ICT Security MAGAZINE

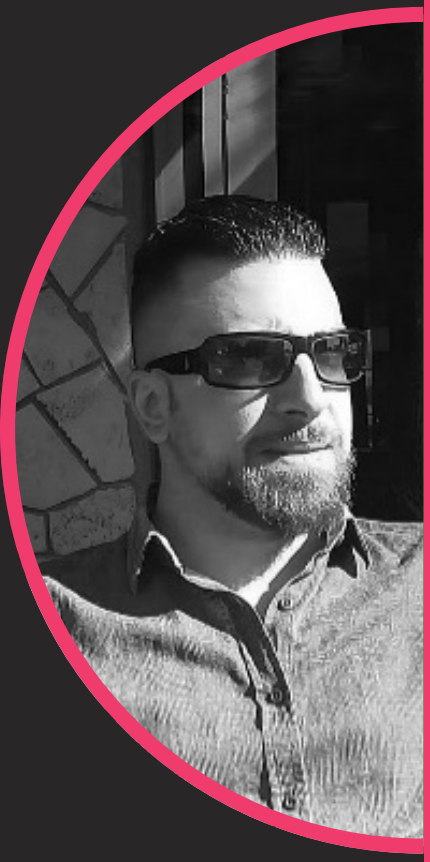
Jammer nelle carceri: limiti, rischi e alternative

A cura di **Stefano Cangiano**

Whitepaper
Aprile 2026

www.ictsecuritymagazine.com

Indice



About the author

Stefano Cangiano

CYBER SECURITY SPECIALIST &
FOUNDER/CEO DELLA SOCIETÀ ISK.

Titolare delle licenze EJPT e ECPPT (Professional Penetration Tester) della società eLearnSecurity. Svolge attività di Network Security in particolare Penetration Test & VA – Vulnerability Assessment.

Nel 2019 fonda la società ISK (www.isksecurity.it), partner strategico ed esterno per attività di Security specializzata. Svolge attività di bonifiche ambientali da microspie, attività di Security Assessment e Mobile Security.

Introduzione

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

Il fenomeno dei telefoni cellulari non autorizzati all'interno degli istituti penitenziari italiani è in costante e preoccupante crescita, e rappresenta oggi una delle sfide più complesse per l'amministrazione penitenziaria e per l'intero sistema della sicurezza nazionale.

Dati interni del Dipartimento dell'Amministrazione Penitenziaria (DAP) mostrano che i sequestri di dispositivi mobili sono passati da circa 1.084 unità nel 2022 a oltre 2.250 nel 2024, con un aumento superiore al 100% in soli due anni. Questo *trend* esponenziale, oltre a indicare l'efficacia e la capillarità delle reti criminali nel far entrare telefonini occultati attraverso canali sempre più sofisticati, mette in luce l'impossibilità strutturale di contenere il fenomeno con semplici controlli manuali o perquisizioni periodiche.

Le modalità di introduzione dei dispositivi si sono evolute nel tempo, passando dai tradizionali metodi di occultamento durante i colloqui con i familiari a tecniche sempre più ingegnose: droni che sorvolano i cortili di passeggio, pacchi postali con doppi fondi, corruzione del personale, e persino il lancio di piccoli involucri oltre le mura perimetrali. La miniaturizzazione dei dispositivi ha ulteriormente complicato le operazioni di contrasto: oggi esistono telefoni delle dimensioni di un accendino, perfettamente funzionanti e dotati di connettività 4G, praticamente impossibili da individuare con i *metal detector* tradizionali.

L'impiego di telefoni di contrabbando consente ai detenuti di coordinare traffici illeciti con una facilità impensabile fino a pochi anni fa. Attraverso questi dispositivi vengono impartiti ordini a complici all'esterno, organizzate estorsioni ai danni di commercianti e imprenditori, gestite piaz-

ze di spaccio e persino pianificate intimidazioni a testimoni e magistrati. L'interazione con i *social network* ha aggiunto una dimensione ulteriore al problema: sono documentati casi di boss mafiosi che continuavano a gestire i propri profili Facebook dal carcere, inviando messaggi minacciosi e mantenendo viva la propria presenza simbolica nel territorio di riferimento.

In molti casi, le chiamate vengono effettuate in piena notte o in momenti di massima distrazione del personale, rendendo quasi impossibile l'intervento tempestivo. La carenza cronica di organico che affligge il sistema penitenziario italiano - con rapporti agente-detenuto tra i più sfavorevoli d'Europa - contribuisce a creare finestre di opportunità che i detenuti più scaltri sanno sfruttare con precisione quasi scientifica. Il problema assume inoltre rilievo di sicurezza nazionale quando cellule criminali o terroristiche cercano di contattare vittime o pianificare azioni esterne sfruttando la paradossale "libertà comunicativa" garantita dal carcere. Per arginare questo rischio, molte amministrazioni hanno valutato o implementato dispositivi di *jamming*, ossia disturbatori di segnale radio in grado di inibire le comunicazioni GSM, LTE e Wi-Fi. La promessa di questi apparati è apparentemente semplice: creare una "bolla" elettromagnetica attorno all'istituto penitenziario che renda impossibile qualsiasi comunicazione cellulare. Tuttavia, come emergerà nei capitoli successivi, queste soluzioni presentano criticità significative su più fronti, tali da renderle non solo inefficaci ma potenzialmente dannose.

Sul piano dell'inefficacia tecnica, i *jammer* non coprono in modo omogeneo tutte le bande di frequenza, lasciano inevitabili "zone d'ombra" dovute alla conformazione architettonica degli edifici, e richiedono costosi aggiornamenti per seguire l'evoluzione delle reti 4G/5G. I rischi operativi sono altrettanto rilevanti: questi dispositivi bloccano indiscriminatamente anche le linee di emergenza (112/118), le comunicazioni istituzionali del personale di polizia penitenziaria, e possono interferire con dispositivi medici salvavita come pacemaker e defibrillatori impiantabili.

Non meno importanti sono i vincoli legali: in Italia i *jammer* sono vietati fuori da ambiti strettamente autorizzati e possono configurare i reati di "interruzione di pubblico servizio" (art. 340 c.p.) e di "installazione di apparecchiature per impedire comunicazioni altrui" (art. 617-bis c.p.).

Di fronte a queste criticità, emerge con forza la necessità di soluzioni alternative che superino la logica del disturbo indiscriminato in favore di un approccio più intelligente e mirato. I rilevatori di attività radio cellulare basati su analisi passiva dello spettro rappresentano oggi la frontiera più promettente. Tali sistemi non emettono segnali di disturbo, monitorano costantemente tutte le bande in *uplink*, catalogano ogni *burst* di traffico dati o voce, e permettono di localizzare con precisione il punto di trasmissione, consentendo interventi mirati e tempestivi.

Nel seguito di questo articolo esploreremo in dettaglio perché i *jammer* sono una risposta sbagliata, analizzando i loro limiti tecnici, operativi e normativi; i vantaggi dei rilevatori SDR passivi, con particolare attenzione a come funzionano, come interpretano i segnali e come si integrano nel complesso ecosistema della sicurezza penitenziaria; e infine un case *study* di un progetto sperimentale condotto in ambiente isolato, che dimostra concretamente l'efficacia del rilevamento passivo in condizioni analoghe a quelle di un vero istituto di pena.

Capitolo 1

Breve storia dei jammer nelle carceri

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

1.1
Le ragioni della scelta iniziale

Nel contesto temporale in cui maturò la decisione (2018), la scelta del Dipartimento dell'Amministrazione Penitenziaria di ricorrere ai *jammer* rispondeva a una combinazione di fattori concreti e contingenti che meritano di essere analizzati con attenzione per comprendere come si sia giunti alla situazione attuale. L'utilizzo di disturbatori di segnale appariva, in quel momento storico, come la soluzione più rapida da implementare per fronteggiare un fenomeno percepito come emergenziale, caratterizzato da un incremento costante dei sequestri di telefoni cellulari e da una crescente attenzione mediatica sul tema delle comunicazioni illecite dal carcere.

I *jammer* offrivano un approccio apparentemente "chiavi in mano", con tempi di installazione relativamente brevi, costi iniziali contenuti e una promessa di efficacia immediata sulle tecnologie allora prevalenti, in particolare GSM e prime reti LTE. In un quadro segnato da forte pressione politica e sindacale - con i sindacati di polizia penitenziaria che denunciavano quotidianamente l'impossibilità di garantire la sicurezza con gli strumenti disponibili - tale scelta consentiva inoltre all'amministrazione di dimostrare un intervento visibile, facilmente comunicabile all'opinione pubblica e coerente con una linea di fermezza nei confronti della criminalità organizzata.

Il contesto politico dell'epoca non può essere sottovalutato. La questione delle comunicazioni illecite dal carcere era diventata un tema caldo nel dibattito pubblico, alimentato da inchieste giornalistiche che documentavano come *boss* mafiosi continuassero a gestire i propri affari criminali dalle celle di massima sicurezza. La pressione per una risposta immediata e visibile era fortissima, e i *jammer* sembravano offrire esattamente questo: una so-

luzione tecnologica tangibile, un investimento dimostrabile, un'azione concreta da poter esibire di fronte alle critiche.

A ciò si aggiungeva la limitata maturità, in quegli anni, di soluzioni alternative basate su analisi passiva dello spettro radio e sistemi di rilevazione selettiva. Queste tecnologie, pur esistendo già in ambito militare e di *intelligence*, richiedevano competenze altamente specialistiche raramente disponibili nel contesto dell'amministrazione penitenziaria, infrastrutture dedicate con costi di implementazione significativi, e soprattutto un cambio di paradigma operativo non immediato per un'organizzazione tradizionalmente orientata a soluzioni hardware piuttosto che a sistemi di analisi e intelligence.

In questo quadro si collocano anche le posizioni espresse pubblicamente dal Procuratore Nicola Gratteri, [1] figura di riferimento nel contrasto alla 'ndrangheta e voce autorevole nel dibattito sulla sicurezza penitenziaria. Gratteri, pur denunciando più volte l'inefficacia complessiva delle misure adottate e i ritardi strutturali dello Stato nel contrasto alle comunicazioni illecite dal carcere, ha in diverse occasioni riconosciuto l'utilità dei *jammer* almeno come strumento temporaneo nei reparti di alta sicurezza. In interviste e audizioni pubbliche, il Procuratore ha infatti sottolineato come, in assenza di soluzioni tecnologicamente più avanzate e strutturate, i *jammer* potessero rappresentare una risposta transitoria per limitare le comunicazioni dei detenuti più pericolosi, in attesa di un approccio più organico e duraturo.

Tali posizioni contribuiscono a chiarire come il tema dell'impiego dei *jammer* non sia riconducibile a una contrapposizione ideologica tra "falchi" e "colombe", ma vada letto come il risultato di scelte contingenti, maturate in un contesto emergenziale e sotto la spinta di pressioni multiple. Oggi quel contesto appare superato dall'evoluzione tecnologica e dalla disponibilità di strumenti più efficaci, selettivi e sostenibili nel lungo periodo.

1 https://www.poliziapenitenziaria.it/gratteri-nuovo-appello-per-lutilizzo-degli-jammer-per-bloccare-uso-dei-telefonini-in-carcere-utilizzare-risorse-del-pnrr/

1.2 Cronologia essenziale

La storia dell'adozione dei *jammer* nelle carceri italiane si snoda attraverso alcune tappe fondamentali che meritano di essere ricostruite con precisione documentale, anche per comprendere l'entità degli investimenti pubblici che rischiano oggi di rivelarsi largamente improduttivi.

Il **17 ottobre 2018** segna l'avvio formale della gara d'appalto per l'acquisto dei primi apparati *jammer*, con la firma del decreto da parte del Direttore generale Buffa e un ordinativo iniziale di circa 47 unità destinate agli istituti di massima sicurezza. La scelta di partire dai reparti ad alta sicurezza rispondeva a una logica di priorità: era lì che si concentravano i detenuti più pericolosi, i *boss* mafiosi e i terroristi per i quali l'isolamento comunicativo rappresentava un obiettivo strategico primario. La documentazione di riferimento, non più accessibile attraverso l'archivio *online* del Ministero della Giustizia (che rende consultabili solo gli atti pubblicati a partire dal 2020), è ricostruita attraverso fonti DAP e Il Sole 24 Ore nel documento disponibile presso POLPENUIL – Blocco telefoni carcere *jammer*.[2]

Nel **maggio 2019** si procede alla consegna e installazione dei dispositivi in vari istituti ad alta sicurezza, accompagnata da un programma di formazione per gli operatori. Questa fase ha rivelato immediatamente alcune criticità: la complessità degli apparati richiedeva competenze tecniche che il personale penitenziario non possedeva, e l'integrazione con le infrastrutture esistenti si rivelava più problematica del previsto. Sono stati necessari interventi di adeguamento impiantistico, con costi aggiuntivi non pre-

2 https://www.polpenuil.it/images/blocco_telefoni_carcere_jammer_sole_24.pdf

visti nel *budget* iniziale (Circolare acquisizione sistemi jammer).[3]

Tra **agosto e settembre 2023** vengono condotte prove pilota in 20 strutture, mirate a verificare l'efficacia dei sistemi su reti 4G e a condurre *test* preliminari su bande 5G, ormai in fase di diffusione capillare sul territorio nazionale. Da queste sperimentazioni emergono zone d'ombra significative e criticità tecniche che mettono in discussione l'intera strategia: i *jammer*, progettati per tecnologie ormai superate, faticano a contrastare le nuove frequenze, mentre la conformazione architettonica degli istituti - spesso edifici storici con muri spessi e strutture metalliche - crea sacche di copertura irregolare (Resoconto Camera dei Deputati).[4]

Nel **gennaio 2025** prende avvio la sperimentazione di un sistema alternativo di filtraggio passivo, volto a superare i problemi sanitari e di interferenza non selettiva che avevano caratterizzato l'esperienza con i *jammer*. L'abbandono di fatto del sistema *jammer*, dopo anni di investimenti largamente inutilizzati e con apparati che giacciono in molti casi ancora imballati nei magazzini degli istituti, è documentato da diverse fonti giornalistiche che parlano esplicitamente di "rottamazione" di un sistema mai realmente entrato in funzione (HuffPost[5] e Ristretti Orizzonti[6]).

3 https://www.polpenuil.it/circolari/8698-acquisizione-sistemi-inibitori-di-telefoni-cellulari-jammer.html

4 https://documenti.camera.it/leg19/resoconti/assemblea/html/sed0452/leg.19.sed0452.allegato_a.pdf

5 https://www.huffingtonpost.it/esteri/2025/02/13/news/in_carcere_ce_campo_telefonini_sempre_piu_diffusi_47_jammer_comprati_inutilizzabili_si_torna_a_perquisire-18424329/

6 https://ristretti.org/boss-al-telefono-in-carcere-lo-stato-rottama-il-sistema-di-schermatura-mai-partito

1.3
Le ragioni dell'adozione

Le motivazioni che portarono alla scelta dei *jammer* possono essere ricondotte a quattro fattori principali, che vale la pena analizzare nel dettaglio per comprendere la razionalità (sia pure limitata) di quella decisione.

In primo luogo, le **pressioni mediatiche e sindacali**. Le segnalazioni frequenti di contatti illeciti tra detenuti e organizzazioni criminali esterne avevano creato un clima di urgenza che richiedeva risposte immediate. I *media* riportavano con cadenza quasi quotidiana episodi di *boss* che continuavano a impartire ordini dal carcere, di estorsioni coordinate via cellulare, di minacce a pentiti e testimoni. I sindacati di polizia penitenziaria denunciavano l'impossibilità di svolgere efficacemente il proprio lavoro senza strumenti tecnologici adeguati. La pressione convergente di questi attori rendeva politicamente insostenibile l'inazione.

In secondo luogo, la **rapidità di implementazione**. I *jammer* costituivano una soluzione apparentemente pronta all'uso, con tempi di installazione contenuti rispetto a sistemi passivi o reti di sorveglianza RF più sofisticate. In un contesto di emergenza percepita, la possibilità di "fare qualcosa subito" aveva un valore politico e comunicativo che superava considerazioni più ponderate sull'efficacia di lungo periodo.

Il **costo iniziale contenuto** rappresentava un terzo elemento di attrattiva. L'investimento per singolo apparato risultava inferiore a quello richiesto per infrastrutture di *monitoring* e analisi dati, che avrebbero comportato non solo l'acquisto di *hardware* sofisticato ma anche la formazione di personale specializzato, la creazione di sale operative dedicate, e costi di manutenzione e aggiornamento continuativi.

Infine, la **visibilità politica**. L'adozione dei *jammer* veniva percepita come un intervento risolutivo e "intransigente" contro l'illegalità nel carcere, facilmente comunicabile all'opinione pubblica. Un annuncio del tipo "abbiamo installato sistemi di disturbo in tutti i penitenziari di massima sicurezza" aveva un impatto mediatico immediato, molto più di discorsi complessi su sistemi di analisi dello spettro e algoritmi di rilevazione.

1.4
Cosa sono i Jammer

Prima di procedere all'analisi delle criticità, è opportuno chiarire con precisione cosa siano i *jammer* e come funzionino dal punto di vista tecnico. I *jammer* sono dispositivi di disturbo radio progettati per emettere segnali nelle bande di frequenza utilizzate dai telefoni cellulari, creando un "rumore" elettromagnetico che impedisce la connessione tra il terminale e le celle di rete. Le frequenze interessate includono tipicamente la banda 900 MHz (GSM), 1800 MHz (DCS), 2100 MHz (UMTS/3G), e nelle versioni più recenti anche le bande 800 MHz, 1800 MHz e 2600 MHz del 4G/LTE, fino ai 3,5 GHz necessari per disturbare le comunicazioni 5G. Il principio di funzionamento è relativamente semplice: il *jammer* emette un segnale di potenza superiore a quello della cella telefonica legittima sulla stessa frequenza, "sovrastando" il segnale utile e rendendo impossibile al telefono stabilire o mantenere una connessione.

Questa semplicità concettuale nasconde però una complessità operativa significativa. Per essere efficace, un *jammer* deve coprire tutte le bande utilizzate dagli operatori attivi sul territorio, deve emettere con potenza sufficiente a superare il segnale delle celle (che può variare significativamente in funzione della posizione geografica dell'istituto), e deve farlo in modo uniforme su tutta l'area da proteggere. Ognuno di questi requisiti presenta sfide tecniche non banali, come vedremo nel capitolo successivo.

L'aspetto più critico è che i *jammer* agiscono in modo totalmente indiscriminato: bloccano qualsiasi tipo di comunicazione RF nell'area di copertura, senza possibilità di distinguere fra traffico legale (comunicazioni del personale, sistemi di emergenza, dispositivi medici) e traffico illegale (telefoni dei detenuti). Questa caratteristica intrinseca rappresenta il limite fondamentale della tecnologia e la ragione principale per cui essa si sta rivelando inadeguata.

Capitolo 2

Perchè i jammer sono inefficaci e pericolosi

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

2.1 Premessa

L'impiego di apparati *jammer*, seppur concepito come soluzione "rapida" per bloccare le comunicazioni non autorizzate in carcere, si è dimostrato in diverse occasioni né selettivo né affidabile. Oltre all'efficacia limitata in contesti fortemente schermati come quelli penitenziari, i rischi associati al loro utilizzo superano di gran lunga i benefici attesi. Analizziamo nel dettaglio le principali criticità.

2.2 L'impatto sul contesto circostante

Il primo e più evidente limite dei *jammer* è la loro totale incapacità di discriminare tra comunicazioni legittime e illegittime.

Questi dispositivi bloccano tutte le comunicazioni RF - LTE, GSM, Wi-Fi, *Bluetooth* - nel raggio d'azione, senza alcuna distinzione tra traffico lecito e illecito. Si tratta di una caratteristica intrinseca della tecnologia, non di un difetto risolvibile con migliorie tecniche. Le conseguenze di questa indiscriminatezza sono molteplici e gravi, e investono sia la sicurezza operativa dell'istituto sia la tutela dei diritti delle persone che vi operano o vi transitano.

I *jammer* possono interferire con le comunicazioni di emergenza (112, 118, forze dell'ordine), ostacolando

l'invio o il ricevimento di chiamate urgenti in situazioni che potrebbero richiedere interventi salvavita. Si pensi a un detenuto colto da malore cardiaco: il personale sanitario interno potrebbe trovarsi nell'impossibilità di chiamare il 118 per richiedere un'ambulanza, con conseguenze potenzialmente fatali. Analogamente, in caso di sommossa o evasione, le comunicazioni con le forze dell'ordine esterne potrebbero risultare compromesse proprio nel momento di massima necessità.

I dispositivi medici rappresentano un'altra area di rischio critico. *Pacemaker* di ultima generazione, defibrillatori impiantabili, pompe insuliniche e altri dispositivi salvavita utilizzano sempre più spesso tecnologie *wireless* per la trasmissione di dati clinici e per la ricezione di comandi di regolazione. L'interferenza dei *jammer* con questi dispositivi può avere conseguenze che vanno dal semplice malfunzionamento temporaneo fino a situazioni di pericolo di vita. Il problema riguarda non solo i detenuti ma anche il personale e i visitatori che potrebbero essere portatori di tali dispositivi.

I *jammer* creano inoltre "zone d'ombra" per colleghi e visitatori in aree adiacenti all'istituto. Gli istituti penitenziari sono spesso situati in contesti urbani o semi-urbani, con abitazioni, esercizi commerciali e uffici nelle immediate vicinanze. L'effetto dei *jammer* non si ferma alle mura del carcere ma si estende, sia pure con intensità decrescente, alle aree circostanti, creando disservizi per cittadini estranei alla vicenda penitenziaria.

Infine, paradossalmente, i *jammer* possono ridurre l'efficacia degli stessi sistemi di sicurezza interni. Molti istituti hanno implementato sistemi di videosorveglianza con trasmissione *wireless*, sensori antintrusione collegati via radio, e altri dispositivi di sicurezza che utilizzano frequenze suscettibili di interferenza. L'attivazione dei *jammer* può quindi degradare proprio quegli strumenti pensati per garantire la sicurezza dell'istituto.

2.3
I rischi per la salute

Sul fronte sanitario, le preoccupazioni sono altrettanto serie e documentate da una crescente letteratura scientifica. L'esposizione prolungata ai campi elettromagnetici generati dai *jammer* solleva questioni che non possono essere ignorate, soprattutto considerando che il personale penitenziario trascorre in questi ambienti l'intera giornata lavorativa, giorno dopo giorno, per anni.

I *jammer* emettono onde elettromagnetiche a potenza elevata per coprire distanze ampie e superare il segnale delle celle telefoniche legittime. Questa potenza di emissione può facilmente superare i limiti di sicurezza raccomandati da organismi internazionali quali l'ICNIRP (*International Commission on Non-Ionizing Radiation Protection*) e il CEI (*Comitato Elettrotecnico Italiano*). Le linee guida internazionali stabiliscono soglie di esposizione che, nel caso dei *jammer* operanti in ambienti chiusi, possono essere superate in modo significativo, soprattutto nelle aree più vicine agli apparati.

Gli studi epidemiologici disponibili, pur non essendo ancora conclusivi, suggeriscono possibili correlazioni tra esposizione prolungata a radiofrequenze e una serie di disturbi: mal di testa cronici, disturbi del sonno, difficoltà di concentrazione, alterazioni cognitive e neurologiche. Alcuni studi su modelli animali hanno evidenziato effetti sulla contrattilità muscolare e sui parametri ematologici in seguito a esposizione a campi elettromagnetici generati da *jammer*. Sebbene la trasposizione di questi risultati all'uomo richieda cautela metodologica, il principio di precauzione suggerirebbe di evitare esposizioni non strettamente necessarie.

In presenza di campi RF intensi si possono inoltre generare correnti parassite nei tessuti biologici, con

rischio di danni termici localizzati dovuti a sovrariscaldamento. Questo fenomeno è particolarmente rilevante per soggetti portatori di impianti metallici o dispositivi elettronici impiantati, che possono fungere da "antenne" concentrando l'energia elettromagnetica.

Particolarmente a rischio risultano i soggetti vulnerabili: detenuti con patologie cardiache o impianti metallici (*pacemaker*, neurostimolatori, protesi metalliche), donne in gravidanza, e personale sanitario che opera in prossimità degli apparati. Per questi soggetti, l'esposizione ai campi generati dai *jammer* può comportare rischi aggiuntivi che meriterebbero una valutazione caso per caso, praticamente impossibile da realizzare in un contesto operativo.

Le emissioni dei *jammer*, se non accuratamente calibrate e certificate, possono peraltro violare il Decreto Legislativo 81/2008 sulla tutela della salute e della sicurezza nei luoghi di lavoro. La normativa italiana impone al datore di lavoro - in questo caso l'amministrazione penitenziaria - di valutare tutti i rischi per la salute dei lavoratori, compresi quelli derivanti dall'esposizione a campi elettromagnetici, e di adottare le misure necessarie per eliminarli o ridurli al minimo. L'installazione di *jammer* senza un'adeguata valutazione del rischio e senza le necessarie misure di mitigazione espone l'amministrazione a responsabilità civili e penali in caso di danni alla salute del personale.

L'adozione di *jammer* in ambienti chiusi come le carceri comporta dunque non solo una perdita di efficacia operativa, ma anche seri rischi per la salute e la sicurezza di tutti gli occupanti, rendendoli uno strumento non sostenibile nel medio-lungo termine. La questione non è solo tecnica ma anche etica: è accettabile esporre centinaia di persone (personale e detenuti) a rischi sanitari significativi per contrastare un fenomeno che potrebbe essere affrontato con strumenti alternativi privi di questi effetti collaterali?

2.4
I problemi legali e regolamentari

L'impiego di *jammer* in Italia è soggetto a una disciplina molto restrittiva, priva di alcuna deroga per strutture penitenziarie o reparti interforze. Questo aspetto, spesso sottovalutato nel dibattito pubblico, rappresenta un vincolo insormontabile per qualsiasi ipotesi di utilizzo sistematico di questi dispositivi.

In base al D.Lgs. 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche), qualsiasi dispositivo che emetta onde radio in banda non licenziata - compresi i *jammer* - è vietato se non rientra nelle "autorizzazioni generali" o non possiede un provvedimento ministeriale *ad hoc*.

La norma è chiara e non ammette interpretazioni estensive: l'emissione di segnali radio è un'attività soggetta a licenza, e l'emissione finalizzata a disturbare comunicazioni altrui è doppiamente vietata.

Contrariamente a quanto talvolta si ritiene, non esistono esenzioni automatiche per carceri, forze di polizia o reparti militari. L'unico uso legittimo di *jammer* è quello previsto da leggi primarie o da decreti ministeriali specifici, con vincoli stringenti su potenza, durata e modalità d'impiego.

In assenza di tali provvedimenti - che nel caso delle carceri italiane non risultano essere stati emanati con la necessaria completezza - l'utilizzo rimane tecnicamente illegale.

Sul fronte delle **sanzioni amministrative**, l'art. 102 del D.Lgs. 259/2003 prevede che chi installa o esercisce un dispositivo di trasmissione radio (inclusi i *jammer*) senza diritto d'uso della frequenza sia punito con sanzione pecuniaria da 1.000 a 10.000 euro. Chi esercisce senza autorizzazione generale incorre in sanzioni da 300 a 3.000 euro. Queste sanzioni

possono essere applicate per ogni singolo apparato installato e per ogni periodo di funzionamento, con effetti potenzialmente molto rilevanti sul piano economico. La violazione delle norme sulla sicurezza sul lavoro (D.Lgs. 81/2008) può inoltre comportare ulteriori multe e responsabilità civili per gli enti pubblici che non rispettano i limiti di esposizione ai campi elettromagnetici.

Sul piano **penale**, l'art. 340 del Codice Penale punisce con la reclusione fino a un anno chiunque cagiona un'interruzione o turba la regolarità di un ufficio o servizio pubblico o di un servizio di pubblica necessità. L'interferenza non selettiva dei *jammer*, qualora raggiunga reti civili, servizi di emergenza (118, polizia, vigili del fuoco) o sistemi di trasporto (ad esempio radiocomunicazioni ferroviarie), può configurare questo reato.

Non si tratta di un'ipotesi teorica: un *jammer* installato in un carcere situato in area urbana può facilmente interferire con le comunicazioni di emergenza nel raggio di diverse centinaia di metri, interessando abitazioni, esercizi commerciali e strade pubbliche.

L'art. 617-bis c.p., che punisce l'installazione di apparecchiature atte a impedire comunicazioni telegrafiche o telefoniche, rappresenta un'ulteriore fattispecie potenzialmente applicabile. La norma tutela la libertà e la segretezza delle comunicazioni, diritto costituzionalmente garantito dall'art. 15 della Costituzione, e la sua violazione può comportare conseguenze penali significative.

Qualora l'installazione sia disposta da figure apicali (direttore di istituto, provveditore regionale, dirigenti del DAP), anche la "catena di comando" può essere chiamata a rispondere, sia penalmente sia civilmente, per abuso d'ufficio o omissione di cautele. È quindi obbligatorio che ogni provvedimento comprenda un atto formale di autorizzazione da parte del Ministero delle Imprese e del Made in Italy (ex Ministero dello Sviluppo Economico), con definizione chiara delle aree di copertura, delle caratteristiche tecniche degli apparati, e delle misure di mitigazione adottate.

In sintesi, l'uso di *jammer* al di fuori delle casistiche espressamente previste dalla legge espone a un quadro sanzionatorio multiplo (amministrativo, civile e penale) e richiede garanzie procedurali stringenti che, nella pratica, si sono rivelate difficilmente realizzabili nel contesto operativo dell'amministrazione penitenziaria.

Capitolo 3

Il vantaggio dei rilevatori di radiofrequenze cellulari

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

3.1 Premessa

L'impiego di sistemi di monitoraggio passivo delle attività radio consente di superare radicalmente le criticità insite nei *jammer*, offrendo un approccio selettivo, sicuro e pienamente conforme alle normative vigenti. In particolare, i rilevatori basati su *software-defined radio* (SDR) rappresentano oggi lo stato dell'arte tecnologico e garantiscono vantaggi significativi su tutti i fronti critici analizzati nei capitoli precedenti.

3.2 Analisi passiva, non invasiva

La differenza fondamentale tra *jammer* e rilevatori passivi sta nel principio di funzionamento. Un rilevatore SDR passivo (quale ad esempio HackRF abbinato a *software* di analisi dedicato) non emette alcun segnale, limitandosi ad "ascoltare" le trasmissioni presenti nel raggio d'azione. Non disturba, non interferisce, non blocca: osserva. Questa caratteristica apparentemente semplice ha implicazioni profonde. Grazie al campionamento diretto dello spettro RF, un sistema di rilevazione passiva può identificare in tempo reale la presenza di terminali LTE/UMTS/GSM anche se criptati o dotati di

SIM non registrate. Il sistema non ha bisogno di "conoscere" il telefono per rilevarlo: è sufficiente che il dispositivo tenti di comunicare con una cella telefonica perché la sua presenza venga registrata.

L'analisi dell'attività in *uplink* - ovvero delle trasmissioni dal telefono verso la cella - consente di identificare *ping* di rete, SMS, *handshake* di sessione dati e chiamate voce attraverso l'analisi dei pattern caratteristici di ciascun tipo di comunicazione. Ogni tecnologia (GSM, UMTS, LTE) ha una "firma" riconoscibile che consente al sistema di classificare automaticamente il tipo di attività rilevata.

Particolarmente importante è la capacità di determinare il luogo e l'orario di prima attivazione del dispositivo. Mediante correlazione dei livelli di potenza rilevati da più sensori (triangolazione) o attraverso l'uso di antenne direzionali e *array*, è possibile localizzare con precisione crescente il punto di trasmissione. Nei test condotti, l'accuratezza ha raggiunto i 5 metri, sufficiente per identificare la cella detentiva o il settore dell'istituto da cui proviene il segnale.

Questo approccio non altera né interrompe le comunicazioni legittime - quelle del personale, dei visitatori, dei sistemi di emergenza e dei dispositivi medici - eliminando alla radice tutti i problemi di interferenza che affliggono i *jammer*.

Permette inoltre di costruire un *log* cronologico dettagliato di tutti gli eventi radio rilevati, creando una base documentale solida per eventuali procedimenti disciplinari o penali. Gli interventi di bonifica possono così essere concentrati esclusivamente sui segnali sospetti, riducendo drasticamente tempi, costi e rischi per la salute e la sicurezza complessiva dell'istituto.

3.3 Intelligenza operativa

Gli avanzati sistemi di rilevazione passiva non si limitano a "sentire" il segnale grezzo, ma integrano moduli di analisi sofisticati in grado di trasformare i dati RF in informazioni operative immediatamente utilizzabili dal personale di sicurezza.

Gli algoritmi di correlazione con celle telefoniche note rappresentano una delle funzionalità più utili. Ogni operatore mobile gestisce una rete di celle (BTS/*NodeB*/*eNodeB*) le cui caratteristiche sono note e mappabili. Il sistema può associare ogni trasmissione rilevata al sito cellulare di appartenenza, permettendo di identificare non solo la presenza di un telefono attivo ma anche l'operatore utilizzato e, in alcuni casi, di stimare la direzione verso cui il dispositivo sta comunicando.

La configurazione di soglie e *alert* su attività sospette consente di generare notifiche immediate quando si verificano pattern anomali.

È possibile, ad esempio, impostare allarmi per attività notturne (quando teoricamente i detenuti dovrebbero dormire), per picchi di traffico SMS (che potrebbero indicare coordinamento di attività illecite), o per la comparsa di nuovi dispositivi non precedentemente rilevati. Il personale di sorveglianza può così concentrare l'attenzione sugli eventi più significativi, senza dover monitorare continuamente un flusso indifferenziato di dati.

L'analisi cronologica per la ricostruzione di *pattern* d'uso rappresenta uno strumento investigativo di grande valore. Correlando l'attività rilevata nel tempo, è possibile evidenziare orari ricorrenti di utilizzo, identificare possibili turni di "passaggio" del telefono tra detenuti, riconoscere finestre temporali che coincidono con de-

terminati eventi (cambio turno del personale, orari dei pasti, visite dei familiari). Queste informazioni possono orientare sia le attività di perquisizione sia eventuali indagini su complicità interne.

3.4
Rispetto delle norme

L'adozione di rilevatori passivi garantisce piena conformità al quadro legislativo vigente e tutela i diritti fondamentali di tutte le persone coinvolte, aspetto che - come abbiamo visto - rappresenta uno dei punti più critici nell'impiego dei *jammer*.

Non emettendo alcuna trasmissione, i sistemi di rilevazione passiva non ostacolano in alcun modo le chiamate d'emergenza, le reti civili o i sistemi sanitari di monitoraggio remoto. Un rilevatore passivo è, dal punto di vista elettromagnetico, equivalente a una radio FM che si limita a ricevere le stazioni senza trasmetterne di proprie. Non serve alcuna autorizzazione per l'ascolto dello spettro radio, così come non serve autorizzazione per possedere un apparecchio radio.

Sul fronte della tutela della *privacy*, l'analisi si limita all'identificazione di tecnologia attiva (MAC *address* RF, livelli di potenza, celle di appartenenza) senza intercettare contenuti o conversazioni. Il sistema non "ascolta" cosa viene detto al telefono, ma solo che un telefono sta trasmettendo. Questa distinzione è fondamentale: l'intercettazione del contenuto delle comunicazioni richiede autorizzazione dell'autorità giudiziaria, mentre la mera rilevazione della presenza di un dispositivo trasmittente è un'attività di sicurezza che non presenta profili di illegittimità.

La compatibilità con le infrastrutture esistenti rappresenta un ulteriore vantaggio operativo. I sistemi di rilevazione passiva possono essere integrati con reti di videosorveglianza IP, sistemi di controllo accessi e piattaforme di sicurezza già in uso negli istituti penitenziari, confluendo in un'unica *console* di monitoraggio centralizzato.

L'investimento richiesto può così essere ottimizzato, evitando duplicazioni e sfruttando competenze già presenti nell'organizzazione.

Capitolo 4

Case study: test sperimentali in ambiente controllato

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

4.1 Premessa

Per validare l'efficacia dei sistemi di rilevazione passiva in condizioni realistiche, sono stati condotti *test* approfonditi utilizzando *hardware* HackRF One presso un sito isolato appositamente predisposto. L'obiettivo era verificare la capacità del sistema di rilevare, classificare e localizzare attività cellulare non autorizzata in un ambiente che simulasse le condizioni operative di un istituto penitenziario.

4.2 L'ambiente di test

Per sviluppare e valutare il sistema di rilevamento in condizioni controllate, è stato creato un ambiente isolato completamente privo di copertura cellulare legittima, caratteristiche che lo rendevano analogo a un'ala carceraria idealmente schermata. In questo spazio "pulito" dal punto di vista elettromagnetico, ogni segnale radio percepito nelle bande cellulari proveniva necessariamente da un telefono di prova introdotto deliberatamente, eliminando qualsiasi ambiguità nell'interpretazione dei risultati.

Sono stati introdotti in modo casuale più telefoni di diversi operatori (Vodafone, TIM, WindTre, Iliad) in vari momenti della giornata e della notte, simulando l'accensione spo-

radica e imprevedibile dei dispositivi da parte di uno o più detenuti. L'uso dei telefoni è stato distribuito nel tempo secondo *pattern* variabili, talvolta concentrato nelle ore diurne, talaltra nelle ore notturne, per ricreare le condizioni di imprevedibilità che caratterizzano l'uso reale dei telefoni di contrabbando. Questo *setup* ha permesso di mettere alla prova il sistema nelle stesse condizioni operative di un vero carcere.

4.3
Sorveglianza continua dello spettro

All'interno dell'area simulata, il sistema ha monitorato ininterrottamente tutte le bande cellulari rilevanti (700, 800, 900, 1800, 2600 MHz) oltre alle frequenze Wi-Fi e *Bluetooth*, 24 ore su 24, 7 giorni su 7.

La sorveglianza continua è essenziale perché un telefono di contrabbando potrebbe trasmettere solo per pochi secondi in orari totalmente inaspettati: una chiamata breve alle 3 di notte, un SMS inviato durante il cambio turno, una sessione dati di pochi minuti durante l'ora d'aria.

Nella pratica carceraria reale si impiegano più sonde o antenne distribuite strategicamente nell'istituto, convogliando i dati su una console centrale per garantire che nessuna zona resti scoperta. Non appena un telefono avvia una chiamata, invia un SMS o si collega ai dati mobili, i suoi segnali RF di *uplink* vengono captati in tempo reale. In un ambiente privo di segnali cellulari legittimi, ogni *burst* di trasmissione risalta in modo netto e inequivocabile, come una luce accesa in una stanza buia.

4.4 Registrazione automatica e post analisi

Ogni evento RF catturato durante i *test* è stato registrato automaticamente dal sistema, generando un *log* cronologico completo con data, ora precisa al secondo, frequenza/banda di trasmissione, potenza del segnale ricevuto e classificazione automatica del tipo di attività (chiamata voce GSM, chiamata voce LTE, SMS, traffico dati). Ogni attivazione dei telefoni di prova ha creato un *record* dettagliato e permanente nel *database* del sistema.

Questo approccio garantisce che anche se il personale di sorveglianza non dovesse intervenire immediatamente - per qualsiasi ragione - l'attività rimane tracciata e consultabile in seguito per analisi forensi, procedimenti disciplinari o indagini penali. Il *log* costituisce una prova documentale solida, con *timestamp* verificabili e dati oggettivi non soggetti a interpretazione.

L'interfaccia del sistema permette di navigare agevolmente nei dati storici, selezionando data e ora per ottenere un resoconto visivo degli eventi rilevati in qualsiasi periodo. È possibile, ad esempio, ispezionare le ore notturne di un determinato giorno per verificare eventuali trasmissioni, o confrontare l'attività di settimane diverse per identificare *pattern* ricorrenti. Una *timeline* grafica mostra i *burst* rilevati con indicazione del tipo e della potenza, mentre filtri configurabili permettono di isolare le trasmissioni per operatore, per banda o per tipologia di traffico.

4.5
Sistema di rilevamento inelligente

Il cuore della soluzione testata è un motore di analisi intelligente che riconosce automaticamente le firme RF caratteristiche di chiamate GSM, SMS e traffico dati LTE/4G. Diversi tipi di trasmissione presentano *pattern* distintivi: una chiamata vocale LTE genera un flusso continuo di pacchetti su bande specifiche con caratteristiche temporali riconoscibili, mentre un SMS produce un *burst* breve e concentrato. Il traffico dati presenta *pattern* ancora diversi, variabili in funzione dell'applicazione utilizzata.

Il *software* classifica automaticamente l'attività rilevata sulla base di questi *pattern*, minimizzando i falsi allarmi e riducendo il carico di lavoro interpretativo per il personale di sorveglianza. Durante i *test*, ogni volta che i telefoni di prova avviavano una chiamata, inviavano un messaggio o generavano traffico dati, il sistema identificava correttamente il tipo di evento e generava una notifica appropriata.

Gli algoritmi avanzati implementati nel sistema sono inoltre in grado di distinguere i segnali autorizzati (radio di servizio del personale, Wi-Fi della rete interna, dispositivi IoT legittimi) da quelli illeciti, mantenendo alta l'affidabilità delle segnalazioni ed evitando di sommergere gli operatori con allarmi irrilevanti.

Il sistema ha dimostrato capacità di gestire efficacemente anche situazioni complesse, come l'attivazione simultanea di più dispositivi. Quando due telefoni venivano accesi contemporaneamente in punti diversi dell'area di *test*, entrambi gli eventi venivano rilevati, classificati e *loggati* separatamente, ciascuno con il proprio operatore, la propria banda e la propria stima di localizzazione.

4.6 Architettura di collegamento e sicurezza operativa

L'implementazione di sonde RF in ambiente penitenziario reale richiede particolare attenzione al trasporto dei dati e alla compatibilità elettromagnetica complessiva del sistema. L'utilizzo di connessioni *wireless* per il collegamento delle sonde alla centrale di monitoraggio è tecnicamente sconsigliato: tali segnali potrebbero interferire con le analisi di spettro generando falsi positivi, e in alcuni casi potrebbero violare le stringenti *policy* di sicurezza del Ministero della Giustizia.

Per questo motivo, l'architettura raccomandata prevede un sistema interamente cablato, preferibilmente tramite fibra ottica. Questa soluzione garantisce totale immunità da emissioni RF (la fibra trasmette luce, non onde radio), elevata sicurezza contro intercettazioni (il segnale ottico non può essere captato senza interrompere fisicamente la fibra), e lunga portata senza degrado del segnale. In alternativa, laddove la posa in fibra non sia praticabile per vincoli architettonici o di costo, è accettabile l'uso di cavi *Ethernet* schermati (Cat6a STP) in canaline protette.

Ogni sonda può operare in due modalità distinte a seconda delle esigenze operative e delle caratteristiche dell'istituto. La modalità online cablata prevede l'invio continuo dei *log* verso la centrale di monitoraggio tramite *switch* PoE o *uplink* in fibra, consentendo il monitoraggio in tempo reale. La modalità *offline* prevede invece la memorizzazione locale cifrata dei dati e il successivo scarico fisico del *file* di *log* mediante connessione diretta USB o SSD rimovibile, seguendo rigorose procedure di catena di custodia per garantire l'utilizzabilità forense dei dati.

La centrale di controllo deve essere collocata in area tecnica protetta, accessibile solo a personale autorizzato, e deve ricevere i dati attraverso canali fisici isolati.

La cifratura *end-to-end* e la sincronizzazione dei *timestamp* tramite sorgenti affidabili (*server* NTP autenticato o *clock* OCXO di alta precisione) completano il quadro delle garanzie di sicurezza e integrità dei dati. Questa architettura elimina qualunque necessità di trasmissione radio da parte del sistema di monitoraggio, mantenendolo totalmente passivo, sicuro e *forense-compliant*. Il principio operativo può essere sintetizzato nella formula: «Osservare senza interferire».

Conclusioni

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

L'analisi condotta in questo articolo ha messo in luce, con dati di fatto e considerazioni tecniche approfondite, i molteplici limiti e i rischi connessi all'impiego di *jammer* nelle carceri italiane, contrapposti alle potenzialità concrete di una strategia basata sulla rilevazione passiva delle attività radio mobili.

Sintesi dei limiti dei jammer

L'efficacia operativa dei *jammer* risulta fortemente ridotta dalle tipiche barriere architettoniche dei penitenziari - muri spessi in calcestruzzo armato, strutture metalliche, configurazioni planimetriche complesse - che causano inevitabili zone d'ombra dove il segnale di disturbo non arriva o è insufficiente. L'evoluzione continua delle reti mobili verso 4G/5G e oltre obbliga a costanti aggiornamenti *hardware* e *software*, con costi aggiuntivi significativi e periodi di fermo operativo durante i quali il sistema è inefficace.

L'impatto indiscriminato su tutte le trasmissioni RF genera effetti collaterali inaccettabili sulle comunicazioni di emergenza, sui dispositivi medici, sulla strumentazione di sicurezza interna e sulle comunicazioni legittime di personale, visitatori e operatori esterni. I rischi per la salute legati alle emissioni elettromagnetiche di potenza elevata sollevano questioni etiche e giuridiche che non possono essere ignorate, mentre il quadro sanzionatorio multiplo - amministrativo, civile e penale - espone l'amministrazione e i singoli responsabili a conseguenze potenzialmente gravi.

I vantaggi strategici della rilevazione passiva

I rilevatori SDR passivi offrono invece un paradigma completamente diverso, caratterizzato da non invasività e piena conformità normativa, precisione e granularità nella raccolta dei dati, intelligenza operativa avanzata con algoritmi di *machine learning* e *pattern recognition*, e una scalabilità che consente l'integrazione fluida con le piattaforme di sicurezza già esistenti negli istituti.

Il passaggio dai *jammer* ai sistemi di rilevazione passiva non è semplicemente un aggiornamento tecnologico: rappresenta un cambio di filosofia operativa, dalla logica del

"bloccare tutto" a quella del "comprendere per intervenire". Il primo approccio è rozzo, inefficiente e rischioso; il secondo è intelligente, mirato e sostenibile.

Raccomandazioni operative

Per tradurre questi vantaggi in pratica operativa, si propone un percorso articolato in fasi successive. La prima fase dovrebbe consistere in una mappatura preliminare del rischio RF in ogni ala carceraria, con rilievo dello spettro esistente, identificazione delle frequenze "pulite" e dei punti critici, e definizione di un piano di posizionamento delle sonde con criteri di ridondanza.

L'implementazione graduale del sistema di rilevazione dovrebbe poi procedere attraverso un pilotaggio iniziale in 2-3 istituti di diversa tipologia (alta, media e bassa sicurezza), seguito da un *roll-out* esteso su tutte le sedi con *training on-site* per il personale, e infine da una fase di monitoraggio e revisione periodica con *upgrade software* e affinamento degli algoritmi. Fondamentale è l'investimento in formazione degli operatori e nella definizione di procedure standardizzate: addestramento specifico sull'uso delle interfacce, sull'interpretazione dei *log* e sui protocolli d'intervento in caso di rilevazione sospetta. Le politiche di *governance* dovrebbero includere la stipula di convenzioni con fornitori di tecnologia SDR comprendenti certificazioni di conformità CE e documentazione tecnica completa.

Un piano di comunicazione trasparente verso il personale penitenziario e le organizzazioni sindacali è essenziale per evitare resistenze culturali e false aspettative, chiarendo sia i benefici sia i limiti degli strumenti adottati.

Prospettive di sviluppo

Guardando al futuro, sarà necessario prevedere l'estensione della capacità di rilevazione alle bande emergenti che accompagneranno l'arrivo della tecnologia 6G e delle reti satellitari a bassa orbita. L'integrazione con intelligenza artificiale avanzata permetterà di sviluppare modelli predittivi capaci di anticipare comportamenti illeciti sulla base di *pattern* storici. Soluzioni *Platform as a Service* potrebbero ridurre i costi di

manutenzione e garantire aggiornamenti automatici. Collaborazioni con università e centri di ricerca potranno validare scientificamente le soluzioni e ottimizzare ulteriormente gli algoritmi.

Considerazione finale

La scelta degli apparati e delle strategie di controllo delle comunicazioni in carcere non è solo una questione tecnologica, ma un tema che investe sicurezza, salute pubblica, rispetto del diritto e qualità della *governance*. I *jammer*, pur apprezzati a suo tempo per l'immediatezza d'uso e la facilità di comunicazione politica, si sono dimostrati una soluzione parziale, rischiosa e sempre più obsoleta di fronte all'evoluzione delle tecnologie di comunicazione.

I sistemi di rilevazione passiva basati su SDR offrono invece un percorso innovativo e sostenibile, caratterizzato da selettività operativa (interventi mirati solo sui segnali sospetti), rispetto pieno delle normative (zero interferenze non autorizzate), tutela della salute (assenza di emissioni nocive), solidità delle evidenze documentali (*log* a prova di contestazione per procedimenti disciplinari o penali), e flessibilità di adattamento alle evoluzioni tecnologiche future.

Le soluzioni tecnologiche per contrastare efficacemente l'uso illecito di telefoni cellulari all'interno delle carceri esistono già, sono scientificamente validate e tecnicamente implementabili senza alcun rischio per la salute né interferenze sui servizi legittimi. Il problema, oggi, non è più tecnico ma politico e organizzativo. Continuare a considerare i *jammer* come soluzione "ufficiale" al problema dei cellulari in carcere rappresenta una sconfitta culturale prima ancora che ingegneristica: si sceglie di disturbare indiscriminatamente anziché comprendere selettivamente. Qualunque tecnico di sicurezza delle comunicazioni - che si occupi di SIGINT, TSCM o analisi elettromagnetica - sa perfettamente che la tecnologia per affrontare questo problema in modo intelligente ed efficace non manca: manca la volontà di applicarla.

«Il progresso non nasce dall'invenzione, ma dal coraggio di sostituire ciò che non funziona.»

Riferimenti bibliografici

Jammer nelle carceri:
limiti, rischi e alternative

a cura di STEFANO CANGIANO

Linee guida internazionali e standard di esposizione ai campi elettromagnetici

1. **ICNIRP** (2020). Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz). Health Physics, 118(5), 483–524.
DOI: 10.1097/HP.0000000000001210
PMID: 32167495
Disponibile in open access: https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf

2. **ICNIRP** (2020). Differences between the ICNIRP (2020) and previous guidelines. Documento esplicativo ufficiale.
URL: https://www.icnirp.org/en/differences.html

3. **ICNIRP** (2020). RF EMF Guidelines 2020 – Frequently Asked Questions.
URL: https://www.icnirp.org/en/activities/news/news-article/rf-guidelines-2020-published.html

Documentazione dell'Organizzazione Mondiale della Sanità (OMS/WHO)

4. **World Health Organization** (2024). Electromagnetic fields: health topics overview.
URL: https://www.who.int/health-topics/electromagnetic-fields

5. **World Health Organization** (2024). Radiation: Electromagnetic fields – Questions and Answers.
URL: https://www.who.int/news-room/questions-and-answers/item/radiation-electromagnetic-fields

6. **World Health Organization** (1996-ongoing). The International EMF Project.
URL: https://www.who.int/initiatives/the-international-emf-project

7. **World Health Organization – Department of Environment, Climate Change and Health** (2024). Electromagnetic fields and public health.
URL: https://www.who.int/teams/environment-climate-change-and-health/radiation-and-health/non-ionizing/emf

Pareri scientifici della Commissione Europea

8. **Scientific Committee on Emerging and Newly Identified Health Risks – SCENIHR** (2015). Opinion on Potential Health Effects of Exposure to Electromagnetic Fields (EMF). European Commission, Directorate-General for Health and Consumers.
ISBN: 978-92-79-30134-6
URL: https://health.ec.europa.eu/latest-updates/scenihr-final-opinion-potential-health-effects-exposure-electromagnetic-fields-emf-2015-03-06_en

9. **SCENIHR** (2015). Potential health effects of exposure to electromagnetic fields – Factsheet for citizens.
URL: https://ec.europa.eu/health/scientific_committees/opinions_layman/electromagnetic-fields2015/en/

10. **Scientific Committee on Health, Environmental and Emerging Risks – SCHEER** (2023). Preliminary Opinion on potential health effects of exposure to electromagnetic fields (EMF): Update with regard to frequencies

between 1 Hz and 100 kHz. European Commission.
URL: https://health.ec.europa.eu/consultations/scheer-public-consultation-preliminary-opinion-potential-health-effects-exposure-electromagnetic_en

Quadro normativo italiano

11. **Decreto Legislativo 1° agosto 2003, n. 259** – Codice delle comunicazioni elettroniche. Gazzetta Ufficiale della Repubblica Italiana.
URL: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259

12. **Ministero delle Imprese e del Made in Italy – MIMIT** (2024). Piano Nazionale di Ripartizione delle Frequenze (PNRF).
URL: https://www.mimit.gov.it/it/digitale/gestione-spettro-radio/piano-nazionale-ripartizione-frequenze

13. **Autorità per le Garanzie nelle Comunicazioni – AGCOM** (2024). Gestione delle frequenze.
URL: https://www.agcom.it/competenze/comunicazioni-elettroniche/reti/frequenze

14. **Decreto Legislativo 9 aprile 2008, n. 81** – Testo unico sulla salute e sicurezza sul lavoro. Titolo VIII, Capo IV: Protezione dei lavoratori dai rischi di esposizione a campi elettromagnetici.
URL: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2008-04-09;81

Normativa e avvisi delle autorità statunitensi sui jammer

15. **Federal Communications Commission – FCC** (2024). Jammer Enforcement.
URL: https://www.fcc.gov/general/jammer-enforcement

16. **Federal Communications Commission – FCC** (2024). Jammers – Enforcement Areas.
URL: https://www.fcc.gov/enforcement/areas/jammers

17. **Federal Communications Commission – FCC** (2014, aggiornato 2024). Enforcement Advisory: Warning – Jammer Use by the Public and Local Law Enforcement Is Illegal.
Document DA-14-1785A1
URL: https://www.fcc.gov/document/warning-jammer-use-public-and-local-law-enforcement-illegal

18. **Federal Communications Commission – FCC** (2024). Cell Phone and GPS Jamming – Consumer Information.
URL: https://www.fcc.gov/general/cell-phone-and-gps-jamming

19. **Federal Communications Commission – FCC** (2024). Jamming Cell Phones and GPS Equipment is Against the Law – Consumer Alert.
URL: https://www.fcc.gov/general/jamming-cell-phones-and-gps-equipment-against-law

20. **U.S. Department of Homeland Security & Federal Communications Commission** (2025). JAMMING? Understanding the Risks – Infographic for First Responders.

URL: https://www.dhs.gov/sites/default/files/2025-01/25_0115_st_DHS-FCC_joint_jammer_infographic_0.pdf

21. **U.S. Department of Homeland Security – Science & Technology Directorate** (2022). JamX 22: Counter-Jamming Event – Fact Sheet.
URL: https://www.dhs.gov/sites/default/files/2022-02/Factsheet_JamX%2022_508.pdf

Studi sperimentali sugli effetti biologici dei jammer

22. **Rafati, A., Rahimi, S., Talebi, A., Soleimani, A., Haghani, M., & Mortazavi, S. M. J.** (2015). Exposure to Radiofrequency Radiation Emitted from Common Mobile Phone Jammers Alters the Pattern of Muscle Contractions: an Animal Model Study. Journal of Biomedical Physics and Engineering, 5(3), 133–142.
PMID: 26396969
PMCID: PMC4576874
URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC4576874/

23. **Shojaeifard, M. B., Jarideh, S., Owjfard, M., Nematollahii, S., Talaei-Khozani, T., & Malekzadeh, M.** (2018). Electromagnetic Fields of Mobile Phone Jammer Exposure on Blood Factors in Rats. Journal of Biomedical Physics and Engineering, 8(4), 403–408.
PMID: 30568930
PMCID: PMC6280113
URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6280113/

24. **Shekoohi Shooli, F., Mortazavi, S. A. R., Jarideh, S., Nematollahii, S., Yousefi, F., Haghani, M., Mortazavi, S. M. J., & Shojaei-Fard, M. B.** (2016). Short-term Exposure to Electromagnetic Fields Generated by Mobile Phone Jammers Decreases the Fasting Blood Sugar in Adult Male Rats. Journal of Biomedical Physics and Engineering, 6(1), 27–32.
PMID: 27026952
PMCID: PMC4795326
URL: https://europepmc.org/article/pmc/4795326

25. **Yazdanpanahi, M., Namazi, A., Shojaeifard, M. B., Nematolahi, S., & Pourahmad, S.** (2023). Evaluating the Effect of Jammer Radiation on Learning and Memory in Male Rats. Journal of Biomedical Physics and Engineering, 13(1), 29–38.
PMID: 36818009
PMCID: PMC9923240
URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9923240/

26. **Mortazavi, S. M. J., Rahimi, S., Talebi, A., Soleimani, A., & Rafati, A.** (2015). Survey of the Effects of Exposure to 900 MHz Radiofrequency Radiation Emitted by a GSM Mobile Phone on the Pattern of Muscle Contractions in an Animal Model. Journal of Biomedical Physics and Engineering, 5(3), 121–132.
PMID: 26396968
PMCID: PMC4576873
URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC4576873/

Rassegne scientifiche recenti su campi elettromagnetici e 5G

27. **Korkmaz, E., Yilmaz, H., & Comlekci, S.** (2024). A comprehensive review of 5G NR RF-EMF exposure assessment tools and measurement methodologies. Environmental Research, 263, 120128.
DOI: 10.1016/j.envres.2024.120128
URL: https://www.sciencedirect.com/science/article/pii/S0013935124014294

28. **International Telecommunication Union – ITU** (2022). Report ITU-R SM.2452-1: Electromagnetic field measurements to assess human exposure from radio base stations.
URL: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2452-1-2022-PDF-E.pdf

Fonti documentali sul caso italiano (jammer nelle carceri)

29. **POLPENUIL – Sindacato Polizia Penitenziaria UIL** (2018). Acquisizione sistemi inibitori di telefoni cellulari (jammer) – Circolare.
URL: https://www.polpenuil.it/circolari/8698-acquisizione-sistemi-inibitori-di-telefoni-cellulari-jammer.html

30. **POLPENUIL – Il Sole 24 Ore** (2018). Blocco telefoni carcere jammer – Ricostruzione documentale.
URL: https://www.polpenuil.it/images/blocco_telefoni_carcere_jammer_sole_24.pdf

31. **Camera dei Deputati** (2023). Resoconto stenografico dell'Assemblea – Seduta n. 452, Allegato A.

URL: https://documenti.camera.it/leg19/resoconti/assemblea/html/sed0452/leg.19.sed0452.allegato_a.pdf

32. **HuffPost Italia** (13 febbraio 2025). In carcere c'è campo: telefonini sempre più diffusi, 47 jammer comprati inutilizzabili. Si torna a perquisire.
URL: https://www.huffingtonpost.it/esteri/2025/02/13/news/in_carcere_ce_campo_telefonini_sempre_piu_diffusi_47_jammer_comprati_inutilizzabili_si_torna_a_perquisire-18424329/

33. **Ristretti Orizzonti** (2025). Boss al telefono in carcere: lo Stato rottama il sistema di schermatura mai partito.
URL: https://ristretti.org/boss-al-telefono-in-carcere-lo-stato-rottama-il-sistema-di-schermatura-mai-partito

34. **Polizia Penitenziaria – Rivista online** (2024). Gratteri: nuovo appello per l'utilizzo degli jammer per bloccare uso dei telefonini in carcere – Utilizzare risorse del PNRR.
URL: https://www.poliziapenitenziaria.it/gratteri-nuovo-appello-per-lutilizzo-degli-jammer-per-bloccare-uso-dei-telefonini-in-carcere-utilizzare-risorse-del-pnrr/

Riferimenti normativi del Codice Penale italiano

35. **Art. 340 c.p.** – Interruzione di un ufficio o servizio pubblico o di un servizio di pubblica necessità.
Testo vigente consultabile su: https://www.brocardi.it/codice-penale/libro-secondo/titolo-ii/capo-i/art340.html

36. **Art. 617-bis c.p.** – Installazione di apparecchiature atte a intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche.
Testo vigente consultabile su: https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617bis.html

6 - 7 maggio 2026

AUDITORIUM DELLA TECNICA, ROMA

CYBER CRIME CONFERENCE

14ª EDIZIONE

ICTSECURITYMAGAZINE.COM