RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0164 • articolo sottoposto a peer review • pubblicato in anteprima il 6 ago. 2024

INDRA MACRÌ

Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR

Il contributo descrive le più recenti indicazioni fornite alle pubbliche amministrazioni a garanzia delle cybersicurezza. L'analisi confronta le differenti disposizioni dirette alle PA in materia di cybersicurezza e ne approfondisce l'ambito di applicazione.

Pubblica amministrazione – Sicurezza cibernetica – Cloud

Strategies and operational models for Public Administrations security at the time of National Recovery and Resilience Plan (RRP)

The paper describes the most recent indications provided to public administrations to guarantee cybersecurity. The analysis compares different provisions for PAs regarding cybersecurity and delves into their scope of application.

Public Administration – Cybersecurity – Cloud

L'Autrice è consigliere dell'area informatica, Servizio studi della Corte costituzionale. Le opinioni espresse nel presente contributo sono riconducibili all'Autrice e non impegnano in alcun modo l'Istituzione di appartenenza

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

1. Introduzione

Quando fra il 2020 e il 2021 il nostro Paese ha definito le scelte strategiche da attuare nel Piano nazionale di ripresa e resilienza (PNRR), è partito dalla digitalizzazione, innovazione e messa in sicurezza della PA.

È, infatti, interamente dedicata alla digitalizzazione, innovazione e sicurezza nella PA la prima componente della prima missione del PNRR italiano. Per digitalizzare la PA non basta garantire riservatezza, integrità e disponibilità dei servizi e dei dati pubblici, ma occorre innovare i processi che fino a quel momento hanno governato l'*agĕre* pubblico. La digitalizzazione di un pre-esistente servizio "analogico", difatti, non necessariamente produce una riduzione dell'onere burocratico, allorquando, piuttosto che innovare, si pretende di riprodurre in digitale le precedenti procedure analogiche, senza analizzare e valorizzare le nuove opportunità che le tecnologie digitali possono offrire sia nella semplificazione verso cittadini e imprese, sia nello snellimento di processi interni.

Lo sviluppo dei servizi digitali pubblici corre necessariamente sui binari tracciati dall'Europa, poiché il PNRR espressamente stabilisce che gli investimenti digitali delle pubbliche amministrazioni devono essere allineati alle indicazioni in materia fornite dalla Commissione[1]. Operazione tutt'altro che facile, visto lo "tsunami normativo europeo" nel settore della digitalizzazione e, in particolare, della cybersicurezza, riflesso nella nostra legislazione per lo più attraverso decreti d'urgenza.

Ad esempio, è contenuto in un decreto d'urgenza[2] l'obbligo dal 28 febbraio 2021 per le pubbliche amministrazioni di utilizzare come sistemi di identificazione in rete dei cittadini e delle imprese per l'accesso ai servizi digitali pubblici esclusivamente SPID e CIE (e in via residuale la CNS) al posto delle credenziali (utenza e password) rilasciate dalle stesse amministrazioni ai loro utenti.

Ed è sempre attraverso un decreto di urgenza[3] che nasce nel 2021 l'Agenzia per la cybersicurezza nazionale (ACN) che si occupa della sicurezza nel campo cibernetico sia di operatori pubblici che privati. Benché siano molti gli attori istituzionali

1. *Piano nazionale di ripresa e resilienza*, p. 12.
2. Cfr. art. 24, co. 1, lett. *e*) ed *f*), d.l. 16 luglio 2020, n. 76, *Misure urgenti per la semplificazione e l'innovazione digitale*, convertito dalla legge 11 settembre 2020, n. 120, che ha modificato gli artt. 64 e 64-*bis* del d.lgs. 7 marzo 2005, n. 82/2005 (*Codice dell'amministrazione digitale*).
3. V. d.l. 14 giugno 2021, n. 82, *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito dalla l. 4 agosto 2021 n. 105.

con competenze in materia cyber, la stessa *Strategia nazionale di cybersicurezza 2022-2026*, presentata da Mario Draghi, Presidente del Consiglio dei ministri dell'epoca, evidenzia la necessità di un approccio "*whole-of-society*", che coinvolge anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza[4]. Anche perché la capillarità e la complessità della società digitale, i suoi effetti sulla sicurezza informatica e, allo stesso tempo, la forte interrelazione fra i molteplici attori richiedono uno sforzo corale e l'impegno del mondo pubblico come di quello privato.

A partire dal 2021, le precedenti funzioni svolte dall'AGID (Agenzia per l'Italia digitale) per la sicurezza cibernetica della pubblica amministrazione digitale sono state trasferite progressivamente all'ACN, che oggi si occupa anche dell'attuazione della strategia cloud pensata a protezione dei dati e dei servizi delle pubbliche amministrazioni.

Come emerge dalla relazione annuale dell'Agenzia per la cybersicurezza nazionale nel 2023 sono stati trattati 1.411 eventi *cyber*[5], per una media di circa 117 al mese, con un picco di 169 a ottobre. Di questi, 303 sono stati classificati come incidenti[6], per una media di circa 25 al mese[7]. Occorre osservare, peraltro, che la cybersicurezza, ben prima del PNRR, aveva attirato non solo a livello europeo, ma anche internazionale, l'attenzione del decisore politico. Le tensioni geopolitiche degli ultimi anni, però, hanno intensificato gli attacchi informatici verso quei Paesi, come l'Italia, che nell'ambito della comunità internazionale, hanno assunto *posizioni di solidarietà e sostegno degli attori statuali in conflitto sia con riguardo alla crisi russo-ucraina, sia con riguardo allo scenario mediorientale*. Partendo da questa considerazione, fra il 2023 e il 2024 sono state pubblicate ben due direttive in materia di cybersicurezza rivolte alle pubbliche amministrazioni, che, tuttavia, come meglio chiarito di seguito, erano già tenute ad attuare specifiche misure in materia di sicurezza informatica.

La legge 28 giugno 2024, n. 90 ha, fra l'altro, ulteriormente rafforzato i compiti assegnati alle amministrazioni pubbliche per cooperare alla difesa cibernetica del Paese.

Nel frattempo, tenuto conto del mutato scenario di rischio, l'Agenzia per la cybersicurezza nazionale ha riordinato la disciplina tecnica in materia di cloud rivolta alle pubbliche amministrazioni, con la pubblicazione lo scorso 27 giugno 2024 del relativo Regolamento[8], adottato con decreto direttoriale n. 21007/24.

2. Le recenti direttive del Presidente del Consiglio dei ministri in materia di cybersicurezza per le PA

Il Presidente del Consiglio dei ministri, al quale sono attribuite in via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza[9], ha formulato specifiche indicazioni per le pubbliche amministrazioni attraverso le direttive del 6 luglio 2023 e del 29 dicembre 2023, rispettivamente pubblicate nella Gazzetta ufficiale dell'8 agosto 2023 e del 16 febbraio 2024.

La prima direttiva del 6 luglio 2023, diretta alle PA del d.lgs. 30 marzo 2001, n. 165[10], individua indirizzi di coordinamento e organizzazione per

4. ACN 2022, p. 8.
5. Evento cyber è un avvenimento «con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti», Cfr. ACN 2023, p. 11.
6. «Incidente è un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima», *ibidem*.
7. *Ivi*, p. 14.
8. Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, per brevità di seguito sarà indicato come "Regolamento cloud ACN" o "Regolamento".
9. V. art. 2, d.l. n. 82/2021.
10. Restano, però, esclusi dall'ambito di applicazione della direttiva, come per buona parte della disciplina in materia di cybersicurezza, quegli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati,

una adeguata gestione delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica. L'altra direttiva, pubblicata a inizio 2024, invece, è più operativa: fornisce ai ministeri le indicazioni pratiche da seguire per assicurare la resilienza cibernetica del Paese attraverso protocolli di intesa con l'ACN irrobustendo la capacità di risposta agli incidenti informatici.

In particolare nella prima direttiva si stabilisce che le PA garantiscono la massima collaborazione con l'ACN e, specificatamente, con gli operatori del CSIRT Italia[11], anche qualora, a seguito di un incidente, vi sia un loro diretto intervento presso la PA. In tal caso è richiesta la piena collaborazione non solo delle pubbliche amministrazioni coinvolte, ma anche delle società *in house* o a controllo pubblico che lavorano a supporto dei sistemi informativi della PA. Tali soggetti dovranno consentire l'accesso ai locali e ai sistemi informativi impattati per tutto il periodo necessario allo svolgimento delle operazioni. L'obiettivo è prendere piena contezza della situazione, anche in considerazione della collaborazione richiesta all'ACN a livello dell'Unione europea in materia di cybersicurezza. L'ACN, infatti, partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando i collegamenti con le organizzazioni internazionali, di cui l'Italia fa parte, necessari per la gestione delle crisi (art. 10, comma 5, lett. e), d.l. n. 82/2021).

La collaborazione istituzionale è così necessaria in ambito cybersicurezza, tanto più che questa non può essere garantita da un solo soggetto: la complessità della materia richiede la sinergia. Cosicché le indicazioni sulla piena collaborazione contenute nella direttiva del luglio 2023 sono state rafforzate dopo poco, introducendo attraverso una specifica norma[12] sanzioni verso determinati soggetti (anche privati) che non forniscono il pieno supporto alle strutture dell'ACN chiamate a intervenire per le operazione di contenimento e mitigazione delle conseguenze provocate da un incidente informatico, consentendo il ripristino quanto più tempestivo possibile dell'operatività dei sistemi compromessi.

La successiva direttiva di fine 2023, che, come richiamato, ha un ambito di applicazione più limitato, riferendosi ai soli Ministeri e non a tutte le PA individuate dal d.lgs. n. 165/2001, stabilisce

alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della l. 3 agosto 2007, n. 124.

11. Ai CSIRT (*Computer security incident response team*) sono attribuiti molteplici compiti, definiti nel d.lgs. 18 maggio 2018, n. 65 e nell'art. 4 del decreto del Presidente del Consiglio dei ministri dell'8 agosto 2019. Essi includono: - il monitoraggio degli incidenti a livello nazionale; - l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; - l'intervento in caso di incidente; - l'analisi dinamica dei rischi e degli incidenti; - la sensibilizzazione situazionale; - la partecipazione alla rete dei CSIRT. Il CSIRT stabilisce relazioni di cooperazione con il settore privato e, per facilitare la cooperazione, promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni. Il profilo completo dello CSIRT Italia è contenuto nel documento RFC 2350.

12. Art. 2-*bis* (*Disposizioni urgenti in materia di contrasto della criminalità informatica e di cybersicurezza*) del d.l. 10 agosto 2023, n. 105, convertito dalla legge 9 ottobre 2023, n. 137, che ha introdotto all'art. 7, co. 1, del d.l. n. 82/2021 la lettera n-*bis*, per stabilire che la mancata collaborazione con l'ACN da parte dei soggetti pubblici o privati che rientrano nel perimetro di sicurezza nazionale cibernetica (definito dall'art. 1, co. 2, lett. *a*) del d.l. 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133, c.d. "Decreto perimetro") che hanno subìto incidenti di sicurezza informatica o attacchi informatici è valutata ai fini dell'applicazione delle sanzioni previste dallo stesso decreto perimetro (art. 1, co. 10 e 14 del d.l. n. 105/2019). Tali sanzioni variano da quelle amministrative pecuniarie (fino a euro 1.800.000) alla reclusione (fino a tre anni). Alle stesse sanzioni sono sottoposte, inoltre, gli operatori di servizi essenziali indicati nel d.lgs. 18 maggio 2018, n. 65 (decreto di recepimento della direttiva NIS, cfr. nota n. 16) e le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, come individuate dall'art. 40, d.lgs. 1° agosto 2003, n. 259, *Codice delle comunicazioni elettroniche*. Dall'applicazione della disciplina restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza.

anzitutto la necessità di definire al più alto livello istituzionale, ossia fra ciascun Ministro e il vertice dell'ACN, degli atti di intesa, dove si precisano le attività che ciascuno, in caso di attacco informatico subìto dal Ministero, è tenuto a svolgere per il contenimento e la mitigazione delle conseguenze dell'incidente informatico. La direttiva, al riguardo, fornisce indicazioni tecnico-organizzative, che costituiscono il presupposto dal quale partire per garantire un ripristino quanto più possibile immediato dell'operatività dei sistemi compromessi delle PA interessate.

Tali indicazioni sono state raggruppate in 4 punti essenziali:

1) un censimento dei sistemi hardware e software, oltre che dei flussi di dati utilizzati per lo svolgimento delle attività istituzionali;
2) un documento con la definizione di ruoli e responsabilità inerenti alla cybersicurezza, sia per il personale interno, che di terze parti che supportano l'amministrazione, con l'individuazione fra il personale della PA di un incaricato per la cybersicurezza, che sia da punto di contatto con l'ACN, oltre che di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi informatici);
3) dei piani per la gestione delle vulnerabilità, dei backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi, delle identità e dei relativi permessi;
4) un piano di risposta in caso di incidente, che definisca puntualmente le articolazioni interne che – in stretto raccordo con l'incaricato per la cybersicurezza – sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un eventuale incidente cibernetico.

La seconda direttiva, quindi, intende porre l'ACN al fianco delle PA centrali, definendo un "modello operativo", attraverso il quale rispondere molto più efficacemente agli incidenti di sicurezza, evitandone la propagazione e, allo stesso tempo, affida all'ACN medesima il compito di monitorarne l'adozione da parte dei Ministeri.

A ben guardare, come approfondito di seguito, buona parte delle indicazioni contenute nella sopra citata direttiva del Presidente del Consiglio dei ministri pubblicata nel 2024 sono state fornite alle pubbliche amministrazioni già da diversi anni. La vera novità di questa direttiva sta nel fatto che, per garantire la cybersicurezza dei dati e dei servizi pubblici, è investito il più alto vertice dell'amministrazione, ossia lo stesso Ministro e non solo la dirigenza tecnica. La cybersicurezza, quindi, dirompe sempre più in una dimensione politica, non potendo essere contenuta esclusivamente in quella tecnico-amministrativa, dove nella maggioranza dei casi era stata relegata.

3. Le precedenti indicazioni alle PA in materia di sicurezza informatica

Le circolari AGID del 2017 nn. 1 e 2 (la seconda è un aggiornamento della prima) introducono le misure minime di sicurezza e si rivolgono, da ultimo, a tutte le pubbliche amministrazioni indicate dall'art. 2, comma 2 del CAD (*Codice dell'amministrazione digitale*, d.lgs. 7 marzo 2005, n. 82), che comprendeva – alla data di emanazione della circolare n. 2 (18 aprile 2017, G.U. 5 maggio 2017, n. 103) – oltre alle PA individuate dal d.lgs. n. 165/2001, anche le società a controllo pubblico non quotate (art. 2, circolare). La circolare AGID n. 2/2017 stabiliva che l'adozione delle misure minime dovesse avvenire entro il 31 dicembre 2017 (art. 5) e che responsabile dell'attuazione fosse direttamente il Responsabile per la transizione digitale (art. 3). Tali circolari nascono dalla direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015, dove si prevedeva, fra l'altro, che tutte le amministrazioni e gli organi chiamati a intervenire in caso di eventi cibernetici dovessero dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di sicurezza per prevenire e mitigare gli effetti di potenziali attacchi informatici. Nel 2015 la stessa direttiva affidava all'Agenzia per l'Italia digitale la messa a disposizione degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia era parte. Già il 26 aprile 2016 l'AGID in attuazione della citata direttiva aveva pubblicato le *Misure minime di sicurezza ICT*[13] per le pubbliche amministrazioni come

13. ICT sta per *Information and communication technologies*.

parte integrante delle *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni*, richiamando, fra i documenti di riferimento, il CIS, *Critical Security Controls for Effective Cyber Defense* - versione 6.0 di ottobre 2015 e il documento dell'Università La Sapienza del 2015 *Italian Cyber Security Report del CIS*. Quest'ultimo documento, che si ispirava al *Cybersecurity Framework* sviluppato dal *National Institute of Standards and Technology* (NIST), nel 2019 è stato rivisto con il supporto del Garante per la protezione dei dati personali. La nuova versione, *Framework Nazionale per la Cybersecurity e la Data Protection*[14] del febbraio 2019 offre a imprese e pubbliche amministrazioni una guida di supporto nell'implementazione della cybersicurezza allo stesso tempo in linea con le indicazioni in materia di sicurezza contenute nel Regolamento sulla privacy del 2018. Benché non risulti sia stato formalmente recepito con uno specifico provvedimento, tale *Framework* costituisce un riferimento della disciplina regolamentare di settore, tant'è che, ad esempio, è espressamente citato dal Regolamento cloud ACN.

Le misure minime di sicurezza di AGID, formalmente adottate prima come linee guida e poi aggiornate e pubblicate in allegato alla citata circolare, hanno costituito già dal 2016 un'importante guida alla quale amministrazioni pubbliche e gestori di pubblici servizi avrebbero dovuto attenersi. Nel 2019 i loro contenuti sono stati per buona parte ripresi dal *Framework Nazionale per la Cybersecurity e la Data Protection* e poi da ultimo ribaditi nella direttiva del Presidente del Consiglio dei ministri di febbraio 2024.

La Tabella 1 mette a confronto le indicazioni sulla cybersicurezza che negli ultimi anni sono state rivolte alle pubbliche amministrazioni.

Sia la recente direttiva del Presidente del Consiglio dei ministri sia i documenti dell'AGID e il successivo *Framework Nazionale per la Cybersecurity e la Data Protection* prendono le mosse da un concetto base della sicurezza: è possibile difendere solo ciò che si conosce. In tutti i provvedimenti sopra richiamati, pertanto, il primo passo richiesto alle amministrazioni pubbliche è il censimento dei loro beni ICT e la predisposizione di un inventario. Applicando la stessa logica per il passaggio al cloud, come meglio rappresentato di seguito, le pubbliche amministrazioni hanno dovuto effettuare una preventiva analisi dei propri dati e servizi, classificandoli con riguardo al livello di protezione richiesto dalla loro natura, al fine di definire la tipologia a loro più consona.

La direttiva, peraltro, pone in rilievo la definizione di ruoli e responsabilità, fondamentale per l'applicazione di un altro principio cardine della sicurezza, cosiddetto "*least privilege*". Il principio del privilegio minimo stabilisce che un soggetto dovrebbe avere accesso soltanto a specifici dati, applicazioni o risorse strettamente necessari per il completamento di una determinata attività della quale il soggetto è responsabile. La sua applicazione richiede, quindi, la predisposizione di una mappa aggiornata dove si evidenziano i soggetti, interni ed esterni all'Amministrazione, con i rispettivi ruoli e responsabilità in funzione dei quali è richiesta l'interazione con determinati sistemi hardware e software dell'Amministrazione stessa.

Allineandosi alla normativa tecnica di settore del NIST alla quale si ispirano, tutti i documenti italiani in materia di cybersicurezza messi a confronto presentano l'indicazione per le PA della predisposizione del piano di gestione delle vulnerabilità e del piano di risposta in caso di incidente. L'obiettivo dei piani è quello di avere un'indicazione puntuale e scritta delle azioni da svolgere sia per la fase di protezione alle possibili vulnerabilità sia per la fase più delicata di risposta a un incidente di sicurezza già avvenuto.

Un'importante novità della direttiva, rispetto alla precedente circolare AGID e all'impostazione del Framework (che ha comunque una visione di più ampia prospettiva essendo rivolto tanto a organizzazioni private che pubbliche), sta nell'individuazione di figure professionali dedicate alla sicurezza all'interno dei Ministeri. Se nel 2017 si chiedeva allo stesso Responsabile per la transizione digitale (RTD) lo svolgimento dei compiti connessi agli aspetti di sicurezza, con la nuova direttiva i Ministeri sono chiamati ad individuare fra il loro personale (e non fra quello delle società delle quali eventualmente si servano per il funzionamento dei propri sistemi informativi) un "incaricato per la cybersicurezza". Si tratta di una figura nuova richiesta ai Ministeri, che sia da punto di contatto

14. Cfr. CIS-Sapienza-CINI Cybersecurity National Lab 2019.

Direttiva del PCM del 29 dicembre 2023 (G.U. 16 febbraio 2024)	Misure minime di sicurezza, Circolare AGID (G.U. 5 maggio 2017)	Framework Nazionale per la Cybersecurity e la Data Protection
censimento dei sistemi hardware e software, oltre che dei flussi di dati utilizzati per lo svolgimento delle attività istituzionali	inventario delle risorse hardware e software (all. 1 alla circolare, ABSC1 e ABSC2); analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica (all. 1 alla circolare, ABSC13).	inventario di dispositivi e software (Appendice A, ID.AM - 1-5)
definizione di ruoli e responsabilità inerenti alla cybersicurezza, sia per il personale interno, che di terze parti che supportano l'amministrazione, con l'individuazione fra il personale della PA di un incaricato per la cybersicurezza, che sia da punto di contatto con l'ACN, oltre che di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi IT)	uso appropriato dei privilegi di amministratore: - assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse; - tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona (all. 1 alla circolare ABSC 5)	sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity, al trattamento e alla protezione dei dati per tutto il personale e per eventuali terze parti rilevanti (es., fornitori, clienti, partner) (ID.AM - 6-7)
piani per la gestione delle vulnerabilità; backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi; identità e relativi permessi	valutazione e correzione continua della vulnerabilità: definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (all. 1 alla circolare, ABSC4); copie di sicurezza (all. 1 alla circolare, ABSC10)	i backup delle informazioni sono eseguiti, amministrati e verificati; viene sviluppato e implementato un piano di gestione delle vulnerabilità; le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza (allegato A, PR.IP-4, PR.IP-12; PR.AC-1)
piano di risposta in caso di incidente, nel quale vengano puntualmente definite le articolazioni interne che – in stretto raccordo con l'incaricato per la cybersicurezza – sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un incidente cibernetico.	difese contro i malware: implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate (all. 1 alla circolare ABSC8)	sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/ disastro (PR.IP-9)

Tab. 1 — *Confronto fra i provvedimenti in materia di cybersicurezza rivolti alle PA (2016-2024)*

con l'ACN. Tale figura, secondo la direttiva, deve essere affiancata da un referente tecnico per la cybersicurezza, che dovendo essere individuato fra il personale responsabile della gestione operativa dei sistemi IT, potrà anche essere estraneo all'Amministrazione. Le figure professionali dedicate alla

cybersicurezza che i Ministeri destinatari della direttiva dovranno individuare integrano le funzioni in materia di sicurezza, che la norma da sempre assegna all'Ufficio per la transizione digitale. In particolare il CAD stabilisce che all'Ufficio del Responsabile per la transizione digitale siano affidati i compiti di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture (art. 17, co. 1, lett. c). Sotto il profilo organizzativo, con riferimento alle figure specializzate in materia di cybersicurezza delle quali le pubbliche amministrazioni devono dotarsi, la direttiva anticipa le indicazioni contenute nella nuova legge varata per il rafforzamento della cybersicurezza nazionale, l. 90/2024, di seguito illustrate.

4. I nuovi obblighi di segnalazione e notifica e le PA coinvolte

Il recente provvedimento legislativo in materia di cybersicurezza in vigore dal 17 luglio 2024 stabilisce che le pubbliche amministrazioni segnalano, secondo modalità predefinite, gli incidenti di sicurezza aventi impatto su reti, sistemi informativi e servizi informatici. Per agevolare la comunicazione con l'ACN, i soggetti che hanno subìto un incidente informatico sono tenuti alla segnalazione e notificazione facendo riferimento alla tassonomia descrittiva degli eventi informatici adottata con apposito provvedimento dell'ACN[15] (art. 1, comma 1, l. n. 90/2024). La tassonomia è una sorta di vocabolario degli incidenti di sicurezza più gravi, che richiedono un intervento immediato per il contenimento dei loro effetti. Le amministrazioni malcapitate dovranno collegarsi al sito dell'ACN per effettuare la segnalazione entro 24 ore dall'accaduto, fornendo entro 72 ore – che la norma espressamente fa decorrere dallo stesso momento – informazioni complete in sede di notifica (art. 1, co. 2, l. n. 90/2024). Mentre le PA centrali sono tenute all'attuazione delle disposizioni sopra richiamate dalla loro entrata in vigore, le restanti, invece, avranno più tempo per adeguarsi, poiché la norma prevede per loro l'entrata in vigore dopo centottanta giorni (art. 1, co. 3, l. n. 90/2024). Qualora l'evento non rientri nella tassonomia sopra richiamata, le PA coinvolte possono comunque procedere alla segnalazione, secondo la disciplina della notifica volontaria, introdotta con il decreto di recepimento della direttiva NIS[16] (art. 1, co. 4, l. n. 90/2024).

L'attenzione del legislatore sulle attività di notifica è forte, anche in considerazione dell'intensificarsi della minaccia cyber, al punto tale che sono previste visite ispettive – da disciplinarsi con un successivo provvedimento dell'ACN – e, nei casi di reiterata inosservanza, sanzioni pecuniarie fino a 125.000 euro a carico delle amministrazioni inadempienti rispetto all'obbligo di notifica, oltre alla responsabilità disciplinare e amministrativo-contabile non limitata ai soli dirigenti, ma anche ai funzionari responsabili (art. 1, co. 5 e 6, l. n. 90/2024).

La legge n. 90/2024 si rivolge a una pluralità di amministrazioni:

- pubbliche amministrazioni centrali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
- regioni, province autonome di Trento e di Bolzano, città metropolitane, comuni con popolazione superiore a 100.000 abitanti e, comunque, comuni capoluoghi di regione;
- società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;

15. Determina 3 gennaio 2023, contenente la *Tassonomia degli incidenti che debbono essere oggetto di notifica*. L'allegato associa un codice identificativo a ciascuna tipologia di incidente (es. con il codice "ICP-C-1" è indicato l'incidente così descritto in tassonomia: «Il soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota»).
16. La direttiva cosiddetta NIS (direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) è stata recepita in Italia con il d.lgs. 65/2018, che all'art. 18 stabilisce, fra l'altro, che il CSIRT Italia tratti le notifiche volontarie con priorità inferiore rispetto a quelle obbligatorie e soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo. Il soggetto notificante, a sua volta, non è sottoposto a nessuno degli obblighi a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

– aziende sanitarie locali;
– società in house delle sopra richiamate amministrazioni che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti (art. 1, co. 1, l. n. 90/2024).

Lo stesso articolo individua, altresì, i soggetti che non sono tenuti all'attuazione del medesimo articolo 1 (art. 1, co. 7, l. n. 90/2024)[17].

La richiamata disposizione individua in questo modo un ambito di applicazione per alcuni versi nuovo e, comunque, non direttamente sovrapponibile con quello cui si riferiscono le principali norme nel settore della digitalizzazione della pubblica amministrazione.

La legge n. 90/2024, in particolare, per le PA centrali si riferisce alla legge in materia di contabilità e finanza pubblica, l. n. 196/2009 che, a sua volta, rimanda alla lista S.13. La lista S.13 – largamente utilizzata nell'ambito della contabilità e finanza pubblica – per quanto attiene alla disciplina di digitalizzazione delle PA, invece, viene utilizzata per la prima volta nel 2020 con riferimento all'obbligo delle PA alla migrazione al cloud[18]. Definita annualmente dall'ISTAT e pubblicata in Gazzetta ufficiale per la sua importante valenza economico finanziaria – in quanto costituisce il riferimento per l'elaborazione dei conti economici nazionali e del conto economico consolidato delle amministrazioni pubbliche, che sono alla base del calcolo degli indicatori trasmessi dall'Istat alla Commissione europea, in applicazione del Protocollo sulla procedura per i deficit eccessivi annesso al Trattato di Maastricht – la lista S.13 risulta composta da tre sotto settori:

– "Amministrazioni centrali";
– "Amministrazioni locali";
– "Enti nazionali di previdenza e assistenza"[19].

Nel definire il perimetro di applicazione, la legge n. 90/2024 cita espressamente le "Amministrazioni centrali" della lista S.13, con ciò escludendo le rimanenti amministrazioni ivi elencate, ossia le "Amministrazioni locali" e gli "Enti nazionali di

17. Sono espressamente escluse dall'applicazione del solo articolo 1 della l. n. 90/2024: - operatori di servizi essenziali, intesi come soggetti pubblici o privati del settore dell'energia elettrica, petrolio, gas; settore del trasporto aereo, ferroviario e marittimo, oltre che stradale (limitatamente alle sole "autorità stradale", ossia qualsiasi autorità pubblica responsabile della pianificazione, del controllo o della gestione delle strade, come definita dal all'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione e i gestori di sistemi di trasporto intelligente definiti all'art. 1, co. 1, lett. *a*), del decreto del Ministro delle infrastrutture e dei trasporti 1 febbraio 2013); settore bancario; settore delle infrastrutture dei mercati finanziari; istituti sanitari compreso ospedali e cliniche; fornitori e distributori di acqua potabile; operatori nel settore delle infrastrutture digitali (essenzialmente gli operatori indispensabili per il funzionamento della rete Internet); fornitori di servizi digitali (art. 3, co. 1, lett. *g*) ed *i*) del d.lgs. 18 maggio 2018, n. 65, con il quale è stata recepita la direttiva NIS che sarà abrogata a partire dal 18 ottobre 2024). Per la definizione di "fornitori di servizi digitali" il decreto di recepimento della direttiva NIS non offre una chiara definizione, rinviando a quella di "servizio digitale" contenuta nella direttiva dir. n. 2015/1535 (direttiva del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione) dove all'art. 1, par. 1, si definisce il servizio digitale come «qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»; - i soggetti elencati nel perimetro di cybersicurezza nazionale (art. 1, co. 2-*bis*, del d.l. n. 105/2019). Tale elenco è adottato con un atto amministrativo non soggetto a pubblicazione (ed escluso dal diritto di accesso), fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco (art. 1, co. 7, lett. *a*), l. n. 90/2024). Inoltre sono esclusi dall'attuazione dell'art. 1, co. 1 della l. n. 90/2024 anche gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza (art. 1, co. 7, lett. *b*), l. n. 90/2024).
18. Art. 33-*septies*, d.l. n. 179/2012, come modificato dall'art. 35, co. 1, lett. *a*), d.l. 16 luglio 2020, n. 76, convertito, dalla l. 11 settembre 2020, n. 120.
19. Istat 2023.

previdenza e assistenza", come ad esempio INPS, INAIL, ecc. Con riguardo alle PA centrali, quindi, la legge n. 90/2024 si estenderebbe astrattamente (a meno di esclusioni derivanti dall'appartenenza al perimetro di sicurezza nazionale) anche agli organi costituzionali, che sono, ad esempio, esclusi dall'applicazione del CAD, ma rientrano, viceversa, nell'ambito di applicazione della disciplina in materia di cloud, in quanto appartenenti alla lista S.13 (art. 33-*septies* del d.l. 18 ottobre 2012, n. 179, convertito dalla l. 17 dicembre 2012, n. 221). Per quanto attiene alle pubbliche amministrazioni locali, la legge n. 90/2024 non si applica a tutte quelle elencate nella lista S.13, ma a un loro sottoinsieme: determinati comuni, individuati sulla base della maggiore numerosità della popolazione residente o dell'essere capoluogo di regione, e le aziende sanitarie. L'interpretazione letterale dell'ambito di applicazione così definito dalla legge n. 90/2024, infine, porterebbe ad escludere in ogni caso gli enti previdenziali e assistenziali. Tali enti, infatti, non sono inclusi in nessuna delle fattispecie sopra elencate, essendo classificati dalla lista S.13 come "Enti nazionali di previdenza ed assistenza", pur rientrando, tuttavia, nell'ambito di applicazione dl CAD, in quanto assoggettati al d.lgs. 30 marzo 2001, n. 165[20].

Se, dunque, l'ambito di applicazione della legge n. 90/2024 è restrittivo con riguardo alle pubbliche amministrazioni territoriali – in quanto esclude quelle di dimensioni inferiori ai 100.000 abitanti, a meno che non siano capoluoghi di regione (Ancona, Aosta, Campobasso, Catanzaro, L'Aquila, Potenza) – con riguardo alle pubbliche amministrazioni centrali, invece, copre una superficie differente da quelle indicata dal CAD.

Altra caratteristica dell'ambito di applicazione della legge n. 90/2024 è rappresentata dall'inclusione di un insieme di aziende definite sulla base della tipologia dell'attività economica svolta: sanità, trasporto pubblico, raccolta, smaltimento o trattamento di acque, gestione dei rifiuti. Si tratta di un'impostazione già presente nella direttiva NIS, ma rafforzata nella direttiva cosiddetta NIS 2[21], in corso di adozione in Italia, che, nell'aggiornare la precedente direttiva NIS, intende, fra l'altro, omogeneizzare fra gli Stati membri l'ambito di applicazione, la cui delimitazione è stata lasciata alla loro discrezione. Una delle principali novità della nuova direttiva NIS sta proprio nell'aver esteso il suo ambito di applicazione prevedendovi, fra l'altro, espressamente le pubbliche amministrazioni[22]. Ciò anche a dimostrazione di quanto la cybersicurezza sia un tema sempre più centrale nell'attività amministrativa degli Stati membri.

La Tabella 2, prendendo a riferimento le principali norme rivolte alle PA in materia di digitalizzazione e cybersicurezza (CAD, disciplina in materia di cloud e la recente disciplina sulla cybersicurezza) riassume il relativo ambito di applicazione.

Per quanto limitata, l'analisi sull'ambito di applicazione delle discipline in materie di digitalizzazione e sicurezza, sopra brevemente illustrata, mostra da un lato la delicatezza con la

20. Gli atti parlamentari, peraltro, con riferimento all'ambito di applicazione non forniscono ulteriori indicazioni (atti parlamentari Camera dei deputati, AC 1717, presentato il 17 febbraio 2024).

21. Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

22. La direttiva NIS2 distingue i soggetti che entrano nel novero di applicazione della direttiva NIS2 in essenziali ed importanti, individuando per essi due regimi differenti. Lo sforzo richiesto alle organizzazioni per l'attuazione della disciplina in materia di cybersicurezza, infatti, è considerevole, cosicché sulla base del tipo di servizio erogato e della sua criticità in caso di interruzione, sono definite misure di protezione differenti. La direttiva definisce le PAC soggetti essenziali e le PAL soggetti importanti, salvo che il singolo Stato membro non le definisca essenziali. Ciascuno Stato membro può identificare una pubblica amministrazione regionale come soggetto essenziale quando il Paese ritenga che tale amministrazione rientri in una delle seguenti casistiche: - rappresenta l'unico fornitore di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali; - una perturbazione del servizio fornito da tale amministrazione potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica o potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero; - risulta critica in ragione della sua particolare importanza a livello nazionale o regionale.

		NORME IN MATERIA DI DIGITALIZZAZIONE E CYBERSICUREZZA DELLE PA		
		CAD (d.lgs. n. 82/2005)	**art. 33-septies, d.l. n. 179/2012**	**legge n. 90/2024 (art. 1)**
TIPOLOGIA DI PA CUI SI APPLICA LA DISCIPLINA SU DIGITALIZZAZIONE E CYBERSICUREZZA	**PAC lista S.13**	X (1)	X	X (8)
	PAL lista S.13	X (2)	X	Solo aziende sanitarie locali e comuni al di sopra dei 100.000 abitanti o capoluoghi di regione
	enti nazionali di previdenza e assistenza	X (3)		
	autorità amministrative indipendenti di garanzia, vigilanza e regolazione	X	X (4)	X (10)
	gestori di servizi pubblici	X	X (9)	X (5)
	società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175	X (6)	X (9)	X (7)

(1) purché assoggettati al d.lgs. n. 165/2001 o autorità indipendenti
(2) purché assoggettati al d.lgs. n. 165/2001 o autorità di sistema portuale
(3) purché assoggettati al d.lgs. n. 165/2001
(4) limitatamente a quelle indicate fra le "Autorità indipendenti" della lista S.13: sono, ad esempio, incluse l'Autorità garante della concorrenza e del mercato, l'Autorità per le garanzie nelle comunicazioni, ma escluse dalla lista S.13 Consob (Commissione nazionale per la società e la borsa, che è l'autorità italiana per la vigilanza dei mercati finanziari) e IVASS (Istituto per la vigilanza sulle assicurazioni, che è un'autorità indipendente)
(5) limitatamente ai servizi di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133)
(6) escluso le società quotate
(7) limitatamente alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e alle società in house delle amministrazioni oggetto della L. n. 90/2024 che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti, purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-*bis*, del d.l. n. 105/2019)
(8) purché non presenti nell'elenco del perimetro di sicurezza nazionale (articolo 1, comma 2-*bis*, del d.l. n. 105/2019)
(9) purché presenti nella lista S.13, sottosettore "Amministrazioni centrali" o "Amministrazioni locali"
(10) limitatamente a quelle indicate fra le "Autorità indipendenti" della lista S.13, purché non presenti nell'elenco del perimetro di sicurezza nazionale

Tab. 2 — *Tipologia di PA cui si applicano le norme in materia di digitalizzazione e cybersicurezza*

quale occorre intervenire laddove nuovi oneri sono posti in capo alle amministrazioni spesso costrette a fronteggiare le nuove disposizioni con personale ridotto, dall'altro la difficoltà di omogeneizzazione in una materia travolta in questi ultimi anni da una convulsa produzione normativa, che allo stato, non ha ancora trovato l'auspicabile sintesi[23].

23. Cfr. al riguardo anche Longo 2024 che ha ribadito la necessità di un coordinamento tra le norme attuali e le emanande disposizioni del decreto legislativo di attuazione [NIS2] nella sua Audizione informale per il disegno

5. Le segnalazioni dell'Agenzia per la cybersicurezza nazionale e i soggetti pubblici e privati coinvolti

Oltre alle segnalazioni *ex-post* che le PA devono effettuare all'ACN in caso di incidente, la legge individua anche la possibilità che *ex-ante* sia l'Agenzia per la cybersicurezza nazionale a segnalare specifiche vulnerabilità cui le PA possono essere esposte. In tal caso le PA sono tenute ad adottare sollecitamente tutti gli accorgimenti indicati dalla stessa ACN e comunque entro quindici giorni. Deroghe a tali termini sono consentite solo qualora vi siano «motivate esigenze di natura tecnico-organizzativa» per le quali non sia possibile provvedere o procedere nei termini indicati. Tali motivate esigenze, in ogni caso, la PA deve farsi carico di comunicarle tempestivamente all'ACN, pena l'applicazione di sanzioni (art. 2, l. n. 90/2024).

Le disposizioni sopra richiamate sono valide non sole per tutte le pubbliche amministrazioni centrali della lista S.13, regioni, province autonome di Trento e di Bolzano, città metropolitane, comuni con popolazione superiore a 100.000 abitanti e, comunque, comuni capoluoghi di regione, società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, aziende sanitarie locali, società in house delle sopra richiamate amministrazioni che forniscono servizi informatici, servizi di trasporto ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, o di gestione dei rifiuti, ma anche per tutti i soggetti, quindi sia pubblici che privati, espressamente esclusi dall'ambito di applicazione dell'articolo 1 della legge n. 90/2024, ossia i soggetti presenti nell'elenco che costituisce il perimetro di cybersicurezza nazionale, gli operatori pubblici o privati di servizi essenziali, quali ad esempio trasporto ed energia (*amplius* nota 17), oltre che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (art. 2, co. 1, l. 90/2024).

6. La struttura e il referente per la cybersicurezza

Le PA centrali e locali, oltre che i gestori di pubblici servizi e le in house, definite nell'art. 1 della legge n. 90/2024, senza nuovi oneri individuano una nuova struttura, qualora non già presente, che segua la cybersicurezza (art. 8, l. n. 90/2024[24]). La norma ne elenca puntualmente le funzioni, che vanno dallo sviluppo delle politiche e procedure di sicurezza alla predisposizione di un piano per la gestione del rischio informatico, oltre che la definizione in un apposito documento dei ruoli e dell'organizzazione del sistema per la sicurezza delle informazioni della PA. La struttura è anche responsabile per la predisposizione di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione da tenere aggiornato, che tenga anche conto della pianificazione di specifici interventi da realizzare per aumentare la capacità nella gestione dei rischi cibernetici. È assegnato a tale struttura, inoltre, il compito di dare attuazione alle linee guida per la cybersicurezza emanate dall'ACN[25], oltre che il monitoraggio e la valutazione continua delle minacce e delle vulnerabilità. Si tratta di adempimenti non nuovi per le amministrazioni, in quanto allineati alle indicazioni del NIST. Presso tale struttura la norma ha stabilito che sia operativo un referente per la cybersicurezza, con specifiche

di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717).

24. L'ambito di applicazione dell'art. 8 della l. n. 90/2024 rinvia a quello dell'art. 1 della stessa legge, a esclusione non di tutte le PA indicate nell'art. 1, co. 7 (cfr. nota 17), ma di un insieme più piccolo. Sono esclusi dall'ambito di applicazione dell'art. 8 della legge n. 90/2024 solo i soggetti inseriti nel perimetro di cybersicurezza nazionale e gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza (art. 8, co. 6, l. n. 90/2024).

25. Come espressamente previsto dall'art. 9 della l. n. 90/2024 dovranno essere attuate le linee guida di ACN in materia di crittografia e conservazione delle password (quest'ultime adottate insieme al Garante per la protezione dei dati personali), verificando che non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati. Tale disposizione si estende anche ai soggetti inclusi nel perimetro e a quelli indicati nella disciplina di attuazione della NIS.

e comprovate professionalità e competenze in materia, che rappresenta il punto di contatto unico dell'amministrazione con l'ACN (art. 8, commi 1 e 2, l. n. 90/2024). In questo modo la norma delinea la necessità, già percepita da diverse istituzioni non solo private, di individuare la figura, generalmente indicata con l'acronimo di CISO (*Chief information security officer*), che recentemente in Italia si è organizzata in associazione[26].

Fermo restando che la struttura descritta e il referente per la cybersicurezza possono coincidere rispettivamente con l'Ufficio per la transizione digitale (UTD) e il suo responsabile (RTD), il legislatore, nella piena consapevolezza della ridotta disponibilità di personale tecnico nella PA, introduce ulteriori opzioni. Anzitutto stabilisce la possibilità di conferire l'incarico di referente per la cybersicurezza a un dipendente di un'altra PA, previo l'autorizzazione di quest'ultima (art. 8, co. 3, l. n. 90/2024) e poi, analogamente alle funzioni di RTD e UTD ne prevede la "forma associata", richiamando espressamente le indicazioni del CAD in materia (art. 8, co. 4, l. n. 90/2024). Quello della "forma associata" è un istituto pensato nel CAD prevalentemente per le PA di dimensioni ridotte, comunque diverse dalle "Amministrazioni dello Stato" che, avendo difficoltà a reperire personale qualificato nei loro ruoli, attraverso un'apposita convenzione definiscono l'UTD e nominano l'RTD insieme, in modo che l'ufficio e il suo responsabile provvedano allo stesso tempo alle esigenze di più amministrazioni. Per supportare le PA nell'attuazione pratica della costituzione dell'UTD e della nomina dell'RTD in forma associata, AGID ha predisposto un apposito *Vademecum* pubblicato lo scorso giugno. Come lascia intendere lo stesso schema di convenzione allegato al Vademecum e la formulazione recentemente novellata del comma 1-*septies* dell'art. 17 CAD, per la nomina dell'RTD in forma associata si può ricorrere anche a personale delle società in house. Pertanto è possibile dedurre anche per la nomina del referente della cybersicurezza che le PA possano farlo in forma associata per il tramite delle loro *in house*[27]. L'obiettivo complessivo è aumentare la resilienza delle PA, motivo per cui la norma assegna all'ACN anche il potere di definire ulteriori modalità e processi di coordinamento e di collaborazione tra le amministrazioni e i referenti per la cybersicurezza (art. 8, co. 5, l. n. 90/2024). In altri termini è ipotizzabile immaginare che laddove le PA per motivi organizzativi non riescano a definire un loro referente, sia la stessa ACN a dettare le modalità operative alternative per garantire il coordinamento in materia cyber.

7. L'approvvigionamento di beni e servizi ICT in sicurezza

Ulteriori adempimenti delle amministrazioni, infine, riguardano l'approvvigionamento di beni e servizi informatici da impiegarsi per la tutela degli interessi nazionali strategici o per la tutela della sicurezza nazionale. L'art. 14 della l. n. 90/2024 stabilisce che con un decreto del Presidente del Consiglio dei ministri saranno individuate specifiche categorie tecnologiche di beni e servizi informatici per le quali devono essere previsti criteri premianti, laddove le proposte o le offerte relative contemplino l'uso di tecnologie di cybersicurezza italiane o di specifici Paesi (appartenenti all'Unione europea o aderenti all'Alleanza atlantica, ecc.). La disposizione sopra richiamata si rivolge a un altro gruppo di amministrazioni, ed esattamente a quelle che costituiscono l'ambito di applicazione del CAD. In attesa che il decreto attuativo chiarisca le forniture cui si applica la disposizione introdotta dalla legge n. 90/2024, è evidente che la norma sopra richiamata intende non solo proteggere le forniture italiane ed europee, ma soprattutto promuovere tecnologie italiane o di Paesi alleati, che, rispetto a quelle di Paesi terzi, possono offrire maggiori garanzie in caso di problemi di sicurezza.

8. Il cloud delle pubbliche amministrazioni

Quando il cloud si è affacciato sul mercato italiano e AGID ne ha previsto l'adozione per le pubbliche

26. Associso.

27. Nel richiamare espressamente anche il comma 1-*sexies* dell'art. 17 CAD, probabilmente il legislatore intende limitare l'applicazione di questa disposizione alle sole PA non statali fra quelle individuate dall'art. 1, co. 1, l. n. 90/2024.

amministrazioni[28], come spesso accade per le nuove tecnologie, un certo gruppo di "addetti" l'ha accolto con ostilità. Quasi sistematicamente in riunioni informali, convegni o seminari veniva sollevata la questione della "sicurezza" del cloud. Il dibattito, quando non sfociava in scenari di apocalittica manipolazione, oscillava comunque fra l'inaccettabile incertezza del luogo dove fisicamente il dato (o il servizio) pubblico erano ospitati e la convinta repulsione verso potenze straniere, detentrici delle tecnologie cloud che avrebbero potuto immagazzinare quel dato, facendone automaticamente vacillare la sovranità. Nel frattempo che la diffidenza sulle tecnologie cloud si sviluppava in modalità per certi versi pretestuosamente ottusa, la naturale obsolescenza delle infrastrutture pubbliche e/o gli attacchi di sicurezza colpivano dati e servizi digitali delle pubbliche amministrazioni nella loro riservatezza, integrità o affidabilità.

I dati e i servizi della pubblica amministrazione oggi sono considerati i nuovi beni pubblici da proteggere adeguatamente. Cosicché già nell'edizione 2019-2021 il piano triennale per l'informatica nella PA introduce il principio *cloud first*, invitando le pubbliche amministrazioni a utilizzare prioritariamente soluzioni cloud. Le tecnologie cloud, fino a poco prima catalogate come anello debole della catena di sicurezza digitale della PA, vengono collocate fra le tecnologie obbligatorie, in quanto abilitanti a garantire la riservatezza, ma soprattutto disponibilità e integrità delle informazioni pubbliche. A tal fine il PNRR dedica i primi due investimenti della prima componente della prima missione al cloud, con uno stanziamento iniziale di circa 2 miliardi di euro[29]. Dopo poco, con la presentazione a settembre 2021 della strategia del Governo italiano sul cloud della pubblica amministrazione, la visione sulle tecnologie cloud è completamente ribaltata: da elemento di erosione a pilastro imprescindibile per la cybersicurezza delle pubbliche amministrazioni.

8.1. La normativa e la strategia sul cloud delle PA

La norma in materia di cloud è contenuta all'interno dell'art. 33-*septies* del d.l. n. 179/2012, che ha subìto fino al 2021 diverse modifiche. L'attuale rubrica dell'articolo 33-*septies* "Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese", che corrisponde a quella originariamente attribuita alla disposizione inserita in sede di conversione del d.l. n. 179/2012, conserva al suo interno la finalità originaria per la quale è stato introdotto il cloud nella pubblica amministrazione: condividere le risorse infrastrutturali delle pubbliche amministrazioni per raggiungere risparmi di spesa. Il provvedimento originario, peraltro, era stato inserito all'interno di uno dei decreti d'urgenza del Governo Monti, che intendevano sostenere l'innovazione per la crescita del Paese[30]. Già nello scorso decennio, infatti, si puntava al digitale, come volàno per far ripartire l'economia italiana, duramente provata dalla crisi finanziaria del 2011.

28. Il Piano triennale nel 2017-2019 indicava come «le Infrastrutture fisiche perseguono l'obiettivo di aumentare la sicurezza, ridurre il costo delle infrastrutture tecnologiche e migliorare la qualità dei servizi software della Pubblica amministrazione, attraverso la razionalizzazione dei data center, l'adozione sistematica del paradigma cloud e lo sviluppo della connettività», prevedendo che «la realizzazione del cloud della PA» avrebbe consentito di virtualizzare «il parco macchine di tutte le Pubbliche amministrazioni, con importanti benefici in termini di costi e di gestione della manutenzione». Già nel 2017 con la circolare n. 5/2017 l'AGID introduce il tema del cloud per le pubbliche amministrazioni. L'AGID successivamente avvia il censimento dei dati center con il quale si mette a nudo tutta la fragilità delle infrastrutture utilizzate dalle PA. Cosicché con la circolare n. 1 del 14 giugno 2019 viene previsto l'obbligo di "migrare senza indugio al Cloud della PA" per quelle PA, che costituivano la stragrande maggioranza, con data center dalle caratteristiche tecniche inadeguate.
29. In particolare 900 milioni di euro sono stati dedicati alla realizzazione del Polo strategico nazionale, gestito dall'omonima società, per mettere a disposizione delle PA servizi cloud di tipi IaaS (*Infrastructure as a service*), PaaS (*Platform as a service*) e SaaS (*Software as a service*), mentre un miliardo di euro è stato stanziato per tutte le attività connesse all'abilitazione e alla facilitazione di migrazione al cloud delle pubbliche amministrazioni.
30. Il d.l. n. 179/2012 definisce le modalità di attuazione dell'agenda digitale italiana, introdotta dall'articolo 47 del precedente d.l. Monti 9 febbraio 2012, n. 5 e prevede molteplici disposizioni in materia di digitalizzazione (identità digitale, dati di tipo aperto, sanità digitale, giustizia digitale, ecc.).

L'attuale formulazione dell'art. 33-*septies* stabilisce due differenti regimi per le PA centrali e per le PA locali. In entrambi i casi la norma per definire il perimetro di applicazione fa riferimento alla lista S.13 ISTAT.

In particolare, per le PA centrali che abbiano CED (Centri per l'elaborazione dati) non in linea con i regolamenti in materia[31] si configurano tre possibili opzioni di migrazione dei loro CED e dei relativi sistemi informatici:

1) verso il Polo strategico nazionale (PSN);
2) verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dallo stesso Regolamento;
3) verso soluzioni cloud di fornitori esterni, purché esse siano coerenti con le specifiche tecniche, anch'esse definite nel Regolamento cloud ACN (art. 33-*septies*, comma 1, d.l. n. 179/2012).

Anche per le amministrazioni locali, intendendosi tutte quelle elencate nella lista S.13, si configurano similmente alle PA centrali tre possibili scelte per la migrazione, con la differenza che mentre le PAC devono migrare necessariamente verso una "propria" infrastruttura alternativa, viceversa le PAL possono migrare «verso altra infrastruttura già esistente in possesso dei requisiti fissati dallo stesso regolamento» (art. 33-*septies*, co. 1-*bis*, d.l. n. 179/2012). Con ciò si intende consentire alle PAL di avvalersi delle infrastrutture delle proprie società in house.

Come osservato per la legge n. 90/2024, anche in questo caso, l'analisi letterale della disposizione porterebbe a dedurre che gli enti nazionali di previdenza e assistenza, compresi INPS e INAIL, siano fuori dall'ambito di applicazione dell'art. 33-*septies* del d.l. n. 179/2012. Benché le esclusioni e i limiti di applicazioni della disciplina siano elencati in specifici commi[32], tuttavia l'art. 33-*septies* cita espressamente soltanto le PA centrali e le PA locali della lista S.13, che non includono gli enti previdenziali e assistenziali, annoverati nel relativo sottosettore.

La strategia italiana sul cloud è stata trasposta nella Regolamentazione tecnica di settore. Occorre premettere che, diversamente dalla strategia in materia di cybersicurezza rivolta tanto al settore pubblico quanto a quello privato, la strategia cloud del Governo italiano si riferisce esclusivamente alle pubbliche amministrazioni. Essa prevede la costruzione di una "casa moderna" per i dati e i servizi con più "stanze" aventi livelli crescenti di sicurezza commisurati alla tipologia di dati e servizi pubblici da ospitare.

La strategia si articola su tre direttrici, che coinvolgono:

- le singole PA per la classificazione di dati e servizi;
- i fornitori privati che erogano servizi cloud (c.d. CSP, ossia *cloud service provider*) per la qualificazione dei servizi cloud erogati alle PA;
- il PSN[33].

Di seguito si approfondiscono i principali adempimenti in capo alle PA in materia di cloud.

8.2. La classificazione dei dati e dei servizi pubblici

Per l'attuazione della strategia cloud le PA sono tenute anzitutto a classificare i propri dati e servizi in ordinari, critici o strategici sulla base degli

31. Emanati originariamente da AGID, poi emendati dall'ACN, i regolamenti sul cloud sono stati consolidati nel recente Regolamento cloud ACN.

32. Sono esclusi i CED delle PA centrali soggetti alla gestione di dati classificati secondo la normativa in materia di tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle classificate nazionali (art. 33-*septies*, co. 3); sono previste inoltre le stesse limitazioni indicate dal CAD all'art. 2, co. 6, d.lgs. n. 82/2005, dove si stabilisce la disapplicazione della disciplina «limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile», ma se ne prevede espressamente l'applicazione «al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico» (art. 33-*septies*, co. 4- *quater*); sono inoltre disapplicate le norme dell'art. 33-*septies* nell'esercizio delle attività relative alla difesa e sicurezza nazionale svolte dalle infrastrutture digitali dell'amministrazione della difesa (art. 33-*septies*, co. 4-*bis*).

33. Dipartimento per la Trasformazione Digitale–Agenzia per la Cybersicurezza Nazionale 2021.

effetti che la perdita di un dato o l'interruzione di un servizio può produrre. Ad esempio, i dati e servizi afferenti alle funzioni essenziali dello Stato saranno classificati come strategici, i dati sanitari dei cittadini saranno classificati come critici, mentre dati e servizi relativi a portali istituzionali delle amministrazioni saranno classificati come ordinari, in quanto le informazioni ivi contenute sono già note a tutti. La classificazione dei dati e servizi pubblici è un'operazione necessaria e propedeutica per la migrazione al cloud, ma anche per l'erogazione degli stessi servizi. Tant'è che se i servizi non sono preventivamente stati classificati ne è vietata l'erogazione agli utenti (art. 3, co. 6, Regolamento cloud ACN). Si tratta di una disposizione non presente nel previgente Regolamento sul cloud[34], con la quale si intende anche garantire l'utenza: un servizio pubblico può essere fruito solo se si è provveduto alle preventive operazioni di classificazione.

Il citato Regolamento, riprendendo il concetto di classificazione introdotto nella strategia cloud, prevede tre differenti classi per i dati e servizi delle PA:

a) «ordinari», qualora la loro compromissione non determini i pregiudizi di cui alle seguenti lettere b) e c);
b) «critici», se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
c) «strategici», se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale[35].

Lo stesso Regolamento disciplina nell'allegato 1 le modalità per la predisposizione dell'elenco e della classificazione dei dati e dei servizi della pubblica amministrazione, prevedendo delle semplificazioni per le PA. In particolare si stabilisce che l'ACN predisponga con cadenza almeno biennale elenchi predefiniti di dati e/o servizi, già corredati della relativa classificazione, per gruppi omogenei di amministrazioni sulla base di tre parametri: anzitutto, il rischio e l'evoluzione della minaccia di natura cibernetica, poi, la normativa e gli standard nazionali, europei e internazionali del settore, infine, i rischi per i diritti e le libertà delle persone fisiche (art. 4, co. 2 e 3 del Regolamento cloud ACN). Le PA, sulla base delle indicazioni fornite da ACN e rese disponibili sulla piattaforma digitale[36], stilano la propria classificazione dei loro dati e servizi (art. 5, comma 1, Regolamento cloud ACN) e provvedono a darne comunicazione all'ACN. Anche per le PA è previsto l'aggiornamento della classificazione dei dati e servizi con cadenza biennale[37] o comunque in presenza di una variazione nel frattempo intervenuta. L'ACN provvede alla verifica di conformità e comunica alla PA gli esiti di tale verifica, che possono concludersi con la convalida della piena conformità dell'elenco e della classificazione dei dati e dei servizi digitali, oppure con la conformità con prescrizioni o con la non convalida.

La classificazione dei dati e dei servizi, quindi, è un'operazione che la PA svolge secondo direttrici ben precisate dall'ACN, cui, in ogni caso spetta l'ultima parola. Una classificazione incauta, dove, ad esempio, servizi strategici fossero classificati come ordinari, esporrebbe potenzialmente l'amministrazione pubblica ad attacchi che potrebbero compromettere la sicurezza nazionale. Viceversa una classificazione

34. AGID, determinazione n. 628/2021, *Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione*.
35. Art. 3, co. 4, Regolamento cloud ACN.
36. Indicata in allegato 1, che a sua volta rinvia alla lettera z), invece che alla lettera u) dell'art. 1, comma 1 del Regolamento, la piattaforma digitale è accessibile dalla sezione "cloud" del sito istituzionale dell'ACN e consente tutte le operazioni (classificazione dei dati e dei servizi della pubblica amministrazione, adeguamento delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni ovvero dei servizi cloud erogati da operatore pubblico, qualificazione dei servizi cloud).
37. L'art. 5, co. 1, del previgente Regolamento stabiliva che le PA presentassero per la prima volta all'ACN entro il 18 luglio 2022 la classificazione dei dati e dei servizi digitali. Cosicché da luglio 2024 le PA dovranno aggiornare la classificazione dei dati e servizi precedentemente presentata all'ACN.

dei dati eccessivamente prudente, nella quale, ad esempio, dati ordinari sono classificati come strategici, comporterebbe spese inutili, conseguenti a una protezione dei dati esagerata rispetto al rischio della loro eventuale compromissione.

8.3. I livelli minimi delle infrastrutture e dei servizi cloud

Il capo III del Regolamento cloud ACN definisce sia i livelli minimi delle infrastrutture digitali per le pubbliche amministrazioni[38], sia i livelli minimi delle infrastrutture che ospitano i servizi cloud destinati alle PA[39] (infrastrutture digitali per i servizi cloud), oltre che le caratteristiche dei servizi cloud che le PA possono acquisire. Non tutti i servizi cloud, infatti, possono essere utilizzati dalle pubbliche amministrazioni, ma solo quelli che siano rispondenti a determinati requisiti dettagliati nell'allegato 2, anche sulla base del *Framework nazionale per la cybersecurity e la data protection* (art. 6, co. 1, Regolamento cloud ACN), a dimostrazione dell'evidente stretta correlazione fra la qualità della fornitura cloud e le garanzie di sicurezza associate. L'allegato 2 del Regolamento è strutturato in più sezioni che delineano i livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture necessari per ospitare dati e servizi ordinari. Oltre agli aspetti di riservatezza, affidabilità e integrità dei dati e servizi, devono essere osservati anche specifici requisiti connessi alla sostenibilità ambientale: quanto minore è il consumo energetico rispetto alla capacità elaborativa prodotta tanto minore sarà l'impatto per il pianeta[40]. In particolare i dati e servizi ordinari delle PA possono utilizzare solo infrastrutture conformi alle specifiche tecniche indicate nella sezione 2 dell'allegato 2; i dati e servizi critici, invece, possono utilizzare solo infrastrutture che garantiscano la conformità non solo alle specifiche tecniche indicate nella sezione 2 dell'allegato 2, ma anche a quelle indicate nella sezione 3. Infine i dati e servizi strategici devono utilizzare solo servizi cloud che, oltre a rispondere alle caratteristiche già richieste per i servizi critici (e quindi ordinari), rispondono anche alle caratteristiche indicate nella sezione 4 dell'allegato 2 (art. 7, Regolamento cloud ACN). Quanto più delicati, quindi, sono i dati e i servizi da proteggere, tanto più stringenti sono i requisiti richiesti alle infrastrutture che li ospitano.

Sono definite, invece, nell'allegato 3 le caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità e di portabilità dei servizi cloud dei quali le PA possono approvvigionarsi. In modo analogo a quanto descritto per le infrastrutture, l'allegato 3 stabilisce che:

- i dati e servizi ordinari possono utilizzare servizi cloud che rispondono ai requisiti della sezione 2;
- i dati e servizi critici possono utilizzare servizi cloud che rispondono ai requisiti delle sezioni 2 e 3;
- i dati e servizi strategici possono utilizzare servizi cloud che rispondono ai requisiti delle sezioni 2, 3 e 4 (art. 8, Regolamento cloud ACN).

8.4. La migrazione delle PA al cloud

La definizione dei livelli minimi per le infrastrutture e delle caratteristiche per i servizi cloud sono funzionali alle attività di migrazione che le PA

38. "Infrastrutture digitali per le pubbliche amministrazioni": le infrastrutture digitali tramite le quali sono erogati i servizi digitali delle amministrazioni, ivi inclusi: i CED delle PA, il PSN, le componenti di un'infrastruttura digitale di terzi a disposizione delle PA per l'erogazione di servizi cloud (es. housing) oppure finalizzati all'incremento delle prestazioni nell'erogazione in prossimità dei servizi digitali delle amministrazioni (c.d. infrastrutture di prossimità). Nello specifico, si può trattare di un singolo server o di un altro insieme di risorse di calcolo connesse, operati nell'ambito di un'infrastruttura di prossimità, generalmente situati all'interno di un data center che opera all'estremità dell'infrastruttura, e quindi fisicamente più vicini agli utenti destinatari rispetto a un nodo cloud in un data center centralizzato (art. 1, co. 1, lett. *m*) del Regolamento cloud ACN).

39. Cosiddette "Infrastrutture dei servizi cloud per le pubbliche amministrazioni", ossia le infrastrutture digitali per le PA fornite da un operatore di infrastrutture digitali, tramite le quali sono erogati i servizi cloud per le pubbliche amministrazioni, (art. 1, co. 1, lett. *n*) del Regolamento cloud ACN).

40. Tutte le misure del PNRR di ciascuno Stato membro, peraltro, richiedono il rispetto di specifici requisiti di sostenibilità ambientale, riassunti nel principio cosiddetto DNSH (*Do Not Significant Harm*), connesso alla politica del *Green deal* europeo che mira a far diventare l'Europa il primo continente a impatto climatico zero.

dovranno effettuare, in attuazione del capo IV del Regolamento. Coerentemente con quanto indicato nella strategia sul cloud, infatti, il Regolamento ribadisce che i dati e servizi delle PA migrano verso infrastrutture e servizi cloud che abbiano rispettivamente livelli di servizio e caratteristiche commisurate con la particolarità del dato e del servizio da ospitare. Infrastrutture e servizi cloud adeguati per dati e servizi strategici lo saranno anche per i dati e servizi critici ed ordinari. Come pure infrastrutture e servizi cloud adeguati per dati e servizi critici potranno ospitare anche quelli ordinari, ma non quelli strategici, perché non saranno conformi ai livelli minimi/caratteristiche indicati nella sezione 4 rispettivamente dell'allegato 2 e dell'allegato 3 al Regolamento. La migrazione al cloud, che le PA devono effettuare in attuazione del citato art. 33-*septies* del d.l. n. 179/2012, va completata entro il 30 giugno 2026 (art. 11, comma 4, Regolamento cloud ACN), data che peraltro coincide con la chiusura del PNRR. L'attività richiede, fra l'altro, la predisposizione di piani di migrazione da caricare sulla piattaforma messa a disposizione dal Dipartimento per la trasformazione digitale, alla quale accedono anche l'ACN e l'AGID per le attività di rispettiva competenza. In particolare all'AGID è assegnato un ruolo di vigilanza, verifica, controllo e monitoraggio del rispetto degli obblighi di transizione digitale. In caso di violazione di tali obblighi, l'art. 18-*bis* del CAD – introdotto come ulteriore leva a garanzia dell'attuazione del PNRR – arriva a prevedere, in caso di reiterata e grave inottemperanza da parte della PA, la nomina di un commissario *ad acta* da parte del Presidente del Consiglio dei ministri.

8.5. L'adeguamento delle infrastrutture e dei servizi, la qualificazione dei servizi cloud

Il Regolamento stabilisce 4 livelli per i requisiti di adeguamento, da AI1 a AI4, dettagliati nell'allegato 4, che sono relativi alle infrastrutture digitali per le pubbliche amministrazioni e alle infrastrutture dei servizi cloud per le pubbliche amministrazioni (art. 12). I requisiti di ciascun livello sono elaborati tenuto conto di diversi aspetti: fattori di rischio ed evoluzione della minaccia cibernetica; normativa e standard nazionali, europei e internazionali; schemi di certificazione nazionali ed europei progressivamente adottati; migliori pratiche e linee guida di settore.

In particolare i dati e i servizi digitali classificati "ordinari" sono erogati tramite infrastrutture digitali per le pubbliche amministrazioni ovvero infrastrutture dei servizi cloud per le pubbliche amministrazioni accreditate AI1, AI2, AI3 o AI4; quelli "critici" tramite infrastrutture accreditate AI2, AI3 o AI4; mentre quelli "strategici" sono erogati tramite infrastrutture accreditate AI3 o AI4 (art. 12, co. 3). Le modalità e i termini per l'adeguamento delle infrastrutture digitali per le pubbliche amministrazioni sono disciplinati nell'articolo 13, mentre l'art. 14 del Regolamento definisce le modalità di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni.

Anche i servizi cloud per le pubbliche amministrazioni erogati da un soggetto pubblico, da società in house, ovvero, per espressa previsione normativa, da società a controllo pubblico, sono suddivisi in 4 livelli AC1, AC2, AC3, AC4, dettagliati in apposita sezione dell'allegato 4. I requisiti di ciascun livello, analogamente a quanto avviene per le infrastrutture, sono elaborati tenuto conto di diversi aspetti: fattori di rischio ed evoluzione della minaccia cibernetica; normativa e standard nazionali, europei e internazionali; schemi di certificazione nazionali ed europei progressivamente adottati; migliori pratiche e linee guida di settore. Con la stessa logica delle infrastrutture, anche per i servizi cloud, il Regolamento ha stabilito che i dati e i servizi digitali classificati "ordinari" possono essere erogati tramite servizi cloud di livello AC1, AC2, AC3 e AC4, quelli "critici" possono essere erogati tramite servizi cloud di livello AC2, AC3, AC4, mentre quelli "strategici" possono essere erogati solo tramite servizi cloud di livello AC3 e AC4 (art. 15, co. 5[41]).

Se i soggetti che erogano i servizi cloud sono differenti da quelli sopra menzionati, ossia soggetto pubblico, società in house, società a controllo pubblico, ma si tratta di fornitori privati, allora il Regolamento stabilisce 4 livelli di qualificazione (non di adeguamento), cloud di livello 1 (QC1), cloud di livello 2 (QC2), cloud di livello 3 (QC3), cloud di livello 4 (QC4), anche essi descritti nell'allegato 4. Con la stessa logica sopra

41. Si osserva che il comma 5 dell'art. 15 rinvia al comma 1, mentre invece il rinvio è da intendersi al comma 2 dello stesso articolo che disciplina i diversi livelli di adeguamento per i servizi cloud.

richiamata, il Regolamento dispone che i dati e i servizi digitali classificati "ordinari" possono essere erogati tramite servizi cloud accreditati QC1, QC2, QC3, QC4; quelli classificati "critici" possono essere erogati tramite servizi cloud accreditati QC2, QC3, QC4; mentre quelli "strategici" possono essere erogati tramite servizi cloud accreditati QC3 e QC4 (art. 17 del Regolamento cloud ACN). Il possesso della qualifica è sempre sottoposto a monitoraggio da parte dell'ACN, perché sulla base dell'aderenza o meno ai requisiti indicati nell'allegato 4 si gioca la sicurezza dei dati e dei servizi delle PA, che impatta la sicurezza nazionale. Le PA interessate potranno consultare il *Catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni*[42], che contiene l'elenco delle infrastrutture digitali, delle infrastrutture dei servizi cloud e dei servizi cloud, oltre che le relative informazioni descrittive compreso il livello di qualificazione ottenuto da ciascun fornitore per ognuno dei servizi cloud erogati.

9. Conclusioni

La scelta del Governo italiano di dare priorità all'innovazione della pubblica amministrazione per la ripresa e la resilienza del Paese deriva dalle raccomandazioni delle istituzioni europee, che hanno individuato proprio nella digitalizzazione dei servizi pubblici la chiave di volta per la crescita economica dell'Italia[43]. Tali raccomandazioni hanno caratterizzato il nostro Piano nazionale di ripresa e resilienza che punta anzitutto allo sviluppo digitale dei servizi pubblici. Confrontando le scelte italiane con quelle operate, ad esempio, dal Governo francese per la definizione del proprio PNRR, emerge come la digitalizzazione e la cybersicurezza in Francia – pur rappresentando uno dei pilastri insieme alla transizione ecologica sui quali orientare gli investimenti e le riforme – non risultano misure altrettanto prioritarie. Il PNRR italiano affronta la digitalizzazione e la cybersicurezza dei servizi pubblici nella prima componente della prima misura (p. 86 ss.) con un'allocazione iniziale complessiva di 9,75 miliardi di euro, pari a poco più del 5% delle risorse complessivamente stanziate. La versione del 2021 del PNRR (*Plan national de relance et de résilience*) francese, invece, tratta la digitalizzazione dei servizi pubblici solo nella componente 7 (p. 330 ss.) – terz'ultima delle 9 componenti in cui è articolato il PNRR – destinandovi complessivamente poco più di un miliardo di euro, pari a circa il 2,6% della stima iniziale del piano francese. Proporzionalmente ai finanziamenti originariamente stanziati per la realizzazione del PNRR dei due Paesi, pur nell'approssimazione del confronto qui suggerito, risulta che l'Italia dedica alla digitalizzazione della PA quasi il doppio delle risorse rispetto ai vicini cugini d'oltralpe.

Il nuovo scenario apertosi con il PNRR insieme al mutamento geopolitico hanno prodotto in capo alle amministrazioni pubbliche un aumento degli adempimenti di cybersicurezza, adempimenti destinati a crescere ulteriormente con l'imminente recepimento della direttiva NIS 2. Un carico enorme per le amministrazioni, come ad esempio quelle comunali. Al punto tale che l'Associazione Nazionale Comuni Italiani (ANCI), con riferimento al recente provvedimento in materia di cybersicurezza, l. n. 90/2024, ritiene che «pur in presenza di casi virtuosi di singole amministrazioni comunali capaci di difendersi e rispondere agli attacchi in maniera efficace, per gli enti locali» permanga «una generalizzata difficoltà ad attrezzarsi adeguatamente». Secondo ANCI fra i principali motivi ostativi all'adozione di adeguate misure di sicurezza vi sono la «carenza di risorse umane dipendenti con competenze tecniche adeguate, unita alla difficoltà a reperirne sul mercato di così specialistiche, anche a causa della bassa appetibilità, in termini retributivi, delle posizioni di lavoro all'interno dei Comuni», oltre che la «ristrettezza di risorse di

42. Curato dall'ACN e reso disponibile sul suo sito.

43. Raccomandazione del Consiglio del 20 luglio 2020 sul Programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2020 dell'Italia (2020/C 282/12), GUUE 26 agosto 2020, *Migliorare l'efficienza del sistema giudiziario e il funzionamento della pubblica amministrazione* (punto 4) e Raccomandazione del Consiglio del 9 luglio 2019 sul programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2019 dell'Italia (2019/C 301/12), GUUE 5 settembre 2019, *Migliorare l'efficienza della pubblica amministrazione, in particolare investendo nelle competenze dei dipendenti pubblici, accelerando la digitalizzazione e aumentando l'efficienza e la qualità dei servizi pubblici locali* (punto 3).

bilancio da dedicare a interventi organizzativi e sui sistemi informativi», problemi «irrisolti, a meno dell'adozione di misure di supporto successive o in fase di decretazione attuativa»[44].

Se da un lato digitalizzazione, innovazione e sicurezza della PA costituiscono sempre più la forza propulsiva della crescita economica del Paese, d'altro canto appaiono persistere diversi vincoli alla loro concreta diffusione. Ciò nonostante, se guardiamo la pubblica amministrazione italiana con gli occhi degli anni passati, bisogna riconoscere che molti passi in avanti sono stati realizzati, come confermano i progressi dell'Italia, misurati dall'Europa (da ultimo *Digital Decade Country Report 2024: Italy*). Ad esempio l'istituzione dell'ACN. Sin da quando l'amministrazione pubblica ha avviato a partire dagli anni Ottanta la sua informatizzazione, è stata evidente la necessità di difenderla anche nella sua dimensione digitale. Benché siano state diverse le iniziative legislative e organizzative intraprese nel corso degli anni in materia di sicurezza cibernetica delle PA, era stato osservato come la loro parcellizzazione e il mancato coordinamento rendevano «assolutamente indispensabile» l'istituzione di «una unica autorità nazionale, investita del compito di provvedere in tema di sicurezza dei sistemi informativi pubblici»[45]. Dal 2021 le funzioni di protezione cyber delle PA italiane e, in generale, del Paese, sono state finalmente affidate a un unico punto di riferimento in materia, l'Agenzia per la cybersicurezza nazionale, scelta che segna un deciso cambiamento[46]. Le recenti direttive in materia cyber si rivolgono al vertice politico delle istituzioni pubbliche, evidenziando la consapevolezza che occorre un coinvolgimento di alto livello per l'efficacia dell'azione di contrasto alla cybercriminalità. Come osservato, infatti, i «processi di digitalizzazione, per loro natura, necessitano di una regia unitaria, poiché devono svilupparsi in modo uniforme e l'ordinamento nazionale ed europeo si conformano a questa dinamica, anche per garantire un quadro chiaro e immediato nelle interrelazioni, che hanno carattere tecnico e politico assieme»[47]. Anche perché la trasformazione digitale della pubblica amministrazione italiana e la sua cybersicurezza non rappresentano più soltanto una quota parte della trasformazione digitale del Paese, ma costituiscono il mezzo attraverso il quale si innesca il motore dell'innovazione dell'intero Paese[48].

L'attuazione delle politiche in materia di cybersicurezza delle PA, però, richiede ulteriori sforzi. Anzitutto occorre armonizzare la disciplina, che nel suo continuo mutare crea una tale incertezza da diventare potenzialmente il principale alibi alla sua disapplicazione. Mutamenti che sarebbe scorretto attribuire *tout court* alla velocità dell'evoluzione tecnologica, visto che la regolamentazione del dettaglio attuativo è opportunamente affidata alla normativa tecnica secondaria. In secondo luogo è necessario intensificare i piani formativi sulla cybersicurezza diretti specialmente alla dirigenza pubblica, doverosamente tenuta a incrementare le proprie conoscenze nel suo ruolo di cinghia di trasmissione fra le indicazioni politiche e l'azione amministrativa. Occorre poi adottare misure innovative per attrarre talenti in grado di realizzare i cambiamenti organizzativi e tecnologici attesi. La "bassa appetibilità, in termini retributivi", d'altra parte, non costituisce di per sé l'unico ostacolo, come mostrano gli studi in materia: servono, altresì, un ambiente stimolante e l'orgoglio di lavorare per il Paese, rappresentato da una classe manageriale illuminata e preparata, che l'immaginario collettivo non ancora attribuisce pienamente alle PA italiane.

Riferimenti bibliografici

44. ANCI 2024, pp. 1-2.
45. Cfr. Sarzana di S. Ippolito 2010, p. 315 ss.
46. Cfr. Viola–De Biase 2023, pp. 115-121.
47. Cfr. Calzolaio 2024, p. 103.
48. Cfr. AGID 2023, «Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito Piano triennale) è uno strumento fondamentale per promuovere la trasformazione digitale del Paese attraverso quella della Pubblica Amministrazione italiana», p. 7. In tal senso la trasformazione digitale della PA diventa il mezzo attraverso il quale raggiungere la trasformazione digitale del Paese.

ACN (2023), *Relazione annuale al Parlamento 2023*, 2023

ACN (2022), *Strategia nazionale di cybersicurezza 2022-2026*

AGID (2023), *Piano triennale per l'informatica nella Pubblica Amministrazione (2024-2026)*, dicembre 2023

ANCI (2024), *Nota di lettura Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" pubblicata nella Gazzetta Ufficiale SG n. 153 del 2 luglio 2024*, 2024

S. Calzolaio (2024), Autorità indipendenti e di governo della società digitale, in F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024

CIS-Sapienza, CINI Cybersecurity National Lab (2019), *Framework Nazionale per la Cybersecurity e la Data Protection*, febbraio 2019

Dipartimento per la Trasformazione Digitale, Agenzia per la Cybersicurezza Nazionale (2021), *Strategia Cloud Italia Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA,* 2021

Istituto nazionale di statistica (2023), *Elenco delle amministrazioni pubbliche inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica)*, settembre 2023

E. Longo (2024), *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717). Camera dei Deputati, Commissioni riunite I e II - Roma, 28 marzo 2024*, in "Rivista italiana di informatica e diritto", 2024, n. 1

C. Sarzana di S. Ippolito (2010), *Informatica, internet e diritto penale*, Giuffrè, 2010

R. Viola, L. De Biase (2023), *Il codice del futuro. La carta europea dei diritti digitali e il senso dell'innovazione*, in "Il Sole 24Ore", 24 maggio 2023