Rivista Italiana di
Public Management

Vol. 3, n. 2 | 2020

La gestione delle "Infrastrutture critiche" durante la crisi Covid

Roberto Setola*

Abstract

In Italy, the first wave of the Covid-19 pandemic and the consequent lockdown period resulted in no interruptions in the provision of essential services to the population. This was made possible – in spite of the abnormal and highly complex situation – thanks to the policies adopted by the various operators and to effective Public Private Partnership (PPP) as illustrated in this article. After providing an overview of what is meant by the term "Critical Infrastructures," this article goes on to illustrate the main actions implemented by operators during the pandemic, along with the initiatives taken by public authorities – initiatives that, on the whole, have been found effective in ensuring continuity in the provision of essential services to the population.

Keywords: *crisis management, control room, essential services, service continuity.*

Durante la fase di lockdown non si è registrata alcuna interruzione nell'erogazione dei "Servizi essenziali". Questo è stato possibile, nonostante la complessità della situazione, grazie alle politiche adottate dai diversi operatori e dalla collaborazione in essere con le autorità pubbliche. L'articolo, dopo aver fornito un inquadramento di ciò che si intente per "Infrastrutture critiche", intende illustrare le principali azioni messe in atto dagli operatori durante la pandemia, unitamente alle iniziative adottate dalle autorità pubbliche; iniziative che nel loro complesso si sono rilevate efficaci nel garantire la continuità di erogazione alla popolazione dei "Servizi essenziali".

Keywords*: crisis management, sala di controllo, servizi essenziali, infrastrutture critiche.*

** Università CAMPUS Bio-Medico di Roma*

Introduzione

L'esperienza Covid-19 ha messo in evidenza da un lato la strategicità delle cosiddette "Infrastrutture critiche" e dall'altro la complessità della loro gestione legata all'esistenza di un intrigato insieme di interazioni ed interdipendenze. Il Covid ha, inoltre, fatto accrescere la consapevolezza negli operatori delle "Infrastrutture critiche" della centralità del fattore umano, quale elemento imprescindibile per la loro gestione.

È emerso, inoltre, con evidenza la carenza nel nostro ordinamento di una norma specifica che individui e contraddistingua quali siano le "Infrastrutture critiche" nazionali. Infatti, sebbene sia stato recepito con il d. lgs. 61/2011 la Direttiva europea in tema di "Infrastrutture critiche europee" (Ice), non esiste ancora una norma per quel che riguarda le infrastrutture nazionali.

Questi aspetti sono emersi con tale rilevanza durante l'emergenza che il legislatore ha sentito la necessità di normare la tematica mediante l'art. 211*bis* "Continuità dei servizi erogati dagli operatori di "Infrastrutture critiche" del d.l. 19/05/2020, n. 34 (il così detto decreto "Rilancio"). Tale articolo impone agli operatori di "Infrastrutture critiche" di inserire in modo esplicito nei loro piani di sicurezza, cioè all'interno del "Piano di sicurezza dell'operatore" (Pso), misure di gestione delle crisi derivanti da emergenze di natura sanitaria. Per ciò che attiene in particolare la gestione dell'emergenza Covid, l'operatore di "Infrastrutture critiche" dovrà tener conto delle linee guida emanate dai ministeri competenti e dai "Principi precauzionali" elaborati dalla Presidenza del Consiglio dei Ministri (Segreteria "Infrastrutture critiche", 2020). La norma, nelle more dell'emanazione di una normativa organica sulla materia, individua per l'applicazione del suddetto articolo, quali operatori di "Infrastrutture critiche", coloro che[1]:

- Gestiscono le infrastrutture individuate come critiche dai decreti dirigenziali del Ministero dello Sviluppo Economico e dal Ministero delle Infrastrutture e dei Trasporti ai sensi del d.lgs. 61/2011 (Direttiva "Infrastrutture critiche europee");

- Gli operatori di servizi essenziali e i fornitori di servizi digitali individuati ai sensi del d. lgs. 65/2018 (Direttiva NIS);

- Le società e gli enti che gestiscono i sistemi spaziali di interesse nazionale ed europeo.

Il legislatore ha, inoltre, dato facoltà al Presidente del Consiglio dei Ministri di designare ulteriori "Infrastrutture critiche" con proprio Dpcm su proposta dei ministeri competenti.

1. La lista degli operatori, così come l'indicazione puntuale degli elementi individuati come "Infrastrutture critiche", non è disponibile in quanto dato classificato.

La *ratio* della norma non risiede solo nella volontà di evidenziare la necessità/obbligo da parte degli operatori di "Infrastrutture critiche" di dotarsi di un adeguato piano di gestione delle emergenze pandemiche, ma anche quello di favorire, come specificato nei commi 2 e 4, di una sinergia pubblico-privato con l'obiettivo di garantirne la continuità operativa. Tale obiettivo si fonda da un lato su alcuni obblighi posti a carico degli operatori di "Infrastrutture critiche", e dall'altro dalla emanazione da parte dei ministeri competenti di specifiche direttive tese a favorire l'adozione di quanto necessario per il corretto funzionamento di queste infrastrutture. Il tutto con una visione olistica e inter-ministeriale che consente di cogliere in un quadro unitario i diversi aspetti, superando in parte la visione parcellizzata dei singoli dicasteri consentendo una maggiore comprensione della valenza sistemica delle "Infrastrutture critiche". Infatti, come meglio illustrato nel corpo dell'articolo, l'emergenza ha evidenziato come la complessità organizzativa e funzionale di tali sistemi richieda l'adozione di specifiche iniziative che, in alcuni casi, hanno necessità di operare in deroga rispetto alla gestione ordinale dell'emergenza pandemica.

L'insieme di queste iniziative, unitamente alle strategie ed alla professionalità messa in campo dagli operatori di "Infrastrutture critiche" ha fatto sì che non solo i diversi servizi essenziale siano stati erogati con continuità durante l'emergenza, ma anche che il tasso di contagio del personale operante in queste infrastrutture, nonostante la necessità di operare in situazione di esposizione a rischio di contagio maggiore della media della popolazione, è risultato inferiore, e in alcuni casi anche in modo estremamente significativo, rispetto alla media nazionale/locale.

Questo è stato il frutto di una strategia che si è delineata nel corso degli anni e che ha visto la proficua collaborazione in primo luogo privato-privato e poi anche pubblico-privato oltre che l'adozione da parte dei diversi operatori di adeguate iniziative che hanno potuto contare in modo significativo sullo spirito di abnegazione e coinvolgimento dei propri dipendenti.

1. Stato dell'arte

Le problematiche connesse alla gestione delle "Infrastrutture critiche" trovano la loro genesi iniziale nella Direttiva "Critical infrastructure protection" (Pdd-63) emanata negli USA, dal presidente Clinton, nel 1998 (US Governemnt, 1998). Tale Direttiva si prefiggeva di mettere in atto quanto necessario per garantire che le interruzioni nell'erogazione dei servizi essenziali fossero infrequenti, limitate nel tempo e nello spazio e con minimo impatto sul benessere e la salute dei cittadini, la sicurezza, e l'economia nazionale.

La Pdd-63 nasceva dalla costatazione della crescente rilevanza di queste infrastrutture nei paesi sviluppati, dal fatto che la quasi totalità delle stesse è gestita/posseduta da sog-

getti privati e, soprattutto, che il loro assetto architetturale stava subendo un significativo mutamento. Infatti, in conseguenza di una serie di fenomeni sociologici, economici, culturali e tecnologici questi complessi sistemi, un tempo gestiti da operatori monopolistici nazionali con una organizzazione verticistica, autonoma e sostanzialmente autosufficiente, stavano divenendo sempre più interconnessi ed integrati (Setola, 2003).

La principale conseguenza di questo mutato assetto, in parte dovuta alla pervasiva introduzione di tecnologie proprie della *Information technology* (Ict), è la crescente presenza dei fenomeni di dipendenza ed interdipendenza. Ovvero che il singolo operatore di una infrastruttura critica necessita dei servizi erogati da altri operatori per poter erogare i propri. Tutto questo crea un complesso ed intrigato insieme di relazioni, come ben illustrato nell'articolo di (Rinaldi et al., 2001), che devono essere adeguatamente considerate e gestite per prevenire effetti "domino", ovvero che un evento negativo in una infrastruttura possa propagarsi ad altre compromettendo l'erogazione di un significativo insieme di servizi essenziali, come drammaticamente evidenziato dai black-out del 2003.

La presa di coscienza di questa necessità ha portato nel corso degli anni all'adozione da parte dei diversi governi ed organismi internazionali di specifiche iniziative quali la creazione del *Cybersecurity and Infrastructure Security Agency* (Cisa) negli USA, e alla emanazione della Direttiva europea sulle "Infrastrutture critiche" (2008/114/EC).

In particolare la Direttiva europea 2008/114/CE, recepita nell'ordinamento italiano con il d.lgs. 61/2011, indica come "Infrastrutture critiche": "infrastruttura, ubicata in uno Stato membro dell'Unione europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni". Definizione che, per altro, riprende quella presente già nel Pdd-63 emanata dal governo americano. Come può vedersi la definizione indentifica le "Infrastrutture critiche" come quegli enti necessari ad erogare o servizi vitali (oggi indicati come servizi essenziali) alla popolazione prospettando l'opportunità di adottare un approccio "All-Hazard" – ovvero considerando minacce di carattere naturale, antropico (sia accidentale che doloso) e tecnologico –. La Direttiva indicava che in sede di prima attuazione le "Infrastrutture critiche" dovevano essere individuate nell'ambito dei settori dell'energia e dei trasporti.

Tale direttiva ha avuto il pregio di sollecitare gli stati membri ad una riflessione sulla rilevanza delle "Infrastrutture critiche" e sulla conseguente necessità di una loro maggiore protezione sia in termini di robustezza nei confronti delle diverse minacce che di resilienza in presenza di eventi avversi. La quasi totalità degli stati membri – con l'eccezione dell'Italia – ha colto l'occasione del recepimento della direttiva per strutturare specifici assetti organizzativi tesi a migliorare la protezione oltre che delle "Infrastrutture critiche" europee anche di quelle nazionali. Iniziative che prevedono da un lato la disamina

dei rischi e delle minacce per le diverse infrastrutture, e dall'altro l'adozione da parte degli operatori di opportune contromisure per la mitigazione e gestione dei diversi rischi. Un comune denominatore in queste attività è una stretta cooperazione pubblico-privata sia nella fase di valutazione dei rischi che un costante *information sharing*. Per una disamina sulle iniziative adottate dai diversi paesi europei si rimanda al volume (Lazari, 2014)).

In parallelo a tali iniziative si è sviluppato uno specifico filone di ricerca che mira a comprendere il comportamento del complesso insieme di infrastrutture al fine di supportare i diversi stakeholder nella definizione di specifiche strategie per quel che riguarda gli aspetti di prevenzione, contrasto, repressione e ripristino rispetto ad eventi avversi in ottica di migliorarne della loro resilienza in una prospettiva "All-Hazard" (Lewis, 2019). Con un approccio in cui vengono considerare in modo unitario le diverse tipologie di minacce – indipendentemente dal fatto se esse siano di natura accidentale o dolosa, minacce fisiche, naturali o cyber in quanto l'obiettivo finale non è tanto e solo la protezione dell'infrastruttura e dei suoi singoli asset, quanto piuttosto la salvaguardia della loro capacità di erogare con continuità i propri servizi (essenziali); – quello che ci si prefigge è lo sviluppo di iniziative in grado di favorire/garantire la capacità di "service continuity" di queste infrastrutture a dispetto di eventi endogeni e/o esogeni sia di natura accidentale che dolosa (Yusta et al., 2011).

Occorre, però, evidenziare che, sebbene vi sia una significativa letteratura scientifica per quel che concerne la modellistica e l'analisi delle "Infrastrutture critiche" – per una disamina si veda (Setola et al., 2016) e (Ouyang, 2014) - il fattore umano è stato solo in parte analizzato e per lo più nell'ambito della dimensione *cyber* in termini di sua intrinseca vulnerabilità rispetto ad azioni dolose quali attacchi di *social engineering* (Corradini, 2020).

In questo quadro, l'impatto di un evento pandemico sulla capacità di erogazione dei servizi essenziali è stato preso in considerazione solo dopo l'esperienza dell'influenza aviaria (H1N1).

1.1. Attività sviluppate a valle della influenza aviaria (H1N1)

A partire dal 2009, alla luce della minaccia legata alla influenza aviaria (H1N1), è iniziata ad emergere la necessità di considerare, all'interno dei piani di *business continuity*, anche il fattore umano. Infatti, fino a quella data le diverse organizzazioni avevano predisposto procedure e piani per la gestione di eventi avversi focalizzati quasi esclusivamente sugli aspetti di tipo tecnologico e procedurale; sulla necessità/opportunità, cioè, di: eseguire *backup* e copie dei dati; dotarsi di siti di *disaster recovery*; ridondare i sistemi di comunicazione; migliorare la robustezza dei processi produttivi; creare postazioni di lavoro in altri siti per gestire l'eventuale indisponibilità di quello principale; etc. Il tutto, però, senza un'adeguata gestione delle problematiche del personale. Solo ragionando sullo scenario legato a quello influenzale ci si rese conto che, per ragioni di efficienza e razionalità –

soprattutto per alcune funzioni altamente qualificate – le aziende non possedevano una adeguata ridondanza in termini di operatori in grado di svolgere tali compiti. Il numero di operatori era, infatti, dimensionato rispetto alle normali esigenze lavorative, ma in presenza di un evento pandemico tale dimensionamento non consentiva di garantire la corretta gestione dell'infrastruttura; questo sia perché parte del personale poteva essere contagiato – e quindi non operativo – sia in relazione alle esigenze familiari dirette (assistenza a eventuali congiunti contagiati) e indirette (*childcare*) – ovvero causate da situazioni di stress emotivo che potrebbero indurre i lavoratori a comportamenti isterici (Zagaria, 2009). Questa problematica emerse con maggior rilevanza per le figure impegnate nelle sale di controllo dove la contaminazione di un soggetto poteva facilmente estendersi all'intera squadra e dove le competenze degli operatori ne rendono di fatto impossibile la sostituzione con altro personale.

Un altro aspetto non adeguatamente gestito riguardava le problematiche di mobilità sul territorio. Per esempio, se il suggerimento per la localizzazione di un sito di *disaster recovery* è quello di posizionarlo sufficientemente distante da quello principale in modo che non possa essere soggetto alle medesime avversità, questa ampia distanza può rendere complesso lo spostamento del personale soprattutto in situazioni di vincoli sulla mobilità.

Queste criticità furono oggetto, nel 2009, di specifiche analisi da parte del World Health Organization (Who) con riferimento alle possibili implicazioni che disservizi nelle "Infrastrutture critiche" avrebbero potuto avere sul sistema sanitario; tali criticità sono sintetizzate nel report "While-of-Society Pandemic Readiness" (Who, 2009) che dedica uno specifico capitolo alla gestione delle "Infrastrutture critiche" ed in particolare alle interdipendenze del settore sanitario da queste.

In quest'ottica il governo americano aveva avviato uno studio per comprendere le interdipendenze fra le diverse "Infrastrutture critiche" al fine di meglio indirizzare le azioni di contenimento e supporto (USA, 2007) anche sviluppando specifici strumenti di simulazione (Fair et al., 2007). In quello stesso periodo il Who aveva dato indicazioni alle singole nazioni di dotarsi di uno specifico piano per la gestione delle pandemie.

Purtroppo, passata la paura della aviaria (che ricordiamo era stata significativamente sovrastimata) il problema della gestione delle pandemie è andato nel dimenticatoio, come anche evidenziato dalla quasi totale assenza di documenti sia pubblici che di ricerca sul tema nel periodo dal 2010 al 2019.

A questa assenza di interesse si è in parte contrapposta una presa coscienza da parte di alcuni operatori di "Infrastrutture critiche" riguardo la rilevanza del fattore umano.

Questo si è tradotto nell'adozione di attività di formazione e valorizzazione del personale nell'ottica sia di creare una maggiore "fidelizzazione" dei dipendenti che di far crescere

il numero di addetti con specifiche competenze favorendo politiche di rotazione degli incarichi e mantenendo legami di collaborazione con gli ex-dipendenti.

2. L'esperienza italiana nella gestione delle "Infrastrutture critiche"

Come anticipato precedentemente, durante l'emergenza Covid non si è registrato in Italia nessun disservizio per quel che riguarda l'erogazione dei servizi essenziali. Questa aspetto, sfuggito ai più, non è per nulla scontato in quanto da un lato erano da tenere in conto le giuste preoccupazioni dei lavoratori e dall'altro la complessità di gestione di questi sistemi soprattutto per quel che riguarda le attività di manutenzione, nonché la gestione delle loro filiere di approvvigionamento.

Mentre tutti i cittadini erano "invitati" a rimanere nelle loro abitazioni, il personale operante presso le "Infrastrutture critiche" doveva recarsi non solo presso i propri luoghi di lavoro, ma in molti casi operare sul territorio sia per l'esecuzione dei compiti istituzionali che, soprattutto, per la gestione delle criticità nelle varie infrastrutture (guasti, incidenti, etc.). In tutto il periodo di lockdown sono stati migliaia gli interventi eseguiti in "zone rosse" che hanno comportato la necessità da parte del personale di accedere ad aree potenzialmente contaminate onde evitare che i servizi venissero interrotti. Questo ha comportato la necessità di dotare gli operatori di adeguati Dpi. Occorre dire che, a differenza della quasi totalità delle altre aziende, molti operatori di "Infrastrutture critiche" avevano in magazzino specifici Dpi per la protezione delle vie aeree, avendo storicamente la necessità di operare in ambienti "sporchi" e molti di essi avendo percepito il potenziale pericolo avevano provveduto ad acquisire ulteriori quantitativi di Dpi. Questo ha consentito ad alcuni operatori non solo di garantire un adeguato livello di protezioni ai propri lavoratori ma anche, soprattutto nei momenti iniziali della crisi, di condividere con le autorità pubbliche e con gli altri operatori parte delle loro riserve. Inoltre, essi hanno sfruttato le proprie filiere per favorire l'approvvigionamento dall'estero dei Dpi e di attrezzature mediche. Infatti, avendo competenza e consolidati rapporti commerciali con produttori esteri, a partire da quelli cinesi, essi hanno potuto perseguire trattative dirette bypassando la pletora di intermediari che sono spuntati durante le prime fasi della crisi e che, in molti casi, si sono rilevati non affidabili se non addirittura truffaldini.

Questo evidenzia un aspetto interessante che riguarda il "pregio" della globalizzazione: un soggetto con una rete commerciale diffusa e consolidata può accedere con facilità a canali di approvvigionamenti diversificati anche in situazioni di crisi. È emerso, però, in parallelo a questo aspetto positivo anche un risvolto negativo della globalizzazione per almeno due problematiche differenti e solo in parte correlate. Il primo aspetto riguarda la presenza di filiere fragili, ovvero caratterizzate da una serie di *single point of failure*. L'obiettivo di perseguire politiche di miglioramento dell'efficienza e di riduzione dei costi

ha indotto molte realtà produttive a sacrificare la differenziazione a vantaggio di una forte specializzazione. Il tutto si è tradotto per alcune aziende nell'impossibilità di approvvigionarsi di specifiche materie prime e/o semi-lavorati in quanto tutte le forniture erano concentrate nei medesimi distretti industriali se non addirittura in un'unica realtà produttiva. Il che ha comportato in molti casi ripercussioni significative sulle catene di produzione del valore. Questo problema è legato oltre che alla localizzazione dei siti produttivi dei semi-lavorati anche agli aspetti di logistica: la paralisi dei trasporti su lungo raggio, sia marittimi che aerei, ha comportato un significativo allungamento nei tempi di consegna.

Occorre evidenziare che questo aspetto è stato solo in minima parte sofferto dalle "infrastrutture critiche nazionali" i cui flussi di materie prime non sono mai stati interrotti, essendo per la gran parte alimentati da fonti nazionali e/o veicolate tramite infrastrutture dedicate (quindi senza una necessità di utilizzare canali logistici che implicassero lo spostamento di persone). Solo in alcuni limitati casi si è dovuto far ricorso parziale a riserve.

Qualche problema è, invece, emerso per quel che concerne la parte di gestione dei residui di produzione (ovvero dei rifiuti) a causa sia del fatto che la quasi totalità degli impianti nazionali è ubicata nel Nord Italia e che una frazione significativa di questi rifiuti è conferito all'estero. La difficoltà di movimentazione ha creato in questo caso problemi al punto che per alcune situazioni specifiche le autorità locali hanno dovuto emanare provvedimenti per consentire lo stoccaggio temporaneo di tali rifiuti in aree normalmente deputate ad altri scopi.

Un discorso diverso riguarda, invece, le problematiche connesse con la manutenzione degli impianti e delle infrastrutture con riferimento non tanto alla mobilità del personale delle "Infrastrutture critiche", quanto piuttosto per quel che riguarda il personale di ditte terze. Aspetto questo divenuto critico con riferimento ad interventi che necessitano l'intervento di personale altamente specializzato proveniente dall'estero. La criticità, in questo caso, è legata all'impossibilità di conciliare le attività lavorative con gli obblighi di rispettare i periodi di quarantena fiduciaria. Problematica che ha creato diverse situazioni di criticità al punto che il legislatore nel comma 4 dell'art. 211*bis* del d.l. Rilancio ha espressamente richiamato la necessità di definire misure per garantire la mobilità sul territorio nazionale di "soggetti terzi inclusi coloro che provengono dall'estero" che operino per garantire la continuità operativa e manutentiva delle "Infrastrutture critiche".

2.1. I Principi precauzionali della Presidenza del Consiglio dei Ministri

Sebbene i principali operatori di "Infrastrutture critiche" abbiano autonomamente adottato specifici piani per una corretta gestione dell'emergenza Covid, lo stesso non può dirsi per gli operatori più piccoli. Questi ultimi, infatti, non essendo in genere dotati di

specifici dipartimenti di *security* non apparivano nella totalità dei casi in grado di elaborare adeguate strategie per gestire al meglio l'emergenza Covid.

Per venire incontro a questi operatori il 26 marzo 2020 la segreteria "Infrastrutture critiche" della Presidenza del Consiglio dei Ministri ha emanato i "principi precauzionali". Tali principi raccolgono le indicazioni emanate dai diversi ministeri a partire da quello dello Sviluppo economico e sono formulati come indicazioni di "buon senso" nell'ottica di indirizzare le attività degli operatori senza però introdurre vincoli che in un momento di emergenza possono risultare elementi paralizzanti per le strutture operative.

In primo luogo, è evidenziata la necessità in capo agli operatori di definire opportune procedure per la sanificazione dei luoghi di lavoro organizzando le attività in modo da avere il numero minimo di personale in sede e sugli impianti. Ciò può essere ottenuto limitando i presidi fisici ai soli casi di attività indifferibili ed essenziali per la continuità del servizio. A tal fine si suggerisce di revisionare i programmi di manutenzione, limitandoli a quelli indifferibili e rinviando quelli non indispensabili, oltre a favorire un significativo ricorso allo smart working. Con riferimento a quest'ultimo aspetto, i Principi raccomandano "di garantire adeguati livelli di *cybersecurity*, includendo fra tali attività anche l'emanazione di opportune regole di comportamento da parte del personale che opera in modalità smart working". La necessità di adottare un'attenzione specifica agli aspetti di cyber security è stata ulteriormente rafforzata nel comma 1 dell'art. 211*bis* che esplicitamente richiama gli obblighi derivanti dalla Direttiva NIS (d.lgs n. 65/2018) e dalla norma sul "Perimetro nazionale di sicurezza cibernetica" (l. n. 133/2019). In altri termini la necessità di un massiccio ricorso allo smart working non è considerato dal legislatore una situazione esimente rispetto alla salvaguardia del cyberspace nazionale soprattutto con riferimento agli operatori di "Infrastrutture critiche".

Il personale coinvolto in attività *in presenza va organizzato* in squadre composte dal numero minimo di persone necessarie per l'esecuzione in sicurezza (*safety*) delle diverse attività. La composizione di ogni squadra, al fine di aumentarne la resilienza, non dovrà (ove possibile) mutare nel tempo e dovranno attuarsi specifici accorgimenti procedurali per evitare (ovvero limitare al minimo) l'interazione fisica fra più squadre.

Viene inoltre suggerito per le attività da svolgere al di fuori delle sedi aziendali, tipicamente interventi di manutenzione e riparazione, di prevedere che gli operatori possano partire direttamente dal proprio domicilio senza la necessità di passare per le sedi aziendali.

Al fine di aumentare la tutela dei lavoratori viene raccomandata la predisposizione di specifiche regole di comportamento per ciò che riguarda l'esecuzione di interventi presso strutture o abitazioni in cui siano presenti persone in quarantena fiduciaria ovvero risultate positive al Covid-19.

È richiesto, in uno spirito di cooperazione pubblico-privato, di riferire ai *m*inisteri competenti e alla Presidenza del Consiglio dei Ministri tutte le misure intraprese, segnalando eventuali disservizi o criticità che potrebbero riverberarsi, in un'ottica di *service continuity*, sull'erogazione dei servizi essenziali alla popolazione.

L'utilità di questi principi ha trovato una conferma nella decisione del Legislatore di imporre con l'art. 211*bis* del d.l. "Rilancio" l'obbligo in capo agli operatori di "Infrastrutture critiche" di introdurre nei loro piani di sicurezza specifiche misure per la gestione di emergenza sanitaria. Piani che per quel che riguarda la gestione dell'emergenza Covid devono tener conto di quanto previsto dai "Principi precauzionali" e delle linee guida emanate dai ministeri competenti. Con l'approvazione del 211*bis* l'adesione alle linee guida elencate nei "Principi precauzionali" diviene pertanto un obbligo cogente per gli operatori di "Infrastrutture critiche".

Ad ulteriore riprova della utilità di siffatte indicazioni si segnala che anche altri governi hanno emanato durante la crisi specifiche indicazioni sulle modalità di gestione delle "Infrastrutture critiche" come ad esempio gli Stati Uniti (Cisa, 2020a) e il Canada (Canada, 2020). Si noti che, come per i principi, anche le indicazioni elaborate dagli altri governi hanno un carattere di raccomandazione ed evitano di focalizzarsi su aspetti di dettaglio e/o su specifiche soluzioni tecniche o organizzative.

2.2. La gestione delle sale operative

Un aspetto particolare su quale si soffermano i "Principi precauzionali" riguarda la gestione delle sale operative. Queste rappresentano il "cuore" tecnologico di molte infrastrutture e sono essenziali per il corretto funzionamento delle stesse. La loro rilevanza è tale che il governo americano nel mese di aprile ha emanato specifiche *guidelines* per la loro gestione (Cisa, 2020b).

Come evidenziato in precedenza la criticità della gestione delle sale operative risiede nel fatto che in primo luogo sono gestite da personale altamente specializzato e, quindi, non sostituibile. Le attività devono svolgersi gioco forza all'interno di ambienti confinati dove devono cooperare una pluralità di soggetti. Per questi ambienti risulta impossibile l'attivazione di smart working a causa di vincoli tecnologici e di sicurezza. Dovendo, per altro, operare h24, per tali ambienti è intrinsecamente complesso anche lo svolgimento delle misure di sanificazione al cambio turno in quanto le attività si susseguono con soluzione di continuità.

L'aspetto di maggiore criticità risiede, però, nell'alto rischio connesso con il contagio di un addetto che immediatamente si ripercuote sia nella necessità di porre in quarantena fiduciaria l'intera squadra sia nel fatto che l'accesso alla sala stessa diventerebbe precluso fino all'esecuzione delle attività di sanificazione. Cosa che è incompatibile con le esigenze operative di molte infrastrutture.

In questa ottica i "Principi precauzionali" fanno propria l'esperienza e le soluzioni messe in atto nell'immediatezza ad alcuni operatori di "Infrastrutture critiche" che si sono rilevati efficaci soluzioni organizzative (Setola, 2020).

Una soluzione adottata da diversi soggetti, fra cui Bnl, è stata quella di attivare il sito di *disaster recovery* e di dividere gli operatori in due gruppi di squadre che erano indirizzati ad operare in modalità temporalmente sfalsata presso la *control room* principale ovvero in quella del *disaster recovery*. In questo modo si diminuisce il rischio di contagio inter-squadra (nessuna squadra si incontrava essendo i turni alternati sulle due sedi) e vi era la possibilità di effettuare adeguati interventi di sanificazione nelle due sale operative.

Questa soluzione non è però adottabile in quei contesti nei quali è fondamentale avere attivo in modalità "hot" sia il sito principale che quello di secondario in quanto la continuità operativa dell'infrastruttura non può essere mai interrotta. Per ovviare a questa problematica alcuni operatori, come Enel e Terna, hanno creato nel volgere di pochissimi giorni nuove sale di controllo/dispacciamento nel medesimo edificio in cui era presente quella principale in modo da poter separare temporalmente e fisicamente le attività. In realtà la sala di controllo (intesa come core tecnologico) è rimasta unica, quello che è stato duplicato è la sola componente di *front-end*, ovvero l'insieme di postazioni su cui gli operatori agiscono.

L'adozione di una siffatta soluzione è legata alla possibilità strutturale di attrezzare una seconda sala operativa nel medesimo plesso con caratteristiche di sicurezza ed accessibilità tali da prevenire il contagio inter-squadre. Questa soluzione, però, non "preserva" la squadra nella sua interezza dalla possibilità di contagio. Infatti, gli operatori, anche se controllati all'accesso alla sala in termini di stato di salute e misurazione della temperatura, potrebbero incubare il virus (ovvero essere asintomatici) e infettare l'intera squadra. Questo rischio, seppur esistente, è stato considerato accettabile anche alla luce dell'esistenza sul territorio nazionale di ulteriori sale di controllo/dispacciamento strutturate in modo che in situazioni di emergenza potevano assumere la valenza di centro di controllo nazionale sia in termini di requisiti tecnologici (collegamenti) che funzionali (professionalità e competenza degli operatori).

In situazioni in cui questa ridondanza non è presente si è dovuto ricorrere a soluzioni organizzativamente di maggiore complessità come fatto da Telespazio. In questo caso l'azienda in collaborazione con le maestranze ha adottato una soluzione che prevede la "segregazione" volontaria di due squadre per 14 giorni all'interno del sito. In altri termini, gli operatori del centro di controllo svolgevano turni di 14 giorni durante i quali non avevano contatto con nessun soggetto al di fuori dei propri colleghi appartenenti alla medesima squadra. Per garantire l'adeguato supporto logistico si è dovuto attrezzare, grazie alla collaborazione ed il supporto dell'Esercito, una tendopoli per consentire gli accasermamenti per gli operatori e quant'altro necessario per garantire loro la possibilità di "vivere" in isolamento.

Soluzione ancora più "stringente" è quella adottata da Snam che per altro è stata la prima società a mettere in atto specifiche strategie di protezione degli operatori. Questo sia per la vicinanza del centro nazionale di dispacciamento dal luogo dove si è evidenziato il primo focolaio di Covid, ma soprattutto per la cultura della sicurezza che caratterizza Snam. La soluzione adottata prevede l'attivazione sia del sito principale che di quello di *disaster recovery* dove operano distinte squadre. Ognuna di queste squadre (più squadre per ciascun sito) opera in modalità di segregazione volontaria per 14 giorni all'interno della struttura senza alcun contatto con l'esterno. Contemporaneamente altre squadre rimangono in segregazione volontaria presso i propri domicili in modo da non esporsi, neanche in modo indiretto, al contagio. Per meglio garantire quest'ultimo aspetto Snam ha anche messo in campo iniziative per limitare l'esposizione dei loro familiari al virus.

I "Principi precauzionali" suggeriscono, inoltre, come ulteriore misura a salvaguardia della continuità operativa l'opportunità di redigere liste con il personale in esercizio, in quiescenza o in forza presso altri soggetti che, avendo maturato esperienze trasversali, possa utilmente essere impiegato per sostituire il personale specializzato delle sale di controllo e della manutenzione, in caso di prolungata indisponibilità.

Riflessioni conclusive

È evidente che in presenza di una crisi di origine sanitaria, ma queste considerazioni valgono per qualunque tipologia di crisi, è necessario disporre di piani di *preparedness* che prevedano le risorse e le azioni necessarie per fronteggiare la crisi. L'esperienza ha dimostrato che praticamente nessuna organizzazione, né in Italia né nel resto del mondo, aveva predisposto piani specifici per un efficiente contenimento e gestione di un evento pandemico.

Ciò nonostante possiamo affermare che lo sviluppo di approcci "All-hazard", ovvero di approcci olistici alla gestione delle emergenze ha consentito agli operatori di "Infrastrutture critiche" di gestire in modo migliore rispetto ad altri contesti produttivi gli effetti della pandemia sia in termini di salvaguardia del proprio personale che di capacità di erogazione dei servizi alla popolazione.

Ciò è stato possibile grazie alla competenza e alla cultura della sicurezza che pervade molti degli operatori di "Infrastrutture critiche" nazionali e alle disposizioni emanate dagli enti pubblici, ma soprattutto perché il personale operante presso le diverse infrastrutture era adeguatamente preparato e, soprattutto, motivato. Il personale aveva contezza della criticità del servizio erogato e del proprio ruolo, e quindi disponibile ad operare anche in situazioni di estremo disagio personale come la segregazione volontaria all'interno dei luoghi di lavoro pur di garantire il regolare funzionamento delle diverse "Infrastrutture critiche" in un'ottica di effettiva *service continuity*.

Un aspetto che è emerso con chiarezza durante l'emergenza è l'importanza di efficaci canali di *information sharing*. I vari operatori, anche grazie all'azione delle associazioni di categoria come Aipsa, hanno avuto modo di condividere le proprie esperienze e difficoltà, e ciò ha consentito che le esperienze di successo adottate da un operatore si siano subito tramutate in *best-practice* da imitare per gli altri.

In qualche modo anche i "Principi precauzionali" nascono per favorire questa condivisione di esperienze all'interno della quale il pubblico collabora, per quanto di propria competenza, nel "favorire" l'attuazione delle misure atte a garantire la continuità operativa delle "Infrastrutture critiche" (come esplicitato nel comma 4 dell'art. 211*bis* più volte citato).

Questa volontà di favorire, anche durante l'emergenza, una stretta cooperazione pubblico-privato è stata apprezzata da più parti come testimoniato dal fatto che anche società che non erano classificate come "Infrastrutture critiche", hanno ritenuto opportuno condividere con la Presidenza del Consiglio dei Ministri e con i ministeri competenti i propri piani di gestione dell'emergenze oltre che evidenziare le problematiche di attuazione. Problematiche che, come comprovato dall'assenza di interruzione nell'erogazione dei servizi, sono state minimali e gestite in modo adeguato dai vari attori coinvolti.

Riferimenti Bibliografici

- Cybersecurity and Infrastructure Security Agency (2020), Consultabile in https://www.cisa.gov/about-cisa
- Cyber Security & Infrastructure Security Agency (2020a). Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response. Consultabile in https://www.cisa.gov/sites/default/files/publications/Version_3.1_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers.pdf
- Cyber Security & Infrastructure Security Agency (2020b). Critical Infrastructure Operations Centers and Control Rooms – A Guide for Pandemic Response. Consultabile in https://www.cisa.gov/sites/default/files/publications/20_0423_COVID-19_CI_Ops_Center_Control_Room_Guide.pdf
- Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Springer Nature, 2020.
- European Commission (2008). Directive 2008/114/EC — identification and designation of European critical infrastructures and assessment of the need to improve their protection. Consultabile in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013
- Fair, J. M., LeClaire, R. J., Wilson, M. L., Turk, A. L., DeLand, S. M., Powell, D. R., & Izraelevitz, D. (2007). An integrated simulation of pandemic influenza evolution, mitigation and infrastructure response, IEEE Conference on Technologies for Homeland Security, 240-245.
- Government of Canada, (2020). Guidance on Essential Services and Functions in Canada During the COVID-19 Pandemic, 2020. Consultabile in https://ww.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstr-ctr/esf-sfe-en.aspx
- Lazari, A. (2014). European critical infrastructure protection, Springer International Publishing, 2014.
- Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. Hoboken: John Wiley & Sons.
- Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems, Reliability engineering & System safety, - n. 121, 43-60.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE control systems magazine - n. 21(6), 11-25.
- Segreteria Infrastrutture critiche (2020). Principi precauzionali per gli operatori di infrastrutture critiche ai fini della continuità in sicurezza del servizio di interesse pubblico. Consultabile in http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTEII/Allegati/Principi%20precauzionali%20Infracrit%20COVID-19.pdf
- Setola, R. (2003). La protezione delle "Infrastrutture critiche" informatizzate, Automazione e Strumentazione, 27-35.
- Setola, R., Rosato, V., Kyriakides, E., & Rome, E. (2016). Managing the complexity of critical infrastructures: A modelling and simulation approach, Springer Nature, 2016.

– Setola, R. (2020). La sicurezza nazionale alla prova della resilienza. Consultabile in https://formiche.net/2020/04/resilienza-enel-bnl-snam-covid-19/
– US Government (1998). PDD-63 - Critical Infrastructure Protection, 5/20/1998. Consultabile in https://clinton.presidentiallibraries.us/items/show/12762
– US Government (2007). The Prioritization od Critical Infrastructure for a Pandemic Outbreak in the United States. Consultabile in https://www.dhs.gov/xlibrary/assets/niac/niac-pandemic-wg_v8-011707.pdf
– World Health Organization (2005). WHO global influenza preparedness plan. Consultabile in https://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_5.pdf
– World Health Organization (2009), Whole-of-Society Pandemic Readiness - WHO guidelines for pandemic preparedness and response in the nonhealth sector. Consultabile in https://www.who.int/influenza/preparedness/pandemic/2009-0808_wos_pandemic_readiness_final.pdf
– Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art, Energy policy, n. 39(10), 6100-6119.
– Zagaria, C. (2009). Autisti in rivolta, Napoli paralizzata – "Bus sporchi, così ci infettiamo". Consultabile in https://www.repubblica.it/2009/09/sezioni/cronaca/nuova-influenza-3/bus-napoli/bus-napoli.html