AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2026 **n. 2/ 2026** **febbraio 2026**

La protezione degli spazi pubblici, dalla cronaca alla strategia della resilienza

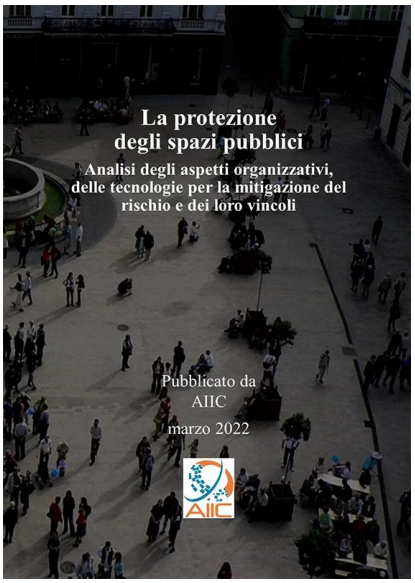
Gli avvenimenti delle ultime settimane hanno rimesso al centro del dibattito nazionale la sicurezza urbana nelle nostre grandi metropoli.
Gli scontri e le tensioni che hanno interessato le città di Milano e Torino si sono concentrati in alcune aree nevralgiche, spesso legate a grandi eventi o a storici presidi antagonisti.
In ambedue i casi, i manifestanti si sono scontrati con la polizia e, oltre alle cariche e all'uso di idranti per disperdere i blocchi stradali che stavano paralizzando il traffico urbano, come risultato di questa guerriglia urbana si sono verificati danneggiamenti significativi agli allestimenti urbani e agli arredi pubblici e privati.
Le zone in cui si sono verificati gli scontri non sono scelte a caso: sono nodi di flusso (stazioni, tangenziali) o simboli istituzionali/economici (piazze storiche, villaggio olimpico) e diventano spesso teatro di tensioni per una combinazione di fattori logistici, simbolici e sociali.
Alcune zone urbane sviluppano nel tempo una sorta di "memoria politica": presenza di centri sociali, reti attiviste radicate, abitudine a ospitare cortei.
A ciò si aggiunge una morfologia urbana favorevole agli scontri: queste zone hanno spesso strade larghe che si restringono, sottopassi, ponti, incroci complessi, numerose vie laterali.
In queste circostanze la polizia può creare sbarramenti, i cortei possono fermarsi o essere bloccati, i gruppi più radicali trovano numerose vie di fuga.
Tutto questo rende più probabile una maggiore concentrazione di manifestanti ed un massiccio presidio da parte delle forze dell'ordine ed il risultato è un maggior rischio di tensione.
In breve, queste aree diventano punti caldi perché uniscono valore simbolico, tradizione di protesta, vicinanza a obiettivi, caratteristiche urbanistiche.

Questi recenti fatti di cronaca legati all'ordine pubblico e alla sicurezza in zone nevralgiche di grandi città sollevano interrogativi cruciali: come possono le nostre piazze rimanere luoghi di aggregazione senza trasformarsi in "aree a rischio"?
Questi eventi non sono isolati, ma rappresentano il sintomo di una necessità più profonda: smettere di considerare lo spazio pubblico solo come arredo urbano e iniziare a trattarlo come una vera e propria ***infrastruttura critica***.
È quindi necessario un cambio di paradigma: la protezione degli spazi pubblici non può più limitarsi al solo presidio fisico delle Forze dell'Ordine ma bisogna andare verso una sicurezza integrata.

È qui che si inserisce il contributo tecnico dell'**AIIC (Associazione Italiana Esperti in Infrastrutture Critiche)**.
Nel suo report "***La protezione degli spazi pubblici: analisi degli aspetti organizzativi, delle tecnologie per la mitigazione del rischio e dei loro vincoli***" (edito a marzo del 2022) l'Associazione sottolinea come le piazze, i nodi di trasporto e i luoghi di grandi eventi debbano essere analizzati attraverso la lente della resilienza.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

La proposta è quella di un ***approccio sistemico e multidisciplinare*** alla sicurezza dei luoghi aperti al pubblico, e in questo senso il report evidenzia come sia necessario:



1. **Riconoscere gli spazi pubblici come infrastrutture critiche**. Gli spazi pubblici – come stazioni ferroviarie, aeroporti, imbarchi portuali, stadi, centri commerciali, piazze e aree urbane di rilevanza sociale – non sono solo luoghi di aggregazione ma anche elementi strutturali essenziali per la vita collettiva. Per questo AIIC li considera parte delle infrastrutture critiche, cioè elementi il cui malfunzionamento o compromissione può avere impatti significativi sulla sicurezza e sulla funzione sociale di un Paese.
2. **Utilizzare tecnologie avanzate per monitoraggio e allerta**. La protezione degli spazi pubblici non deve essere solo fisica, ma anche tecnologica, informativa e organizzativa. Il report esplora come:
   tecnologie digitali (es. sensori IoT) possano raccogliere dati in tempo reale per monitorare flussi di persone e situazioni di rischio;
   una analisi dati avanzata permetta di identificare segnali deboli di potenziali minacce (terrorismo, criminalità, eventi estremi);
   comunicazione pubblica e coinvolgimento dei cittadini aumentino la resilienza delle comunità.
3. **Favorire interoperabilità e cooperazione fra sistemi e istituzioni**. Un concetto chiave è che nessun sistema isolato è sufficiente. Per una protezione efficace:
   i sistemi di sorveglianza devono essere interoperabili tra loro e tra enti diversi (forze dell'ordine, gestione urbana, servizi di emergenza);
   la collaborazione tra istituzioni pubbliche, private e società civile è fondamentale per reagire rapidamente di fronte a condizioni variabili;
   la tecnologia deve essere integrata in un sistema di sicurezza condiviso, non solo installata in singole realtà.
4. **Affrontare gli aspetti etici e di protezione dei dati**. Il report sottolinea le sfide associate all'uso di tecnologie avanzate:
   privacy e protezione dei dati personali devono essere garantite, rispettando normative come il GDPR;
   l'uso di tecnologie come l'IA o il monitoraggio dei dati pubblici comporta rischi etici e di discriminazione se non regolato correttamente;
   è necessario trovare un equilibrio fra sicurezza e libertà civili per non creare spazi monitorati in modo eccessivo.
5. **Investire in formazione tecnica e gestione integrata delle minacce**. La tecnologia da sola non basta, è fondamentale formare personale qualificato in grado di:
   interpretare i dati raccolti;
   integrare strumenti tecnologici nei processi decisionali;
   coordinare risposte operative fra enti diversi durante emergenze.

Questa visione cerca di conciliare efficacia operativa e rispetto delle libertà civili, in un mondo dove la sicurezza urbana richiede risposte dinamiche e tecnologiche.

Oltre il report: le sfide di un mondo che corre

Tuttavia, a quattro anni dalla pubblicazione del report AIIC, è doveroso fare diverse osservazioni e porsi alcune domande.
Anzitutto, la **Direttiva (UE) 2022/2557** (Direttiva CER, recepita in Italia con il D.Lgs. 134/2024) ridefinisce e supera profondamente l'approccio della vecchia Direttiva EPCIP: si tratta di andare oltre la mera protezione delle strutture per puntare su una reale resilienza fisica delle opere strategiche, fondata sulla tenuta complessiva dell'infrastruttura e sulla continuità dei servizi. E per quanto riguarda il settore critico "Trasporti" la sicurezza di alcuni spazi pubblici diventa un prerequisito per la sua resilienza: ad esempio, grandi stazioni ferroviarie o metropolitane, aeroporti, porti sono sia "spazi pubblici" che "soggetti critici" sotto la CER, mentre autostrade e grandi opere viarie strategiche potrebbero esserlo se sono essenziali per l'erogazione di un servizio fondamentale e la loro indisponibilità causerebbe gravi conseguenze sociali, economiche o per la sicurezza.
Il report dell'AIIC già applica questa visione agli spazi pubblici, analizzando come questi luoghi (piazze, stazioni, aree urbane affollate) non siano solo target fisici, ma nodi vitali dove la sicurezza deve essere garantita senza compromettere la fruibilità del servizio pubblico.

Inoltre, il panorama tecnologico del 2022 non è quello odierno.
Sebbene i pilastri del report AIIC restino validi, il biennio 2024-2025 ha introdotto strumenti che allora erano solo teorici: l'esplosione dell'***IA generativa***, il potenziamento del ***deep learning*** per la video-analisi e la diffusione di ***reti 5G*** sempre più capillari hanno spostato l'asticella delle possibilità tecniche. Non parliamo più solo di "sensori", ma di una vera e propria ***intelligenza d'ambiente***. Oggi la tecnologia mette a disposizione:
IA predittiva e analisi dei comportamenti: algoritmi in grado di analizzare i trend sui social media e le dinamiche digitali in tempo reale per prevedere "punti di ebollizione" prima ancora che i manifestanti scendano in strada;
Computer Vision di nuova generazione: sistemi che non si limitano a registrare, ma riconoscono autonomamente comportamenti anomali (come l'abbandono di oggetti o movimenti di folla convulsi) riducendo i tempi di reazione;
Digital twin urbani: modelli 3D dinamici delle città che permettono alle autorità di simulare scenari di crisi, testando l'efficacia di sbarramenti o vie di fuga virtualmente prima di applicarli sul campo.

E contestualmente emergono anche nuove criticità che quattro anni fa erano solo agli albori:
L'efficacia reale dei sensori: in contesti di guerriglia urbana o forti tensioni sociali, quanto possono realmente incidere i dati raccolti in tempo reale se non esiste una capacità di risposta politica e sociale immediata?
Il rischio di "sorveglianza algoritmica": con l'avanzamento tecnologico, il confine tra sicurezza e controllo sociale si è fatto ancora più sottile, rendendo il dibattito etico ancora più urgente rispetto al 2022.
La manutenzione della complessità: sistemi tecnologici avanzati richiedono investimenti costanti e competenze che spesso la pubblica amministrazione fatica a reperire o mantenere.

Purtuttavia, queste "super-tecnologie" aprono paradossi inediti: una piazza tecnologicamente perfetta è davvero una piazza sicura o è solo una piazza sorvegliata? Basta la tecnologia a risolvere il problema? La risposta è, certamente, no. Non è sufficiente aggiornare un software o installare una telecamera con maggiore risoluzione per garantire la sicurezza di una piazza: la tecnologia è uno strumento, non una strategia. Il rischio è che, rincorrendo l'ultima novità tecnica, ci si dimentichi della componente umana.

Per questo, l'approccio dell'AIIC oggi va integrato.
Non basta più il contributo del tecnico delle infrastrutture, forse è giunto il momento di aggiornare quella visione multidisciplinare auspicata da AIIC: la sicurezza delle piazze non può essere delegata solo agli ingegneri o alle forze dell'ordine.
È necessario aprire un tavolo di confronto che includa, oltre alle autorità locali e alle forze dell'ordine:
urbanisti e architetti: per progettare spazi che, per morfologia, scoraggino la violenza senza diventare fortezze;
sociologi e psicologi sociali: per comprendere le dinamiche del dissenso moderno, che spesso nascono online e si scaricano offline, per decodificare perché certi luoghi diventano simboli di scontro e come il design urbano può mitigare la rabbia sociale;
esperti di etica digitale: per garantire che la "sicurezza" non diventi un pretesto per una limitazione permanente delle libertà civili, per stabilire confini invalicabili all'uso di algoritmi predittivi che potrebbero, se non regolati, ledere il diritto costituzionale alla manifestazione.

La sicurezza degli spazi pubblici è una sfida aperta, è il prerequisito della libertà: solo in uno spazio protetto e resiliente la cittadinanza può vivere in pieno la dimensione collettiva. Il report del 2022 ci ha dato le basi, ma oggi serve un passo avanti: non più solo "sicurezza integrata", ma una sicurezza partecipata e consapevole che sappia leggere i cambiamenti sociali prima ancora di quelli tecnologici.
Come ha ricordato recentemente anche l'ex Capo della Polizia **Franco Gabrielli** commentando i fatti di Torino, per la gestione dell'ordine pubblico serve professionalità, addestramento e, soprattutto, una strategia reale che sappia leggere i contesti urbani prima che esplodano. Non si può pretendere che la polizia risolva, da sola e in strada, problemi che nascono da una mancata pianificazione sociale e tecnologica delle città.

Domanda aperta ai lettori
La protezione delle nostre città è un cantiere aperto. La tecnologia ci offre soluzioni sempre più sofisticate, ma la resilienza di una comunità si misura anche nella sua capacità di gestire il conflitto in modo civile, costruendo città capaci di accogliere il dissenso e la protesta senza che questi sfocino sistematicamente nella paralisi o nel danneggiamento del bene comune.
A chi dovremmo affidare la sicurezza delle nostre piazze?
È sufficiente che sia in mano alle Forze dell'Ordine coadiuvate da algoritmi, o è necessario un nuovo "patto di sicurezza" che veda la partecipazione attiva di urbanisti, esperti di etica e degli stessi cittadini?
Invitiamo i nostri lettori, i professionisti del settore, gli esperti di sicurezza, i pianificatori urbani a condividere la propria visione: la sfida della sicurezza urbana è appena iniziata.

Potete inviare i vostri commenti o le vostre idee a segreteria@infrastrutturecritiche.it. Saremo lieti di condividerle.

È possibile consultare il report integrale "La Protezione degli Spazi Pubblici" sul sito ufficiale di AIIC al link https://infrastrutturecritiche.it/wp-content/uploads/2022/03/La-Protezione-degli-Spazi-Pubblici.pdf

Silvano Bari
Docente di Risk Management presso l'Università Campus Bio-medico di Roma

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

RINNOVO ASSOCIATIVO ANNO 2026

Il 31 dicembre 2025 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario, nome e cognome, anno 2026".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Ricordiamo agli associati che non hanno ancora rinnovato la quota: il socio rimane iscritto nel libro soci per tre mesi ma perde il diritto di partecipare alla vita sociale e il diritto di voto e viene cancellato dalle mailing list di distribuzione soci. Scaduti i tre mesi il socio decade per morosità e deve effettuare di nuovo l'iscrizione pagando anche la relativa quota una tantum.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Vi ricordiamo che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'Associazione Italiana esperti in Infrastrutture Critiche**: è accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa. Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

COLLABORAZIONE ALLE ATTIVITA' AIIC

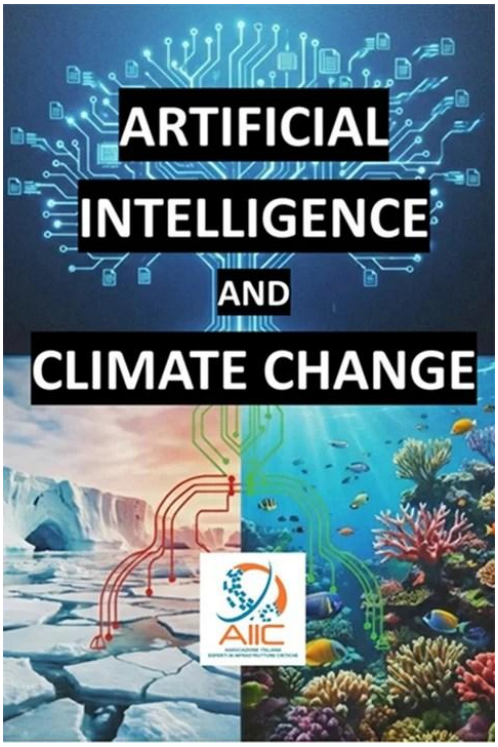
Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

AIIC – GRUPPO DI LAVORO

Artificial Intelligence and Climate Change

Il gruppo di studio AIIC dedicato ai rapporti tra Intelligenza Artificiale e Cambiamenti Climatici ha concluso i lavori ed ha pubblicato il relativo risultato sul sito dell'Associazione al seguente link:

AIIC-Artificial-Intelligence-and-Climate-Change-versione-finale-1.1-30gen2026.pdf



Questo Rapporto è il risultato di un progetto congiunto coordinato da Sandro Bologna e realizzato con il contributo di Silvano Bari, Glauco Bertocchi, Sandro Bologna, Gabriele Balzano, Luigi Carrozzi, Raffaella D'Alessandro, Tommaso Diddi, Elenio Dursi, Adriana Peduto, Beatrice Rosa, Alberto Stefanini, Cristina Turconi, Lorenzo Vandoni, Maria Beatrice Versaci.
L'intelligenza artificiale (IA) sta rapidamente ampliando le frontiere della climatologia, fornendo nuove informazioni sulla nostra comprensione del sistema climatico e contribuendo a trasformare la climatologia in un insieme di informazioni fruibili.
Il Rapporto esplora modi innovativi in cui l'IA può migliorare e accelerare l'azione per il clima, con particolare attenzione al processo decisionale e alle misure di adattamento per promuovere la resilienza contro gli impatti dei cambiamenti climatici.
Il Rapporto offre uno spunto per il dialogo interdisciplinare, al fine di facilitare il coinvolgimento intersettoriale, identificare applicazioni in cui l'IA può orientare l'azione per prevenire e combattere i cambiamenti climatici, e considerare come il più ampio impatto sociale dell'IA influenzi gli approcci per affrontare i cambiamenti climatici. In conclusione, l'IA rappresenta sia un'opportunità che una responsabilità. Se adeguatamente compresa, gestita e integrata, l'IA può contribuire a rendere le infrastrutture più resilienti, a una gestione più efficiente delle risorse e a strategie climatiche più consapevoli.
Il Gruppo di Lavoro auspica che questo Rapporto possa fungere da riferimento costruttivo per iniziative future e da punto di partenza per una più profonda cooperazione tra ricercatori, professionisti e istituzioni, tutti impegnati ad affrontare una delle sfide globali più significative del nostro tempo.

Il Report sarà oggetto di un webinar che si svolgerà nel prossimo mese di aprile 2026. Vi terremo informati sulla data di svolgimento.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NEWS E AVVENIMENTI

Data center in Italia: crescita, consumi energetici e nuove regole tra Europa, Stato e Regioni - La crescita dei data center impone un nuovo equilibrio tra infrastrutture digitali, consumo energetico e pianificazione territoriale. In Italia il quadro normativo è in rapida evoluzione, tra direttive europee, linee guida ministeriali e iniziative regionali. L'articolo analizza regole, procedure autorizzative e criticità operative.

I data center sono infrastrutture strategiche, ma con impatti rilevanti su energia, ambiente e territorio. Per progettisti e tecnici è fondamentale comprendere il quadro normativo che disciplina localizzazione, valutazioni ambientali, connessioni alla rete e recupero energetico. Questo contributo offre una lettura sistematica delle norme europee e italiane, con particolare attenzione al ruolo delle Regioni e agli strumenti urbanistici.

Data center: definizioni chiave

Data center
Infrastruttura fisica progettata per ospitare server, sistemi di archiviazione dati e apparati di rete, operativa 24 ore su 24, essenziale per servizi digitali, cloud e applicazioni critiche.

Hyperscale data center
Centro dati di grandi dimensioni, caratterizzato da elevata potenza installata e scalabilità, tipicamente gestito da grandi provider cloud internazionali.

Colocation
Modello in cui il gestore del data center mette a disposizione spazi, energia e raffreddamento per server di clienti terzi.

Edge data center
Struttura di dimensioni ridotte localizzata vicino agli utenti o alle fonti di dati, per ridurre latenza e traffico di rete.

HPC (High Performance Computing)
Infrastruttura specializzata che concentra elevate capacità di calcolo per simulazioni complesse, modellazioni avanzate e applicazioni scientifiche.

Recupero del calore
Riutilizzo dell'energia termica prodotta dal funzionamento dei server, ad esempio tramite reti di teleriscaldamento o sistemi energetici locali.

La crescita dei data center

Al mondo, nel 2024, se ne contavano 10.332. Di questi oltre cinquemila negli Usa e più di duemila in Europa. In Italia, alla stessa data, ne sono stati censiti 168: un dato, quest'ultimo, che colloca il nostro Paese al tredicesimo posto nella classifica globale.

L'oggetto del discutere si chiama Data Center, vale a dire le infrastrutture fisiche indispensabili per il funzionamento dei sistemi informatici, quali server, archiviazione dati, reti. Impianti attivi 24 ore su 24, 365 giorni l'anno, in grado di garantire l'operatività di servizi essenziali quali Internet, IA, cloud, servizi bancari e pagamenti elettronici, app e social media, pubblica amministrazione e sanità digitali, logistica e e-commerce.

(continua)

https://www.ingenio-web.it/articoli/data-center-in-italia-crescita-consumi-energetici-e-nuove-regole-tra-europa-stato-e-regioni/

Ingenio *- Claudia Mapelli, Pietro Mezzi - 9.01.2026*

Infrastrutture intelligenti: la manutenzione dei ponti è digitale - Il documento analizza come l'integrazione di IoT e AI rivoluzioni il monitoraggio infrastrutturale. Grazie ai bulloni sensorizzati Tokbo, i dati diventano conoscenza predittiva, riducendo i costi e aumentando la sicurezza delle opere civili. Il caso studio di un ponte ferroviario conferma l'efficacia di questa gestione data-driven.
Monitoraggio in tempo reale delle infrastrutture
Il monitoraggio strutturale rappresenta oggi un ambito di crescente rilevanza in numerosi settori dell'ingegneria civile e infrastrutturale, e grazie all'integrazione di tecnologie come Internet of Things (IoT), Intelligenza Artificiale (IA), Building Information Modeling (BIM) e Digital Twin, è oggi possibile acquisire dati in tempo reale delle infrastrutture, interpretarli in modo intelligente e visualizzarli all'interno di modelli digitali dinamici.
Secondo un recente studio i sistemi di monitoraggio intelligenti possono prevenire fino al 27% dei crolli delle strutture più vetuste e ridurre fino al 31% i costi complessivi di gestione delle reti stradali (gallerie, ponti, strade) e altre opere civili, prolungando la vita utile delle infrastrutture. La digitalizzazione dei processi sta ridefinendo i paradigmi di progettazione, esercizio e manutenzione delle opere civili, introducendo approcci data-driven orientati al miglioramento dei livelli di sicurezza, affidabilità e resilienza delle infrastrutture.
Fino a pochi anni fa, il controllo dello stato di salute di ponti e viadotti si basava prevalentemente su ispezioni manuali e verifiche visive periodiche. Tecnici e ingegneri eseguivano rilievi in sito, misurazioni di deformazioni o verifiche di eventuali allentamenti mediante strumenti tradizionali. Sebbene tali attività rimangano fondamentali, esse presentano il limite intrinseco di lasciare ampi intervalli temporali non monitorati, durante i quali la struttura può essere soggetta a sollecitazioni non rilevate, quali vibrazioni anomale, variazioni termiche, eventi sismici, con il rischio che il degrado venga individuato solo quando il danno risulta già evidente.
(continua)
https://www.ingenio-web.it/articoli/infrastrutture-intelligenti-la-manutenzione-dei-ponti-e-digitale/
***Ingenio** - Ivan Moroni - 12/01/2026*

Eventi idrogeologici: mitigazione del rischio e sistemi di allerta preventivi – Un intervento affronta il tema della valutazione e gestione del rischio NaTech da eventi idrogeologici. Focus sugli effetti delle alluvioni sugli impianti PIR, sulla mitigazione delle conseguenze e sui sistemi di allerta preventivi.
Brescia, 26 Gen – In Italia la quasi totalità degli stabilimenti con pericolo di incidente rilevante (PIR) è esposto al cosiddetto rischio NaTech (Natural hazards triggering a TECHnological accident), rischio che scaturisce "dall'interazione tra disastri naturali e rischio industriale".
E se "gli eventi naturali più impattanti sono quelli sismici e quelli idrogeologici (frane e alluvioni)", l'incidenza dei fenomeni idrogeologici, in relazione ai cambiamenti climatici, sta "aumentando in modo significativo". Ed esistono "alcune problematiche specifiche correlate agli eventi NaTech:
si possono verificare rilasci di sostanze pericolose da una o in più fonti all'interno di un'azienda o di più aziende con incremento della frequenza di accadimento degli incidenti rilevanti
i sistemi di sicurezza e mitigazione potrebbero essere indisponibili perché danneggiati dal sisma comportando quindi conseguenze più severe".
(continua…)
https://www.puntosicuro.it/rischio-di-incidente-rilevante-C-86/eventi-idrogeologici-mitigazione-del-rischio-sistemi-di-allerta-preventivi-AR-25901/
***Punto Sicuro** - Redazione, 26/01/2026*

Telecamere LPR e sicurezza urbana: quando la privacy diventa il paravento di un cortocircuito istituzionale - C'è un passaggio, nel provvedimento n. 752 del 18 dicembre 2025 del Garante per la protezione dei dati personali, che merita più attenzione di quanto ne abbia sinora ricevuta. Non tanto per il suo contenuto tecnico, quanto per la portata sistemica delle sue implicazioni: l'affermazione secondo cui, in assenza di un "dettagliato patto per la sicurezza urbana" con la Prefettura, l'impiego comunale di sistemi di videosorveglianza e lettura targhe per finalità di sicurezza urbana sarebbe giuridicamente privo di fondamento.
Un'affermazione che, se presa sul serio fino in fondo, rischia di produrre un effetto dirompente: trasformare uno strumento di cooperazione facoltativa tra livelli istituzionali in una condizione di legittimità dell'azione amministrativa comunale. Con un duplice paradosso. Da un lato, le Prefetture – in assenza di modelli centrali uniformi e procedure standardizzate – risultano nella prassi spesso indisponibili a stipulare tali patti; dall'altro, si finisce per subordinare l'esercizio di funzioni proprie dei Comuni, come la tutela della sicurezza urbana in senso amministrativo, a un atto che l'ordinamento non configura affatto come presupposto giuridico necessario.
È su questo sfondo che va letto l'intero provvedimento, che trae origine dal reclamo di un cittadino sanzionato per mancanza di copertura assicurativa del proprio veicolo, violazione accertata tramite un sistema comunale di lettura automatizzata delle targhe (LPR) installato su una direttrice di uscita dal centro abitato.
(continua…)
https://www.federprivacy.org/informazione/primo-piano/telecamere-lpr-e-sicurezza-urbana-quando-la-privacy-diventa-il-paravento-di-un-cortocircuito-istituzionale
Federprivacy - *Stefano Manzelli, 29 Gennaio 2026*

Il sistema energetico europeo è in ritardo sui target 2030. Lo dice ENEA - Investimenti insufficienti, costi elevati e industria in difficoltà: il bilancio ENEA sullo stato del sistema energetico europeo dopo dieci anni di Energy Union.
Sistema energetico europeo, ENEA: gli obiettivi 2030 si allontanano
Indice dei contenuti

Lo stato dell'arte del sistema energetico europeo
Il sistema energetico europeo mostra un divario crescente tra obiettivi climatici, dinamiche industriali e competitività economica. È questo il quadro che emerge dall'approfondimento curato dagli economisti curato dagli economisti ENEA Daniela Palma e Francesco Gracceva, nell'ambito dell'edizione 2025 del European Public Investment Outlook, che analizza l'evoluzione del settore a dieci anni dall'avvio dell'Energy Union Strategy.
Secondo l'analisi, nonostante le politiche adottate, l'Europa si è progressivamente allontanata dai target di decarbonizzazione al 2030, mentre i costi dell'energia restano strutturalmente più elevati rispetto ai principali concorrenti globali.

Per rientrare negli obiettivi fissati, sarebbe oggi necessario accelerare in modo significativo su consumi, emissioni e diffusione delle rinnovabili, in un contesto segnato da tensioni geopolitiche, crisi industriali e limiti nella governance europea.
(continua…)
https://www.rinnovabili.it/energia/infrastrutture/sistema-energetico-europeo-enea-gli-obiettivi-2030-si-allontanano/
Rinnovabili - *Alessandro Petrone - 30 Gennaio 2026*

Urmet, Nobus e 5T: progetto per la sicurezza urbana, Città di Torino - Urmet SpA, Nobus Srl e la partecipata pubblica 5T hanno contribuito all'ambizioso progetto sperimentale di tutela della sicurezza urbana e monitoraggio delle aree cittadine sensibili, voluto anche dalla Città di Torino, con la collaborazione dell'assessore alla Sicurezza Marco Porcedda.
La sperimentazione, avviata recentemente, ha previsto la realizzazione di un innovativo PoC (*Proof of Concept*) dedicato alla sicurezza urbana smart, con l'installazione di un palo solare equipaggiato con un sistema di videosorveglianza di ultima generazione fornito da Urmet. Il progetto nasce con l'obiettivo di testare nuove soluzioni tecnologiche e sostenibili per il monitoraggio di aree urbane come i Murazzi, una zona di Torino ad alta frequentazione.
(continua…)
https://www.snewsonline.com/urmet-nobus-5t-progetto-sicurezza-urbana-citta-torino/
SNews – *Redazione - 3 Febbraio 2026*

The Great AI Opt-Out: Why Millions Are Racing to Pull Their Data From Google, Meta, and the Machine Learning Pipeline - Millions of users are scrambling to opt out of AI data training by Google, Meta, and others, but buried settings, retroactive data use, and weak U.S. privacy laws make true protection nearly impossible — raising urgent questions about digital consent.
For years, the implicit bargain of the internet was simple: users handed over their data in exchange for free services. Search engines indexed the world's information. Social networks connected billions of people. Email platforms organized digital lives. But as artificial intelligence has surged from a research curiosity into the defining technology of the decade, that bargain is being renegotiated — and millions of consumers are discovering just how difficult it is to claw back what they've already given away.
A growing wave of users across the United States and Europe are attempting to opt out of having their personal data used to train AI models built by Google, Meta, OpenAI, and other technology giants. The process, as reported by The New York Times, is neither straightforward nor particularly transparent — a reality that has frustrated privacy advocates, regulators, and ordinary people alike. The opt-out mechanisms that do exist are buried in labyrinthine settings menus, vary wildly from company to company, and in many cases offer only partial protection against the voracious data appetite of modern machine learning systems.
A Patchwork of Opt-Out Tools That Leave Users in the Dark
Google, for its part, has introduced a series of controls that allow users to limit how their data feeds into its Gemini AI models. Users can navigate to their Google Account's "Data & Privacy" section and toggle off settings related to AI training. But as The New York Times detailed, the toggles are not comprehensive. Certain data — including search queries, YouTube viewing history, and Google Maps location data — may still be used in aggregated or anonymized forms that fall outside the scope of

individual opt-out controls. Google has maintained that anonymized data is not “personal data” under most legal frameworks, a position that privacy researchers have increasingly challenged.
Meta’s approach is similarly convoluted. The company, which operates Facebook, Instagram, WhatsApp, and Threads, has offered European users a formal objection mechanism under the General Data Protection Regulation (GDPR), allowing them to submit requests that their data not be used for AI training. But for American users, the options are far more limited. Meta’s privacy settings allow users to manage some AI-related data usage, but the company has been candid that posts, photos, and comments shared publicly on its platforms may be used to train its Llama family of large language models. The distinction between “public” and “private” data has become a flashpoint, with critics arguing that users who posted content years ago never anticipated it would be fed into AI systems. (continua…)
https://www.webpronews.com/the-great-ai-opt-out-why-millions-are-racing-to-pull-their-data-from-google-meta-and-the-machine-learning-pipeline/
WEBPRONEWS - *Sara Donnelly- February 10, 2026*

AI Agents 'Swarm,' Security Complexity Follows Suit - As AI deployments scale and start to include packs of agents autonomously working in concert, organizations face a naturally amplified attack surface.
The maturing AI landscape increases the likelihood that multiple models, and agents, will need to work alongside each other. And this type of "swarm" orchestration introduces a host of additional security concerns that need to be addressed to ensure the integrity of an organization's security.
AI agents have become an increasing force in LLM-powered deployments in the workplace. Autonomous AI agents, which are sold under the premise that they can work in a mostly self-directed fashion and make "decisions" about what to use next, are used in data analysis, build process automation, software development (to create and manage code), and more. As businesses make the decision to lean more into this technology, it becomes increasingly likely that multiple agents used for different processes will come into contact with each other.
This becomes an even greater concern as open source self-hosted agents like OpenClaw (aka MoltBot) hit the scene — a concern that has come to somewhat humorous fruition in the form of quasi-social-media platform Moltbook, leading to the rise of orchestration products such as GitHub's Agent HQ for software development, which includes features like code review and a single command center to manage multiple agents simultaneously. Countless other vendors, such as Zapier and IBM, offer orchestration tools for various swarm use cases as well.
Roey Eliyahu, CEO and co-founder of Salt Security, tells Dark Reading that while agent orchestration can enable agents to work on parallel tasks simultaneously and specialize, the practice introduces multiple security risks, such as credential sprawl, over-privileged access to tools, and more integrations that may be connected to sensitive data.
"Multiagent orchestration is powerful because it parallelizes work, but it also parallelizes risk," he says. "The security job is to keep every agent narrowly scoped, heavily audited, and blocked from high-impact actions without explicit approval."
Multiple Agents Means Multiplied Security Risks
It almost goes without saying, but if having one agent in one's environment introduces security risks, multiple agents enhance said risk when data security is not put front and center.

That's because, while AI agents aren't human employees, they still need the privilege and access of humans, including tokens and credentials for servers or other tools. That also means, potentially, high-level permissions. LLMs can still be manipulated via prompt injection (even agents), so every integration with some instance or product is another opportunity to divulge sensitive data.
Agents can also make a large number of outputs in a short period of time depending on the task. If not properly audited, Eliyahu explains, that can mean secrets get exposed in outputs or logs, or at the very least, there are more opportunities to make mistakes (which LLMs are prone to when left to their own devices). (continua…)
https://www.darkreading.com/cloud-security/ai-agents-swarm-security-complexity
Darkreading *- Alexander Culafi - February 13, 2026*

AI compliance: roadmap operativa per ridurre sanzioni e incidenti
La compliance, da concetto tecnico, è diventata un paradigma che spinge organizzazioni e individui a dimostrare conformità tramite procedure e documenti. Con l'IA emergono nodi nuovi: opacità, responsabilità distribuita e trade-off tra accuratezza e spiegabilità. L'AI Act rafforza obblighi, ma apre interrogativi etici
La compliance non riguarda più solo "rispettare le regole": oggi significa anche dimostrare, con procedure e documenti, di averle rispettate.
Con l'intelligenza artificiale la sfida cresce, perché molti sistemi sono difficili da capire e le responsabilità si distribuiscono tra tanti attori. **L'AI Act prova a mettere ordine**, ma riapre una domanda: **basta essere conformi, o serve anche essere etici?**
Indice degli argomenti

Compliance dell'intelligenza artificiale: perché oggi è un paradigma

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Il termine compliance – dall'inglese *to comply*, conformarsi – ha subito negli ultimi tre decenni un processo di inflazione semantica che ne ha progressivamente ampliato e, al contempo, sfocato il perimetro concettuale. Da nozione tecnico-giuridica circoscritta all'ambito del diritto societario e bancario, la compliance è divenuta categoria omnicomprensiva che attraversa diagonalmente ambiti normativi eterogenei: dalla **protezione dei dati personali** alla **prevenzione del riciclaggio**, dalla **sicurezza sul lavoro** alla **responsabilità sociale d'impresa**, fino a cristallizzarsi, nell'epoca dell'**intelligenza artificiale**, come esempio regolatorio dominante.

Questa polisemia non è casuale né innocente. Essa riflette, come ha magistralmente mostrato Michel Foucault nella sua genealogia delle pratiche di governo, l'emergere di una razionalità politica specifica – quella neoliberale – che trasforma il diritto da sistema di comandi eteronomi in dispositivo di **autoregolazione responsabilizzante**. La compliance, in questa prospettiva, non è mera obbedienza alla norma, ma **interiorizzazione della normatività**: il soggetto (individuale o collettivo) è chiamato non solo a rispettare la regola, ma a farsi **imprenditore di sé stesso**, a calcolare rischi, a implementare procedure, a documentare diligenze, a dimostrare – secondo la logica dell'**accountability** – di essere conforme.

Quando questo paradigma incontra l'intelligenza artificiale, la complessità si moltiplica esponenzialmente. L'IA, infatti, non è semplicemente un oggetto da regolare tra gli altri. È, come ha argomentato Luciano Floridi, un'*ontological force* – una forza ontologica che rimodella il tessuto stesso della realtà in cui viviamo, le nostre relazioni sociali, i nostri processi cognitivi, i nostri sistemi di valore. La **AI compliance** diviene, così, non solo questione normativa, ma interrogativo filosofico: **come si può essere conformi** a qualcosa che sfida le categorie tradizionali di causalità, intenzionalità, responsabilità? (continua…)

https://www.agendadigitale.eu/industry-4-0/ai-compliance-roadmap-operativa-per-ridurre-sanzioni-e-incidenti/

AGENDADIGITALE - *Enrica Priolo - 13 feb 2026*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare i nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Glauco Bertocchi Silvano Bari Maria Beatrice Versaci *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.