton University Press.

Barber, B. R. (2003). *Strong Democracy: Participatory Politics for a New Age*. University of California Press.

Bennett, C. J., & Lyon, D. (2019). Data-driven elections and democratic accountability. *Surveillance & Society*, 17(1/2), 1–15.

Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, 31(4), 543–556.

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Bommasani, R., Hudson, D. A., Adeli, E., et al. (2022). *On the Opportunities and Risks of Foundation Models*. Stanford Center for Research on Foundation Models.

Borgesius, F. Z., et al. (2018). *Online Political Microtargeting*. University of Amsterdam Institute for Information Law.

Brundage, M., et al. (2018). *The Malicious Use of Artificial Intelligence*. Oxford University Press.

Brundage, M., Avin, S., Clark, J., et al. (2020). *Toward Trustworthy AI Development*. arXiv preprint.

Buchanan, B. (2020). *The Hacker and the State*. Harvard University Press.

Carlini, N., Jagielski, M., Oprea, A., et al. (2023). Poisoning web-scale training datasets is practical. *IEEE Symposium on Security and Privacy*.

Casey, E. (2011). *Digital Evidence and Computer Crime*. Academic Press.

Castells, M. (2012). *Networks of Outrage and Hope*. Polity Press.

Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

Coeckelbergh, M. (2020). *AI Ethics*. MIT Press.

Coeckelbergh, M., & Sætra, H. S. (2023). Democracy, AI and climate governance. *AI & Society*, 38(2), 457–471.

Crawford, K. (2021). *Atlas of AI*. Yale University Press.

Dryzek, J. S., et al. (2019). *The Crisis of Democracy and the Science of Deliberation*. Oxford University Press.

European Commission Joint Research Centre (JRC). (2023). *Cybersecurity of Electronic Voting Systems*. Publications Office of the European Union.

Ferrara, E., et al. (2016). The rise of social bots. *Communications of the ACM*, 59(7), 96–104.

Floridi, L. (2014). *The Fourth Revolution*. Oxford University Press.

Floridi, L. (2023). *Ethics, Governance, and Policies for AI*. Springer.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the ACM Symposium on Theory of Computing*.

Gibson, R. (2010). Studying the effects of internet voting. *International Political Science Review*, 31(3), 275–296.

Gibson, R., Cantijoch, M., & Ward, S. (2020). *Digital Campaigning*. Oxford University Press.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Goodfellow, I. J., et al. (2015). Explaining and harnessing adversarial examples. *International Conference on Learning Representations*.

Gritzalis, D. (2002). Secure electronic voting. *Advances in Computers*, 57, 255–289.

Halderman, J. A. (2016). Practical attacks on real-world voting machines. *Communications of the ACM*, 59(7), 86–94.

Halderman, J. A. (2022). The Antrim County 2020 election incident. *USENIX Security Symposium*.

Howard, P. N. (2020). *Lie Machines*. Yale University Press.

Jankowicz, N. (2020). *How to Lose the Information War*. I. B. Tauris.

Kitchin, R. (2014). *The Data Revolution*. SAGE.

Kshetri, N., & Voas, J. (2017). Blockchain-enabled e-voting. *IEEE Computer*, 50(11), 95–99.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Madry, A., et al. (2018). Towards deep learning models resistant to adversarial attacks. *International Conference on Learning Representations*.

Mebane, W. R. (2013). Election forensics. In *The State of Election Forensics*. Cambridge University Press.

Morozov, E. (2013). *To Save Everything, Click Here*. PublicAffairs.

National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the Vote*. National Academies Press.

Nissenbaum, H. (2010). *Privacy in Context*. Stanford University Press.

Noble, S. U. (2018). *Algorithms of Oppression*. NYU Press.

O'Neil, C. (2016). *Weapons of Math Destruction*. Crown Publishing.

Ohlin, J. D. (2015). *The Law of Cyber Warfare*. Oxford University Press.

Park, S., et al. (2021). Going from bad to worse: From internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1).

Rivest, R. L., & Wack, J. P. (2006). Software independence in voting systems. MIT CSAIL Technical Report.

Rolnick, D., et al. (2022). Tackling climate change with machine learning. *ACM Computing Surveys*, 55(2).

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Schneier, B. (2018). *Click Here to Kill Everybody*. W. W. Norton.

Schneier, B. (2019). Election security: Threats and solutions. *IEEE Security & Privacy*, 17(1), 88–92.

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning. *Proceedings of ACL*.

Sunstein, C. R. (2017). *#Republic*. Princeton University Press.

Tufekci, Z. (2017). *Twitter and Tear Gas*. Yale University Press.

Woolley, S. C., & Howard, P. N. (2018). *Computational Propaganda*. Oxford University Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

Rapporti istituzionali, policy paper e standard internazionali

Council of Europe (2004). *Recommendation Rec(2004)11 on Legal, Operational and Technical Standards for E-Voting*.

Council of Europe (2017). *Recommendation CM/Rec(2017)5 on Standards for E-Voting*.

Council of Europe (2022). *Guidelines on the Use of ICT in Electoral Processes*.

Council of Europe (2023). *Bern Conference Declaration on Electoral Integrity in Times of Crisis*.

Council of Europe – Venice Commission (2020). *Principles for the Use of Digital Technologies in Elections*.

ENISA (2019). *Cybersecurity in Elections*.

ENISA (2020). *Cybersecurity Threat Landscape for Elections*.

ENISA (2023). *Artificial Intelligence and Cybersecurity*.

European Commission (2021). *2030 Digital Compass*.

European Commission (2022). *Strengthened Code of Practice on Disinformation*.

European Union (2022). Regulation (EU) 2022/2065 – *Digital Services Act*.

European Union (2024). Regulation (EU) 2024/1689 – *Artificial Intelligence Act*.

European Union (2024). Regulation (EU) 2024/900 – *Transparency and Targeting of Political Advertising*.

International IDEA (2020). *Elections and COVID-19*.

International IDEA (2023). *Elections During Crises*.

NATO (2023). *Cognitive Warfare and Hybrid Threats*.

NIST (2018). *Cybersecurity Framework*.

NIST (2023). *AI Risk Management Framework*.

OSCE/ODIHR (2020). *Election Observation and New Technologies*.

OSCE/ODIHR (2024). *Handbook on the Observation of Digital Technologies in Elections*.

World Economic Forum (2023). *Global Risks Report*.

World Economic Forum (2024). *Governing AI for Humanity*.

Diritto internazionale, cyber warfare e digital forensics

Boothby, W. H. (2018). *The Law of Targeting*. Oxford University Press.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Council of Europe (2001). *Convention on Cybercrime (Budapest Convention)*.

Council of Europe (2017). *Recommendation CM/Rec(2017)5 on Standards for E-Voting*.

Council of Europe (2022). *Second Additional Protocol to the Budapest Convention on Enhanced Cooperation and Disclosure of Electronic Evidence*.

Council of Europe (2023). *Guidelines on Addressing the Impact of Artificial Intelligence on Electoral Processes*.

Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press.

Gill, T. D., Fleck, D., & Boothby, W. (2020). *The Handbook of the International Law of Military Operations*. Oxford University Press.

Greenberg, A. (2021). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

ICRC (2020). *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*.

ICRC (2022). *International Humanitarian Law and Cyber Operations during Armed Conflicts*.

ICRC (2023). *Digital Risks and Civilian Protection*.

Kerr, O. S. (2021). *Computer Crime Law*. West Academic Publishing.

NATO Cooperative Cyber Defence Centre of Excellence (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

NATO Cooperative Cyber Defence Centre of Excellence (2021). *International Cyber Norms and Democratic Security*.

NATO Cooperative Cyber Defence Centre of Excellence (2023). *Cyber Operations and Democratic Resilience*.

Ohlin, J. D. (2015). *The Law of Cyber Warfare*. Oxford University Press.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

United Nations (2021). *Report of the Secretary-General on Electoral Assistance*.

United Nations (2022). *Information Integrity on Digital Platforms*.

United Nations (2023). *Report of the Secretary-General: Artificial Intelligence and Human Rights*.

United Nations Office on Drugs and Crime (UNODC) (2023). *Cybercrime and Electronic Evidence in Criminal Investigations*.

Venice Commission (2020). *Principles for the Use of Digital Technologies in Electoral Processes*.

Venice Commission (2022). *Guidelines on the Impact of Digital Technologies on Democracy and Elections*.

Disinformazione, deepfake, guerra ibrida e sicurezza cognitiva

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Bradshaw, S., & Howard, P. N. (2019). *The Global Disinformation Order*. Oxford Internet Institute.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753–1819.

Derakhshan, H., & Wardle, C. (2017). *Information Disorder: Toward an Interdisciplinary Framework*. Council of Europe.

Farid, H. (2019). *Photo Forensics*. MIT Press.

Farid, H. (2022). *Fake Photos*. MIT Press.

Garton Ash, T. (2024). *The Defence of Democracy in the Age of AI*. Oxford University Press.

Howard, P. N. (2020). *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press.

Kremlin Watch Programme (2023). *Cognitive Warfare and Electoral Manipulation in Europe*. European Values Center for Security Policy.

Marwick, A., & Lewis, R. (2017). *Media Manipulation and Disinformation Online*. Data & Society Research Institute.

NATO Strategic Communications Centre of Excellence (2020). *Hybrid Threats: A Strategic Communications Perspective*.

NATO Strategic Communications Centre of Excellence (2023). *Artificial Intelligence and Cognitive Warfare*.

Nyhan, B., & Reifler, J. (2015). Displacing Misinformation about Events. *Journal of Experimental Political Science*, 2(1), 81–93.

Rodenas, I. (2025). *Election Interference in the Age of Hybrid Warfare*. Centre for Youth and International Studies (CYIS).

Starbird, K. (2017). Examining the Alternative Media Ecosystem. *Proceedings of ICWSM*.

Starbird, K. (2023). Disinformation as Collaborative Work. *Journal of Democracy*, 34(3), 102–117.

Sunstein, C. R. (2018). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.

Thompson, J. B. (2020). *Political Scandal: Power and Visibility in the Media Age*. Polity Press.

Wardle, C. (2019). Understanding Information Disorder. *First Draft & Harvard Kennedy School*.

Woolley, S. C., & Howard, P. N. (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SUI SISTEMI DI VOTO ELETTRONICO NELL'EPOCA DELLE CRISI GLOBALI

Federica Bertoni

La monografia analizza l'impatto dell'intelligenza artificiale sui sistemi di voto elettronico, indagandone le ricadute normative, tecniche e istituzionali in contesti di crisi globale. Attraverso una lettura incardinata sul diritto e l'informatica giuridica e integrata da elementi di cybersecurity e digital forensics, l'opera esamina criticamente rischi sistemici, opacità algoritmica, vulnerabilità infrastrutturali e scenari regolatori emergenti. L'analisi, aggiornata al 2025, coniuga rigore normativo e consapevolezza tecnologica.

ISBN 979-12-5510-380-6 (print)
ISBN 979-12-5510-384-4 (PDF)
ISBN 979-12-5510-387-5 (EPUB)
DOI 10.54103/infolawsoc.280