

Cybersecurity: il necessario rafforzamento delle competenze informatiche degli Enti locali. Un focus sui servizi a supporto prestati dalle società in house in materia di sicurezza, attraverso lo studio di casi concreti

***Cybersecurity: the necessary
strengthening of local government
IT skills. A focus on the support
services provided by in-house
security firms, through case studies***

Valentina Rustichini*

** Comune di Barberino Tavarnelle*

Abstract

This study aims to investigate the choice by local authorities of the in-house providing institute for the performance of the cybersecurity service, through an examination of national legislation, case law and the study of some cases of institutions that have opted for this choice. In particular, the objective of this paper is to investigate the reasons why local administrations entrust cyber activities to their in-house companies as opposed to free market ones. Can in-house companies constitute a concrete solution for local authorities concerning cybersecurity? Can in-house companies guarantee the application of Cloud-first principle?

Keywords: *Cybersecurity, In house providing, Cyber-attack, Nrrp, Cloud first principle.*

Introduzione

La cybersecurity è una questione di primaria importanza per la Pa, in quanto la vulnerabilità dei sistemi informatici espone gli enti pubblici a rischi. La sicurezza informatica è strettamente connessa pure alla qualità delle infrastrutture degli enti, che offrono costantemente servizi digitali. Anche le amministrazioni locali hanno l'obbligo di dotarsi di una struttura interna che sia responsabile per la definizione di strategie di gestione del rischio informatico e la realizzazione di piani di azione e monitoraggio dei possibili rischi. Proprio per la cybersecurity si è manifestato un utilizzo prevalente da parte degli Enti locali dell'istituto dell'in house providing, ovvero l'affidamento ad un ente strumentale, formalmente autonomo ma funzionalmente, organizzativamente e finanziariamente dipendente dall'amministrazione (Lucca 2019).

In questo scritto si intende esaminare la scelta da parte degli Enti locali dell'istituto dell'in house providing per lo svolgimento del servizio di cybersecurity, attraverso una disamina della normativa nazionale, della giurisprudenza e lo studio di alcuni casi concreti di enti che hanno optato per tale scelta. L'obiettivo è quello di indagare quali siano le ragioni che spingono le amministrazioni locali ad affidare l'attività cyber alle proprie in house od in alternativa alle società del libero mercato.

Nel dettaglio lo studio espone al paragrafo 1 le diverse qualificazioni dell'attività di cybersecurity fornite dalla disciplina nazionale, rispondendo alla domanda se tale attività è considerata come un servizio pubblico o un'attività strumentale.

Nel paragrafo 2 si esaminano le caratteristiche intrinseche dell'attività e del suo mercato, mentre nel paragrafo 3 le peculiarità degli Enti locali ed i loro problemi legati all'approvvigionamento del servizio cyber. Invece, nel paragrafo 4 si analizzano le motivazioni addotte dagli Enti locali circa l'affidamento del servizio in house providing o alle società del libero mercato, soffermandosi anche sul ricorso alle società miste. Si procede successivamente nel paragrafo 5 ad esaminare alcuni casi di affidamenti a società in house e le

pronunce giurisprudenziali in merito. Nell'ultimo paragrafo sono riportate le conclusioni, ovvero sul perché non sia sempre opportuno demonizzare l'istituto dell'in house providing per le attività relative alla cybersicurezza.

1. La qualificazione dell'attività di cybersecurity ("servizio pubblico" o "attività strumentale") e la disciplina applicabile

In merito alla qualificazione dell'attività di cybersecurity, si assiste ad una differenziazione della disciplina in base all'attività che l'ente intende affidare alla propria in house. Il d. lgs. n. 36/2023, quale nuovo Codice dei Contratti pubblici, prevede due livelli di complessità della motivazione a seconda dell'oggetto del contratto, ovvero per i servizi pubblici locali di rilevanza economica (c.d. "servizi all'utenza") e per le prestazioni strumentali alla Pa. Per i primi, come ad esempio la gestione dei procedimenti amministrativi o di fondi pubblici, è necessario dar conto ed evidenziare i vantaggi per la collettività da un punto di vista qualitativo, dell'universalità del servizio, di risparmio di tempo e del razionale impiego delle risorse. Mentre, come analizzato da Mattarella (2023), per i servizi strumentali, l'ente partecipante deve fornire una motivazione più snella, indicando i vantaggi dell'affidamento in termini di economicità, di celerità o di perseguimento di interessi strategici. Il confine tra i diversi ambiti di applicazione dei diversi regimi non è così chiaro, in quanto la normativa non indica quali siano le prestazioni strumentali e tale "lacuna" può determinare incertezze e contenziosi in materia. La giurisprudenza¹ interviene a soccorso di tale lacuna, in quanto identifica i servizi strumentali come quei servizi svolti in favore della Pa e dell'utenza diffusa, al contrario dei servizi pubblici locali che mirano direttamente a soddisfare bisogni o esigenze della collettività. Il Tar Lombardia² ha ancor meglio definito la distinzione tra le due categorie, affermando che essa va ricercata nel beneficiario diretto del servizio: ricorre l'ipotesi del servizio pubblico se la prestazione resa dall'appaltatore viene fornita per soddisfare in via immediata e diretta le esigenze dell'utente/collettività; costituisce, al contrario, servizio strumentale quello le cui prestazioni vengono svolte in favore della stazione appaltante.

Partendo dal presupposto che l'attività di sicurezza dei dati, come quella inerente le banche dati, sono funzioni "nuove", ovvero non riconducibili integralmente né ad un'attività puramente amministrativa né ad un'attività strumentale rispetto alle funzioni core dell'amministrazione, sulla base delle pronunce del giudice amministrativo sopra esposte, si può definire la cybersecurity come un'attività strumentale alla compiuta realizzazione di un sistema It di una pubblica amministrazione.

-
1. Nelle sentenze del Consiglio di Stato si indicano quali servizi strumentali, tutti quei servizi erogati da società ed enti a supporto di funzioni amministrative di natura pubblicistica di cui resta titolare l'ente di riferimento e con i quali lo stesso ente provvede al perseguimento dei propri fini istituzionali, *ex multis*, sezione V, 12 giugno 2009, n. 3766.
 2. Tar Lombardia, Sez. di Brescia, 27 dicembre 2007, n. 1373.

Su tale definizione è intervenuto anche il d. lgs. n. 201 del 23 dicembre 2022, quale Testo unico che riordina la disciplina dei servizi pubblici locali di rilevanza economica, che definisce strumentali i servizi che non realizzano in via immediata un bisogno sociale, ma si limitano a fornire ad un settore dell'amministrazione un dato servizio che, solo in via mediata, è funzionale alla realizzazione dell'utilità collettiva, come ad esempio: la manutenzione degli edifici, del verde, delle strade; i servizi ausiliari e di supporto; la riscossione entrate etc. (Macheda 2024). Anche tale definizione sembra avallare l'ipotesi che il servizio di cybersicurezza sia un'attività strumentale per un ente e pertanto l'amministrazione, che affidi in house providing il servizio di sicurezza informatica, possa beneficiare di un alleggerimento nell'obbligo di motivazione.

In merito a tale obbligo il d. lgs. n. 50/2016, quale vecchio Codice dei Contratti, imponeva un forte onere di motivazione a carico delle amministrazioni, per il quale doveva trasparire chiaramente che l'ente aveva valutato la congruità economica dell'offerta della società in house ed altresì motivare le ragioni del mancato ricorso al mercato e "dare conto dei vantaggi della collettività (...) della congruità economica della prestazione". Un onere di motivazione più gravoso rispetto a quello del Codice dei Contratti del 2016 è richiesto dal d. lgs. n. 201/2022. Secondo il dettato del decreto del 2022 l'ente, che decide di affidare un servizio ad una società in house, deve motivare obbligatoriamente tale scelta. L'ente dovrà dare conto non solo delle ragioni del mancato ricorso al mercato, come indicato dal Codice del 2016, ma altresì dei costi per gli utenti e dell'impatto sulla finanza pubblica ed indicare "i risultati conseguiti in eventuali pregresse gestioni in house". Tali indicazioni hanno l'evidente finalità di rendere più difficile per un ente la scelta dell'affidamento in house providing.

2. Le caratteristiche intrinseche dell'attività di cybersecurity e del suo mercato

Ma cosa si intende per cybersecurity? Posto che il termine ha una natura multidisciplinare e non si ha una definizione unica e condivisa, si può intendere come quel complesso delle misure di protezione di tutte le risorse informatiche di cui si dota un'organizzazione atte a prevenire minacce di natura fisica (es. furti, calamità naturali) o digitale (es. attacchi informatici, perdita accidentale o intenzionale di informazioni). Esplicativo è un episodio accaduto nel dicembre 2023: il gruppo hacker russo Lockbit ha attaccato indirettamente le pubbliche amministrazioni tramite i server di Westpole. La casa di sviluppo del server citato, infatti, fornisce alla società Pa Digitale SpA l'infrastruttura cloud con cui eroga i servizi, che includono i sistemi di rendicontazione di buste paga e di fatturazione elettronica. Le amministrazioni pubbliche servite sono 1.300, con circa 500 comuni, alcune province ed enti, tra cui l'Agenzia per l'Italia digitale (Agid) e l'Autorità Nazionale Anticorruzione (Anac). Tale attacco ha determinato l'impossibilità per diverse pubbliche amministrazioni, di produrre gli stipendi per i propri dipendenti e la conseguente inaccessibilità ai relativi dati.

La cybersecurity consiste nel proteggere i dati e le informazioni nel cyberspazio ed è un sottoinsieme dell'It (Information Technology) e dell'Ict (Information & Communication Technology), in quanto i cyber attacchi indirizzati ai sistemi informatici avvengono all'interno del medesimo dominio. La cybersecurity ha la finalità quindi di garantire riservatezza, integrità, e disponibilità dell'informazione principalmente nel cyberspazio, che si determina come la fonte, lo strumento, il bersaglio e il luogo del crimine informatico. Quindi una società, che fornisce un sistema cloud, dovrà necessariamente aver implementato delle misure di protezione del medesimo e dei dati ivi compresi.

Perseguire una solida postura di cybersicurezza significa anche assicurare la continuità dei servizi essenziali, ovvero implementare misure preventive per evitare attacchi informatici, mitigare i rischi e proteggere le risorse digitali per garantire la sicurezza e l'efficienza di ogni organizzazione. A tal fine il Dipartimento per la trasformazione digitale (Dtd) e l'Agenzia per la cybersicurezza nazionale (Acn) promuovono l'adozione dell'approccio "cloud first" da parte delle pubbliche amministrazioni. Tale principio si inserisce nella Strategia cloud Italia, elaborata dal Dtd e l'Acn, che contiene gli indirizzi strategici per il percorso di migrazione verso il cloud di dati e servizi digitali della pubblica amministrazione. In coerenza con gli obiettivi del Pnrr, la strategia individua un percorso definito per accompagnare circa il 75% delle Pa italiane nella migrazione dei dati e degli applicativi informatici verso un ambiente cloud. La Strategia cloud Italia si pone come metodologia implementativa del principio del "cloud first", quale pilastro del progetto di digitalizzazione della Pa stabilito dal Pnrr. Le Pa sono tenute ad operare secondo tale principio al momento dell'adozione di nuovi progetti o aggiornamenti in materia di cybersecurity e pertanto considerare ed adottare in modo prioritario servizi e soluzioni basate su cloud (SaaS, PaaS, IaaS). Tali indicazioni hanno lo scopo di guidare le amministrazioni verso una maggiore sicurezza (es. rispondendo in maniera organizzata agli attacchi informatici), agilità e costi ridotti. L'obiettivo è quello di fare in modo che tutti i servizi erogati dalle Pa siano basati su applicazioni "cloud native", sviluppate cioè nativamente sulla base dei paradigmi cloud. L'importanza della Strategia cloud Italia è anche quella di regolare l'attività dei provider privati, promuovendo l'adozione di standard di qualità e sicurezza adeguati.

Le amministrazioni locali devono valutare la pluralità di aspetti che implica la cybersecurity, ed allo scopo di adeguarsi alla normativa di settore ed alle best practices, le prime potranno scegliere i propri fornitori all'interno di un vasto mercato. Questo ultimo è composto da una moltitudine di operatori di settore ed anche le società in house delle amministrazioni locali. Il settore è frammentato e fortemente competitivo ed i fornitori devono avere il medesimo fine, ovvero quello di consentire ai propri clienti di prevenire rischi cyber, anche formandone il personale e, in caso negativo, di ovviare alle conseguenze.

Considerato che, da un'analisi dei servizi offerti dai fornitori del settore elencati nei rispettivi siti web, traspare che le attività garantite siano le medesime (es. antivirus, User Identity,

monitoraggio degli incidenti di sicurezza), è possibile dedurre che la scelta dell'amministrazione risenta in primo luogo delle proprie capacità economiche ed in secondo luogo del grado di "affidabilità" dei fornitori. È pur vero che vi sono anche Enti locali che, seppur di limitate dimensioni e budget, hanno affidato il servizio cloud e di cybersicurezza ad un operatore primario del settore, come ad esempio l'Unione Comunale del Chianti Fiorentino che ha affidato i servizi alla società Maggioli SpA.

Come sarò esposto nei paragrafi successivi, in merito al criterio del "livello di affidabilità" dei fornitori gli enti hanno optato in base alle esperienze avute: alcune amministrazioni hanno scelto delle società esterne già in precedenza loro partner tecnologici, dimostrando che le medesime hanno "necessari requisiti di comprovata esperienza nel settore e di affidabilità". Per le società in house coinvolte nel settore cyber, si riscontra la seguente panoramica: alcune contano circa 200 dipendenti, come Informatica Alto Adige SpA e Trentino Digitale SpA, mentre altre hanno un numero inferiore di dipendenti, come Pasubio Tecnologia Srl con 35 dipendenti. Il numero degli occupati non è però proporzionale al numero degli enti partecipanti: ad esempio, l'in house Pasubio Tecnologia conta ben 41 amministrazioni partecipanti di varie dimensioni e fornisce ad alcune di queste i servizi cloud con i relativi sistemi di protezione. Mentre il numero degli enti partecipanti influisce sul fatturato delle società in house: nel 2022, Trentino Digitale ha registrato un fatturato di € 56.399.798,00 avendo nella compagine sociale 168 comuni (oltre ad altri enti).

Spesso le offerte presentate dalle società in house sono più competitive rispetto a quelle delle società del libero mercato e pertanto comportano una spesa inferiore per l'ente locale. Al fine del raggiungimento del miglior risultato le Pa locali devono considerare non solo la garanzia della qualità del servizio, ma anche l'ottimale impiego delle risorse pubbliche.

3. La peculiarità degli Enti locali ed i problemi legati all'approvvigionamento dei servizi di cybersecurity

I rischi cyber si riscontrano non solo nelle grandi amministrazioni, ma anche a livello locale. Per prevenire e/o rimediare ai rischi cyber gli Enti locali sono tenuti ad investire in tecnologie appropriate ed hanno due strade percorribili: affidare ad operatori esterni i servizi connessi; trovare al proprio interno personale specializzato. La prima soluzione è quella preferita dagli enti, in considerazione della complessità della materia e della carenza di personale qualificato all'interno delle amministrazioni locali.

La scelta degli Enti locali della tipologia del fornitore a cui affidare il servizio cyber, risente necessariamente del proprio budget di spesa, che può essere limitato per i piccoli enti. La criticità legata all'aspetto finanziario pesa sulla scelta del fornitore. Proprio per tale motivo i primi optano per un affidamento a società in house, in quanto l'offerta di

queste ultime è spesso più concorrenziale rispetto a quella di società esterne. Per l'aspetto economico gli enti hanno potuto far affidamento sui fondi del Pnrr, facendo così fronte ai necessari investimenti, indispensabili per potenziare la resilienza cyber del territorio e garantire l'evoluzione continua delle difese.

Al fine di valutare in modo compiuto tutti gli interessi coinvolti ed approfondire le rispettive interazioni, alcune amministrazioni locali hanno adottato il seguente *modus operandi*, ovvero gli enti effettuano uno (o più) studio di fattibilità tecnico-economico e giuridico, finalizzato a verificare la decisione di optare per una soluzione di housing rispetto all'alternativa dell'affidamento a società esterne. Per garantire la trasparenza dell'attività amministrativa: la valutazione dovrebbe tener conto dei costi e dei tempi di realizzazione delle attività cyber; tali studi dovrebbero essere resi pubblici, al fine di dimostrare che l'ente abbia operato una reale comparazione di tutti gli interessi pubblici e privati coinvolti. Questo iter è stato seguito dall'Unione delle Terre d'Argine, che per il progetto di investimento Pnrr 1.2 "Abilitazione al cloud per le Pa locali - comuni (Aprile 2022)" ha affidato il servizio cloud (compreso i servizi di disaster recovery e business continuity) alla società partecipata Lepida. L'Unione ha pubblicato gli studi giuridici e tecnici condotti nei siti web degli enti partecipanti all'Unione, motivando la scelta di optare per la propria società in house (Cristoforetti, 2024).

Le in house sono espressione del principio di autonomia organizzativa delle amministrazioni aggiudicatrici e controllanti aventi il diritto di autoprodurre beni e servizi, e, se le prime hanno competenze in ambito It, possono costituire una risorsa per gli Enti locali che cercano, a volte faticosamente, di trovare soluzioni per prevenire il rischio cyber. Anche le società in house devono però ottimizzare al meglio la propria offerta, rendendola adeguata agli Enti locali, integrando specifiche tecniche che consentano di prevenire e/o facilitare un'eventuale soluzione in caso di attacco cyber. In questo modo, relativamente all'ambito digitale, anche gli enti più piccoli, con meno risorse economiche e personale ridotto, possono offrire ai propri cittadini ed alle loro imprese servizi online aggiornati, completi e sicuri, superando eventuali disparità con altre realtà più grandi e riducendo la complessità.

Per quanto riguarda le modalità di approvvigionamento degli Enti locali dei servizi cyber, questi possono impiegare le seguenti soluzioni: affidamento diretto alle proprie in house o a società del libero mercato; effettuare una gara pubblica a cui invitare entrambe le tipologie di fornitori; aderire alle convenzioni offerte dalla Centrale di acquisto nazionale delle Pa (Consip) in materia cyber. Gli Enti locali possono aderire all'accordo quadro pubblicato da Consip, avente ad oggetto i "Servizi di sicurezza da remoto" ed i "Servizi di compliance e controllo". L'accordo prevede 5 fornitori per le Pa locali e 4 fornitori per le Pa centrali. Le amministrazioni possono scegliere i prodotti cyber di differenti produttori indicati nell'accordo, mediante un affidamento di servizi e forniture tramite ordine diretto.

4. Le scelte dei Comuni: l'affidamento in house, il ricorso al mercato e le società miste

In materia di cybersecurity si assiste da parte degli Enti locali ad un crescente utilizzo dell'istituto dell'in house providing. Tale modello si contrappone a quello dell'outsourcing o contracting out (c.d. esternalizzazione), in cui la sfera pubblica si rivolge al privato, demandandogli il compito di produrre e /o fornire i beni e servizi necessari allo svolgimento della funzione amministrativa.

La dottrina ha spesso definito l'in house providing come sinonimo di "affidamento diretto", operato al di fuori di procedure comparative di evidenza pubblica e prescindendo dal rispetto di particolari oneri di pubblicità o trasparenza, comportando solo l'esistenza dell'onere di motivare compiutamente in ordine alla sussistenza dei requisiti legittimanti tale tipo di affidamento. Si tratta pertanto di una scelta organizzativa di autoproduzione del bene o del servizio che è alternativa al mercato. Le società in house si caratterizzano per uno specifico legame con le amministrazioni partecipanti, ed in particolare per essere soggette a un controllo degli enti analogo a quelli che essi esercitano sulle proprie attività (requisito del "controllo analogo").

Ma quali sono le motivazioni addotte dagli enti e come queste sono valutate dalla giurisprudenza. Un caso esplicativo è quello del Comune di Bastia Umbra e della società in house PuntoZero Scarl, a totale capitale pubblico, quale "ente strategico regionale" che si occupa per gli enti soci di una pluralità di servizi Ict. Come si evince dalla determina n. 964 del 2023, il Comune di Bastia Umbra ha affidato a PuntoZero il servizio di datacenter e dei relativi sistemi di sicurezza, mediante una richiesta di proposta tecnico-economica, alla quale l'in house ha risposto, confermando di poter assumere tali attività, in continuità con quanto già in essere in base alla convenzione vigente a condizioni economiche aggiornate, ma comunque congrue in rapporto alla tipologia di servizi. Nella determina del 2023 il Comune affidatario ha motivato la propria scelta, esplicitando che la soluzione proposta da PuntoZero consente: "la gestione unitaria dei sistemi primari degli enti umbri (...) perseguendo maggiori livelli di efficienza e celerità di intervento" e che tale soluzione "realizza un ottimale impiego delle risorse pubbliche con benefici per la collettività anche in termini di qualità dei servizi resi, perseguendo obiettivi di efficacia, efficienza ed economicità nell'ambito della Strategia Cloud della Regione Umbria". La motivazione adottata dal Comune di Bastia Umbra rispecchia la norma di cui all'art. 7 c.2 del d. lgs. n. 36/2023, assumendo implicitamente che il servizio di cybersecurity sia un'attività strumentale.

Non tutti gli enti scelgono le proprie in house per il servizio di cybersecurity, ma optano per affidare il servizio alle società del libero mercato. Questa strada è stata percorsa, ad esempio, dal Comune di Vicenza, il quale ha affidato ad una società esterna il servizio di vulnerability assessment, penetration test e di attività specialistica di affiancamento e

formazione in tema di cybersecurity³. La medesima strada è stata percorsa dal Comune di Barberino Tavarnelle e dal Comune di Bientina, che hanno affidato il servizio cloud e di cybersicurezza a società esterne, già in precedenza partner tecnologici e che presentano “necessari requisiti di comprovata esperienza nel settore e di affidabilità avendo sempre soddisfatto le esigenze dell’ente in maniera tempestiva ed allineando i costi di gestione in maniera congrua anche in considerazione dei continui necessari aggiornamenti ed implementazioni”. Quello che preme sottolineare è la modalità di espletamento della gara, in quanto gli enti appaltanti hanno optato per una trattativa diretta sul mercato elettronico MePa mediante una richiesta di offerta, senza la consultazione di più operatori economici. In maniera simile gli enti partecipanti alla società in house SILFI, che hanno affidato alla medesima i progetti Pnrr, pubblicando una gara sul Sistema telematico acquisti regionale della Toscana. Questa ultima modalità di gara sembra essere in contrasto con l’orientamento della dottrina, secondo il quale “gli affidamenti in house (...) comprimono la concorrenza”.⁴ Dopo aver acquisito l’offerta tecnica ed economica presentata dalla società in house e valutato la congruità economica, gli enti partecipanti hanno sottoscritto con SILFI un contratto di servizio, dove è riportata la tariffa del servizio pubblico, quale corrispettivo del medesimo. In merito alla tipologia di gara si è espresso il Consiglio di Stato,⁵ affermando che: “l’affidamento mediante gara non garantisca (non, quanto meno, nella stessa misura di quello diretto) il raggiungimento degli obiettivi prefissati”.

Inoltre, le amministrazioni possono affidare i servizi a “società a capitale misto pubblico privato” (“società miste”), nelle quali il socio privato viene scelto attraverso l’espletamento di gare con procedure ad evidenza pubblica e secondo il modello della gara unica a doppio oggetto. La selezione del socio privato avviene, pertanto, attraverso una procedura di gara ad evidenza pubblica, assimilata all’appalto / concorso che si caratterizza, rispetto alle altre procedure, per il fatto che la prestazione richiesta dall’amministrazione appaltante (affidente ad elevate conoscenze specialistiche) non viene determinata a priori in ogni sua parte, in quanto le ditte vengono chiamate a fornire il progetto dell’opera che l’ente intende realizzare.

Tra le società Ict pubbliche a capitale misto si potevano annoverare: per la Regione Molise la Molise Dati SpA; per la Regione Abruzzo la società Engineering ScpA; per la Regione Sicilia le società Sicilia e Innovazione SpA e Sicilia e Servizi SpA. Nel corso degli anni 2016 e 2017 tali società hanno ristrutturato la propria organizzazione e sono diventate

3. Determina n. 2680 del 19/12/2018.

4. *“Gli affidamenti in house non convincono appieno ma comprimono la concorrenza, creano disparità, discriminazioni e forse minano le libertà sulle quali si è costruito l’Europa: un grande mercato unico nel quale la sussidiarietà permette l’autonomia ad ogni livello di governo sociale e civile, nel quale tutti gli attori dovrebbero assicurare servizi pubblici di qualità e a prezzi contenuti, nel quale i monopoli o oligopoli non dovrebbero trovare cittadinanza alcuna”* (Lucca, 2004).

5. Cons. Stato, Sez. IV, 19 ottobre 2021, n. 7023.

a totale partecipazione pubblica con l'ente di riferimento come socio e amministratore unico. Ad oggi, dall'esame condotto non risultano affidamenti di servizi di cybersecurity a società miste.

5. Casi concreti di affidamenti in house e orientamenti giurisprudenziali

In Italia è in fase di consolidamento la realtà delle società in house che offrono servizi di cybersecurity alle amministrazioni locali partecipanti. Alcuni esempi sono la società SILFI Firenze Smart SpA⁶ (qui di seguito "Firenze Smart" o "SILFI"), la società Lepida ScpA e la società InnovaPuglia quali società in house partecipate interamente da Enti locali che, con riferimento alle attività Ict, svolgono attività di natura strumentale alle attività istituzionali degli enti partecipanti.

La società SILFI offre i seguenti servizi Ict: contact center quale centro unico di contatto multicanale (i.e. telefono, live-web chat); manutenzione dei siti web ufficiali; servizi online per i comuni. Tali servizi costituiscono delle soluzioni digitali per gli Enti locali, ma devono essere particolarmente attenzionati per i rischi cyber. In merito ai servizi online offerti, Firenze Smart gestisce e rende fruibili ai cittadini 229 servizi online sui portali dei comuni dell'Area metropolitana (i.e. anagrafe e stato civile, pagamento tributi, servizi scolastici, ambiente e territorio sono solo alcuni degli ambiti e dei servizi forniti online ogni giorno). Per tali attività SILFI si occupa della realizzazione e manutenzione dei sistemi informatici, contribuendo così all'organizzazione, allineamento e sicurezza delle soluzioni sviluppate. La gestione avviene attraverso la struttura hardware e software del Centro servizi territoriale attualmente ospitato presso il datacenter di Regione Toscana. SILFI effettua anche la manutenzione ordinaria dell'intero parco impiantistico delle telecamere per la sorveglianza; tale settore è strettamente legato alla cybersicurezza soprattutto per la tutela della privacy. Anche la società in house Lepida ScpA⁷ offre ai propri enti partecipati attività simili a quelle offerte da SILFI, ovvero: formazione e supporto tecnico nell'ambito dell'Ict; servizi di datacenter con funzioni di data storage, backup, disaster recovery; fornitura di tratte di rete e di servizi ad enti pubblici locali e statali, alle forze dell'ordine, per la realizzazione di infrastrutture per il collegamento delle loro sedi nel territorio della Regione Emilia-Romagna. InnovaPuglia SpA⁸ è la società in house della Regione Puglia, che gestisce il datacenter e tutti i servizi infotelematici regionali ed offre anche supporto tecnico alla Regione nella programmazione strategica a sostegno dell'innovazione.

6. SILFI SpA è la società in house della Città Metropolitana di Firenze.

7. Lepida ScpA è a totale capitale pubblico e partecipata da oltre 450 enti soci.

8. InnovaPuglia SpA nasce dall'unione di Tecnopolis Scrl e FinPuglia SpA.

Per tutte queste attività Ict è determinante che le società in house offrano anche una costante attenzione ed implementazione delle difese in materia di cybersicurezza, in quanto le potenziali ricadute possono essere davvero importanti. Il trend del numero di utenti che accedono ai servizi online offerti dalle in house è in costante aumento; si pensi che nell'anno 2021, a fronte dei 435 servizi online offerti da SILFI (di cui 233 di pagamento), sono stati registrati ben 1.826.109 accessi di cui 55% da mobile.

Le società partecipate citate forniscono ai propri enti partecipanti non solo i servizi Ict ma anche i servizi relativi alla cybersicurezza oggetto delle misure del Pnrr.

In merito ai progetti del Piano di resilienza, per i comuni partecipanti a Firenze Smart che hanno aderito al progetto di investimento Pnrr 1.4 “Servizi e cittadinanza digitale” Misura 1.4.4 “Estensione dell'utilizzo piattaforme nazionali di identità digitale Spid Cie – aggiudicazione servizio di erogazione”, la società in house ha fornito il piano formativo agli enti aderenti, avente come focus la sicurezza digitale connessa all'utilizzo dei servizi Spid (Sistema pubblico di identità digitale) e Cie (Carta di identità elettronica), come ad esempio il protocollo di identificazione elettronica “eID” per l'accesso ai servizi pubblici disponibili online. Per i comuni di cui sopra, che hanno aderito al progetto di investimento Pnrr 1.4 “Servizi e cittadinanza digitale” Misura 1.4.1 “Esperienza del cittadino nei servizi pubblici – Comuni (Aprile 2022)”, SILFI ha svolto servizi come la richiesta di accesso agli atti, la richiesta di pubblicazione di matrimoni, richiesta di iscrizione al trasporto scolastico, richiesta di iscrizione all'asilo nido (c.d. misura “pacchetto cittadino attivo”) e la creazione e manutenzione del sito internet (c.d. misura “pacchetto cittadino informato”).

L'Unione delle Terre d'Argine ha aderito al progetto di investimento Pnrr 1.2, affidando il servizio cloud alla società partecipata Lepida, quale fornitore già incaricato dei servizi di datacenter per conto dei comuni della suddetta Unione. Il servizio cloud erogato da Lepida è comprensivo anche dell'attività di disaster recovery e business continuity.

La Regione Puglia ha aderito a due progetti con il supporto tecnico della in house InnovaPuglia, nell'ambito del progetto di investimento Pnrr Misura 1.5 “Cybersecurity”, coinvolgendo una platea di circa 38.000 utenti regionali. Il primo progetto ha l'obiettivo di valutare lo stato della sicurezza e aumentare la protezione dei dispositivi della Regione Puglia, delle aziende sanitarie, delle agenzie e delle altre società in house regionali (i.e. proteggere i dispositivi di ciascun ente, visualizzare le attività anomale in tempo reale per intervenire e ridurre il tempo per il contenimento, aggiungere un livello di sicurezza predittiva basato sull'analisi del comportamento). Il secondo progetto è volto a verificare i livelli di consapevolezza e di vigilanza degli utenti sul rischio digitale attraverso un piano di formazione.

I casi esposti possono dimostrare quanto spesso gli Enti locali scelgono di affidare alle proprie in house i servizi di cybersecurity.

In merito alle motivazioni riportate dagli enti nelle rispettive determine, si è espressa la giurisprudenza amministrativa. Il Tar Liguria⁹ afferma che sia sufficiente per l'ente fornire una "motivazione ragionevole e plausibile delle ragioni che, nel caso concreto" hanno indotto il medesimo a scegliere il modello in house. Sembra pertanto bastare che l'amministrazione "indichi le ragioni, che potranno essere successivamente vagliate dal giudice amministrativo, della preferenza del modello scelto rispetto al ricorso al mercato, nonché dei benefici conseguibili dalla collettività attraverso tale modello". Su tale caso si è espresso anche il Consiglio di Stato¹⁰ il quale, in accordo con altri precedenti della medesima Sezione, precisa che l'onere motivazionale deve essere complesso e unitario e non si può esimere da valutazioni istruttorie, circa le verifiche che attendono al fallimento del mercato, quanto quelle che attengono ai benefici per la collettività del modulo in house. Le motivazioni degli enti che scelgono l'in house providing devono basarsi sostanzialmente su di un comune oggetto di riferimento, rappresentato dagli obiettivi di universalità e socialità, di efficienza, di economicità e di qualità del servizio, nonché di ottimale impiego delle risorse pubbliche¹¹. Tuttavia, il Consiglio di Stato ha precisato che, nella motivazione l'ente debba indicare dettagliatamente l'istruttoria che ha condotto a tale scelta. Dalla motivazione devono emergere quelle ragioni oggettive necessarie per controbilanciare la preferenza accordata dall'ordinamento per l'esternalizzazione. Quindi, anche per il servizio di cybersecurity, non è sufficiente che l'ente indichi genericamente che la scelta dell'in house providing abbia vantaggi in termini di economicità, di celerità o di perseguimento di interessi strategici, ma deve evidenziare quali sono i vantaggi riscontrati, altrimenti la sua scelta non può essere considerata attendibile.

Altresì la giurisprudenza rimarca la centralità della descrizione dell'istruttoria che l'ente deve riportare nell'atto di affidamento. Il Consiglio di Stato indica nella sentenza n. 3562 del 2022¹² che l'ente è tenuto ad indicare ad esempio: "un effettivo confronto tra i dati dell'offerta della partecipata e i dati degli operatori economici privati operanti nel medesimo territorio"; una valutazione dei "costi di gestione dei servizi" e delle "singole voci del servizio"; una comparazione dei "costi attuali sostenuti e quelli che l'ente sosterrà per l'affidamento in house"; una comparazione dei "costi praticati dall'affidataria in house con quelli medi rilevati attraverso l'osservatorio provinciale, constatandosene l'allineamento"; se "i servizi e attività aggiuntive" della società in house sono stati valutati dall'ente "in termini qualitativamente migliorativi rispetto alle pregresse gestioni". Il giudice sottolinea che, l'ente ha indicato nella motivazione che la scelta dell'affidamento

9. Tar Liguria, Sez. I, 8 ottobre 2020 n. 68.

10. Cons. Stato, Sez. III, 12 marzo 2021, n. 2102.

11. Altresì il Consiglio di Stato indica che tale attività istruttoria andrà poi valutata caso per caso "non potendo escludersi la possibilità (...) di un *modus procedendi* che non si traduca nell'effettuazione di specifiche indagini di mercato e/o di tipo comparativo, laddove sussistano plausibili, dimostrabili e motivate ragioni, insite nell'affidamento del servizio all'organismo in house".

12. Cons. Stato, Sez. V, 6 maggio 2022, n. 3562.

in house “consente di ovviare alle problematiche economiche, burocratiche, logistiche e gestionali che una esternalizzazione del servizio necessariamente comporterebbe, ma non si fa alcun riferimento, nemmeno esemplificativo, alle problematiche concretamente riscontrate nel corso della pregressa esternalizzazione effettiva dei servizi”¹³. Il Consiglio conclude affermando che: “in mancanza di detta attività istruttoria,” la scelta dell’ente “è risultata una valutazione di convenienza economica del tutto svincolata dal raffronto con il ricorso al mercato”.

Si prenda anche l’esempio della Regione Puglia, la quale per la Misura Pnrr 1.5 “Cybersecurity” – Progetto “Cybersecurity Posture Assessment e Security Awareness Training” ha affidato il servizio alla società in house InnovaPuglia SpA. Dalla determina di affidamento¹⁴ non si evincono né quali siano i vantaggi di tale affidamento né l’istruttoria condotta, in quanto l’ente si limita a citare l’art. 192 c.2 del Codice dei Contratti pubblici del 2016 ed indicare che l’in house si occuperà del progetto operativo denominato “Supporto tecnico alla progettazione e acquisizione della Piattaforma di simulazione phishing e Security Awareness Training”.

Riflessioni conclusive

Nell’applicazione della normativa in materia degli affidamenti in house per i servizi di cybersecurity le amministrazioni locali hanno trovato due importanti ostacoli: il cospicuo numero di norme prodotte dal diritto nazionale e gli orientamenti della giurisprudenza a volte anche tra loro contrastanti.

Un aspetto interessante dell’indagine condotta è il fatto che, nonostante le incertezze della normativa e della giurisprudenza, gli enti dimostrano una propensione al ricorso all’istituto dell’in house providing per il servizio della cybersecurity. Si possono ipotizzare le seguenti ragioni: la crescente richiesta della normativa europea e nazionale che preme per un maggiore coinvolgimento delle diverse amministrazioni, centrali e locali; l’obiettivo degli enti che è, malgrado la complessità della tematica, quello di avere un servizio col tempo efficace ma anche semplice sia nella configurazione che nella gestione, alla portata anche delle piccole e medie amministrazioni.

Si è osservato che le società in house hanno adeguato la propria offerta in ambito It agli Enti locali, cosicché anche tali amministrazioni possano fornire alla cittadinanza servizi

13. Come indicato nella sentenza, il Consiglio di Stato ravvisa che l’ente avrebbe dovuto, quanto meno, utilizzare lo “storico” dei costi dei servizi per i quali si era già rivolta al mercato e comunque effettuare la comparazione con i prezzi offerti dagli operatori operanti nel mercato, tenendo conto delle compensazioni dovute per i servizi non a domanda.

14. Determina n. 29 del 03/04/2023.

aggiornati e sicuri, creando una sensibilità alla tematica cyber anche all'interno degli enti di piccole dimensioni.

Le interpretazioni, secondo le quali il ricorso “eccessivo” da parte degli Enti locali dell'affidamento diretto dei servizi alle società in house può compromettere il principio del libero mercato e della libera concorrenza, non considerano la dinamicità intrinseca dell'innovazione tecnologica e la quotidianità degli attacchi informatici.

A maggior ragione si ravvisa la necessità che le amministrazioni partecipanti impieghino la metodologia dell'affidamento diretto alle società in house anche per i servizi in materia di cybersecurity. Anche la giurisprudenza si è espressa dando parere positivo, purché l'ente in house “agisca come un vero e proprio organo dell'amministrazione dal punto di vista sostantivo”.¹⁵

Si ponga l'esempio di un'unione comunale che affidi alla propria società in house il servizio cyber: tale scelta può determinare un doppio beneficio, sia in termini di facilità di gestione che in termini economici. In merito al primo aspetto, il valore aggiunto è rappresentato dalla gestione “omogenea” dei servizi digitali da parte dello stesso operatore per i comuni facenti parte dell'unione, che consente anche l'unificazione e lo scambio di esperienze e di prassi. In relazione al secondo aspetto, il vantaggio è rappresentato dalle economie di scala, in quanto le in house offrono spesso servizi ad un minor costo rispetto ai fornitori privati, pur garantendo idonee competenze in materia.

Il nodo principale, come previsto dalla normativa nazionale e oggetto di pronunce giurisprudenziali, resta in particolare l'onere di motivazione a carico degli enti partecipanti. Come indicato da Libertini (2012) la facoltà dell'amministrazione di optare per l'in house providing è vincolata dalla “ragionevole motivazione” che la medesima deve fornire. Le ragioni di tale scelta possono essere ricondotte sia alla valorizzazione di capitale umano ed al know-how già presenti nell'organizzazione partecipata, quanto alla volontà dell'ente di guidare in modo diretto e completo la gestione del ramo di attività interessata. È pur vero che, anche se la cybersecurity può essere intesa come un'attività strumentale e non un'attività puramente amministrativa e pertanto gli enti partecipanti godranno di un onere motivazionale più leggero, questi ultimi saranno comunque tenuti a motivare la loro decisione. La dottrina (Mattarella, 2023) ha valutato la motivazione come una sorta di escamotage che consente alle amministrazioni di abusare dell'autoproduzione e viceversa gli appesantimenti di tale onere, richiesti dalla normativa e dalle decisioni giurisprudenziali, possono “spesso alimentare il lavoro di consulenti giuridici ed economici per dare una veste legittima e razionale a una decisione già presa”.

15. Cons. Stato, Sez. VI, 25 novembre 2008, n. 5781.

Si è davanti ad una rete complessa, in cui devono dialogare la normativa in materia di affidamenti in house, dove è presente uno strato di norme codificate negli anni, e la materia della cybersecurity. Sarebbe allora necessaria una nuova normativa, o un'integrazione della normativa già esistente, che regoli compiutamente le due tematiche, che nasca dalla consapevolezza che gli Enti locali in materia di cybersecurity hanno costi e spesso competenze interne diverse rispetto alle grandi amministrazioni centrali. Demonizzare l'in house providing, inquadrandolo come un abuso dell'autoproduzione, non sembra essere di aiuto.

Incentivare gli investimenti di cybersecurity nelle amministrazioni locali può avvenire anche attraverso una legittimazione esplicita degli affidamenti diretti alle società in house, soprattutto se il servizio offerto da queste ultime determina una minore spesa per gli enti. Per quanto attiene al grado di affidabilità delle in house, si deve considerare che esistono delle norme standard di sicurezza che i fornitori devono rispettare e garantire nel prestare i servizi cyber ai propri clienti, sia pubblici che privati. Anche le società partecipate sono tenute a rispettare tali norme, al pari delle società del libero mercato. La Strategia cloud Italia, che prevede l'implementazione di servizi pubblici digitali sicuri in particolare attraverso la policy del "cloud first", regola l'attività dei provider pubblici e privati. Le società, comprese quelle in house, che offrono sistemi di cybersecurity alle Pa, devono necessariamente adottare e fornire standard di qualità e sicurezza adeguati, tra cui le soluzioni in cloud.

Riferimenti Bibliografici

- Alberti, C. (2001). Appalti in house, concessioni in house ed esternalizzazione. *Rivista Italiana di Diritto Pubblico Comunitario*, 3-4.
- Casalini, D. (2009). *L'organismo di diritto pubblico e l'organizzazione in house*. Napoli: Jovene.
- Cristoforetti, D. (2024). Dati e servizi nel cloud pubblico dell'Unione dei Comuni Terre d'Argine. Sicurezza e valorizzazione delle professionalità interne. *Azienditalia*, 1.
- Libertini, M. (2012). Le società di autoproduzione in mano pubblica: controllo analogo, destinazione prevalente dell'attività ed autonomia statutaria. Un aggiornamento a seguito dell'art. 4 del d.l. 13 agosto 2011, n. 138, convertito con legge 14 settembre 2011, n. 148. *Rivista di Diritto Societario*, 2.
- Lucca, M. (2019). Aiuti di stato e affidamenti in house nei servizi ICT. *ICT Security Magazine*.
- Lucca, M. (2004). Il paradosso degli affidamenti in house, tra meccanismi di incompiuta liberalizzazione e incompatibilità comunitaria. *LexItalia.it*. Consultabile in https://www.lexitalia.it/articoli/lucca_inhouse.htm
- Macchiarulo, L. (2018). Società in house: il controllo analogo tramite patti parasociali o altri accordi. *Rivista di Diritto Societario*, 4.
- Macheda, A. (2024). I servizi pubblici locali: Le scelte gestionali della pubblica amministrazione. *Diritto Amministrativo*, 6.
- Mattarella, B. G. (2023). Ambiguità e vicende degli affidamenti in house. *Rivista Trimestrale di Diritto Pubblico*, 4.