Public procurement e cyber sicurezza nella P.A.

di Mario De Benedetti

Abstract

La circolare dell'Agenzia per l'Italia digitale (AgId) del 24 giugno 2016 sulla modalità di acquisizione di beni e servizi ICT nelle more della definizione del 'Piano triennale per l'informatica nella pubblica amministrazione' ha posto in evidenza il ruolo, e l'utilità per la cyber sicurezza, del sistema italiano di *public procurement*. Il documento sottolinea in particolare il ruolo di Consip, società *in-house* del Ministero dell'economia e delle finanze, a sostegno dell'innovazione e della sicurezza dei sistemi informativi della Pubblica Amministrazione, in coerenza con le linee guida varate dal Governo in tema di prevenzione e protezione dagli attacchi cibernetici provenienti dalla rete Internet.

Questo articolo analizza gli aspetti salienti della circolare per quanto concerne il ruolo del *public procurement* rispetto alla cyber security, fornendo nel contempo utili indicazioni, interpretative e pratiche, alle amministrazioni e società pubbliche direttamente coinvolte.

Profilo dell'autore

Mario De Benedetti è laureato in Relazioni internazionali presso la facoltà di Scienze politiche dell'Università Luiss Guido Carli di Roma. Ha inoltre frequentato, presso lo stesso ateneo, il Master in Management e Politiche delle Pubbliche Amministrazioni.

Keyword Consip, appalti pubblici

Sommario 1. La Consip e le funzioni connesse all'attività di Information Technology - 2. Evoluzione normativa della Cyber Security nella Pubblica Amministrazione italiana - 3. Consip e AgID: la centrale di committenza nazionale per gli acquisti di tecnologie ICT

1. La Consip e le funzioni connesse all'attività di Information Technology

La Concessionaria servizi informatici pubblici (Consip S.p.A), originariamente Concessionaria Servizi Informativi Pubblici (CON.S.I.P.), è una società per azioni qualificabile come *in house*, in quanto interamente partecipata dal Ministero dell'economia e delle finanze (MEF), posta al servizio esclusivo della Pubblica Amministrazione ed operante sulla base degli indirizzi forniti dal Ministero dell'economia e delle finanze stesso.

Al momento della sua istituzione, ad opera del decreto legislativo. n. 414, art. 1, c. 2, del 1997[1] era stata pensata come strumento operativo in base al quale poter attuare un cambiamento nella gestione delle tecnologie informatiche nell'ambito dell'allora Ministero del Tesoro, del Bilancio e della programmazione economica, in quanto responsabile della gestione delle attività informatiche dell'Amministrazione statale centrale in materia finanziaria e contabile.

Il fine dell'azienda era, sostanzialmente, l'esercizio di attività informatiche per conto della Pubblica Amministrazione destinate allo sviluppo di un modello organizzativo e gestionale orientato alla realizzazione dell'efficacia e dell'economicità dell'attività amministrativa pubblica attraverso la promozione e gestione dei sistemi informativi.

Le intenzioni del legislatore erano, all'epoca, quelle di riformare la finanza pubblica attraverso la revisione delle modalità di gestione del bilancio finanziario; si introdusse, allora, la contabilità analitica per centri di costo collegata a criteri di tipo economico[2], la quale necessitava di una struttura organizzativa che fosse portatrice di nuove istanze, basate sull'utilizzo di tecnologie innovative, in particolare informatiche, che fossero di accompagnamento e sostegno al cambiamento nella Pubblica Amministrazione.

Il d.lgs. n. 414 del 1997, in anticipo sui tempi odierni, rilevava la necessità di innovazione del settore pubblico dal punto di vista informatico, conferendo allo Stato l'esercizio esclusivo delle attività informative telematiche, sulla base di un pieno adeguamento tecnico e strutturale delle amministrazioni pubbliche.

Era necessario, quindi, dotare una struttura societaria appositamente costituita, che operasse esclusivamente nell'interesse ed a servizio dello Stato, delle competenze utili alla gestione di queste attività, di importanza strategica per il settore pubblico e, in quanto tali, da sottrarre necessariamente all'affidamento esterno a soggetti privati (*outsourcing*); è così che Consip ottiene l'affidamento della gestione dell'ambito di *Information Technology* (IT) relativo alle pratiche contabili e finanziarie dell'amministrazione statale.

Le funzioni relative al settore IT di cui Consip all'inizio si occupava la vedevano, fondamentalmente, nella posizione di garante dell'effettivo impiego delle tecnologie informatiche e della loro efficiente evoluzione nel settore pubblico, anche nell'ottica di garantire un accesso ottimale al mercato delle imprese fornitrici di tecnologie IT, data la progressiva trasformazione dell'informatica in strumento fondamentale di modernizzazione dell'agire amministrativo, necessario per venire incontro, in tempi ristretti, alle necessità dei cittadini e delle imprese[3].

Al fine di erogare soluzioni migliori ed efficienti resi sia alle amministrazioni pubbliche, sia a cittadini privati e imprese, nell'ambito dei servizi IT la Consip operava come un'organizzazione la cui opera era indirizzata a predisporre attività di consulenza ed analisi di fattibilità, governo e controllo delle forniture, oltre ad impiegare le proprie risorse nella propria attività di centrale di committenza, legata sia all'acquisizione di beni e servizi, sia alla gestione dei diversi fornitori[4].

La Consip opera in qualità di centrale di committenza nazionale, attuando il Programma di razionalizzazione degli acquisti nella Pubblica Amministrazione[5], supportando le singole amministrazioni nelle fasi del processo di approvvigionamento (operando attraverso il sistema delle

Convenzioni) ed attuando gli obiettivi affidati attraverso provvedimenti di legge o atti amministrativi, che necessitano delle competenze nell'ambito del *public procurement*[6].

Tuttavia, il d.l. n. 87 del 2012, le cui disposizioni verranno poi trasfuse, con modificazioni, nel d.l. n. 95 del 2012 (in particolare nell'art. 4, commi 3 bis e 3 ter), dispone il trasferimento in capo a Sogei S.p.A. delle funzioni di supporto alle amministrazioni pubbliche in materia informatica, mediante l'attribuzione a quest'ultima delle attività informatiche riservate allo Stato ed, in particolare, dello sviluppo e della gestione dei sistemi informatici destinati al settore pubblico, lasciando a Consip l'attività di acquisizione dei beni e dei servizi per Sogei[7].

In attuazione di quanto previsto all'art. 20 del medesimo decreto, è stato disposto che la Consip operi in qualità di centrale di committenza anche al servizio dell'Agenzia per l'Italia digitale (AgID)[8] svolgendo, in tale veste, funzioni relative alle Reti telematiche della Pubblica Amministrazione, al Sistema pubblico di Connettività (SPC), alla Rete internazionale della Pubblica Amministrazione ed ai contratti quadro finalizzati alla rimozione delle duplicazioni amministrative di carattere informatico[9].

Ad oggi, la funzione di affidataria delle procedure informatiche riservate allo Stato conferite originariamente a Consip è stata, quindi, fortemente rivista e riformulata, risultando funzionale esclusivamente all'espletamento delle attività collegate al proprio ruolo di centrale di committenza nazionale per l'acquisto di beni e servizi per il settore amministrativo pubblico[10].

2. Evoluzione normativa della Cyber Security nella Pubblica Amministrazione italiana

Il d.P.C.M. 24 gennaio 2013, art. 2, c. 1, lett. i)[11], definisce la *Cyber security* come: «condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi».

Si può quindi sostenere che essa sia equivalente ad un'attività di protezione di informazioni, sistemi ed infrastrutture (interconnessi tra loro) che opera attraverso la prevenzione e la repressione degli attacchi informatici provenienti dal 'Cyber Spazio'[12]. La Pubblica Amministrazione, nell'esercizio della propria attività istituzionale, raccoglie e produce, allo stesso tempo, un'enorme quantità di dati e documenti[13] che, nell'ambito ed in base ai limiti previsti dalle normative vigenti, devono essere resi disponibili anche in formato digitale. La sicurezza informatica in ambito pubblico comporta la necessità di attuare tutte le misure necessarie alla protezione dell'hardware, del software e dei dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza e la protezione da eventuali usi illeciti.

L'impianto normativo a sostegno della sicurezza informatica, tuttavia, non ha trovato, negli anni, un inquadramento organico e coerente, lasciando la disciplina della *Cyber security* regolata da provvedimenti sparsi nel tempo: in Italia, infatti, il processo di digitalizzazione del settore pubblico, in assenza di una totale convergenza verso pratiche omogenee che garantiscano interoperabilità tra le Pubbliche Amministrazioni e tra queste ed il settore privato, costituisce un elemento di debolezza sistemica, piuttosto che un mezzo di crescita e sviluppo[14].

Le norme più importanti che possono essere citate sono: Allegato b) al Codice in materia di protezione dei dati personali (d.lgs. n. 196 del 2003), che costituisce il disciplinare tecnico alle misure minime di sicurezza; l'art. 17, c. 1, lett. a) e c) e l'art. 51 del d.lgs. n. 82 del 2005 (Codice dell'Amministrazione Digitale) i quali, rispettivamente, evidenziano la necessità di concentrare in un unico ufficio il coordinamento strategico dello sviluppo dei sistemi informatici di telecomunicazione e fonia (lettera a) e l'indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture (lettera c)[15] e regolano la sicurezza dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni[16]; l'art. 21 del d.P.C.M. 1 aprile 2008, recante «Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività (SPC)»[17]; il d.l. n. 83 del 2012[18] che, all'art. 19 istituisce l'Agenzia per l'Italia digitale e, all'art. 20, stabilisce che essa detti: «indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità dei linguaggi, delle procedure e degli standard, anche di tipo aperto, in modo da assicurare anche la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione europea»; l'art. 33 septies, c.1 del d.l. n. 179 del 2012, c.d. 'Decreto crescita 2.0', che prevede il «Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese»[19].

È, tuttavia, con il d.P.C.M. del 24 gennaio del 2013 che viene introdotto un quadro organico più strutturato riguardante la sicurezza informatica nella Pubblica Amministrazione: scopo del decreto è quello di definire, in un unico contesto, l'impianto istituzionale integrato dotato della responsabilità della tutela della sicurezza nazionale in materia cibernetica ed informatica, relativamente alle infrastrutture critiche sia materiali, sia immateriali.

L'architettura istituzionale è articolata su tre livelli di intervento: a) indirizzo politico e coordinamento strategico; b) di supporto permanente con funzioni di raccordo tra tutte le amministrazioni ed enti permanenti; c) di gestione delle crisi[20]. Vengono indicati i compiti relativi a ciascun soggetto istituzionale, compresi i meccanismi e le procedure utili alla risposta tempestiva agli attacchi informatici, nell'ottica di creare un modello organizzativo e funzionale che persegua l'integrazione delle funzioni che le Istituzioni coinvolte esercitano in base alle previsioni di legge[21].

In tale contesto è chiamata ad operare l'Agenzia per l'Italia digitale, il cui compito è di tracciare le linee guida strategiche che possano essere condivise dall'intero sistema amministrativo pubblico allo scopo di: a) sensibilizzare e formare il personale della Pubblica Amministrazione in materia di sicurezza informatica; b) offrire una efficace metodologia di analisi e rilevazione dei rischi informatici; c) esaminare e valutare le misure di protezione e le attività di misurazione delle prestazioni poste in essere[22].

All'interno dell'Agenzia opera il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA), organismo deputato al trattamento degli incidenti di sicurezza informatica, le cui funzioni sono finalizzate a supportare le Pubbliche Amministrazioni attraverso le attività di allarme rispetto alle minacce informatiche (*early-warning*), la gestione degli incidenti e l'analisi relativa agli effetti che essi producono, compresa la diffusione della cultura della sicurezza cibernetica e la cooperazione inter istituzionale (anche internazionale), assicurando il potenziamento delle risorse del settore pubblico riguardo la protezione informatica e la risoluzione delle criticità riguardanti le reti della Pubblica Amministrazione.

3. Consip e AgID: la centrale di committenza nazionale per gli acquisti di tecnologie ICT

Il 'Decreto Sviluppo' del 2012 è di fondamentale importanza per la definizione di un modello di condivisione istituzionale delle competenze riguardanti la *Governance* delle tecnologie ICT nella Pubblica Amministrazione italiana. Le funzioni esercitate da Digit PA sono ora trasferite in capo ad AgID e Consip: in base alle previsioni di cui all'art. 20, c. 3, del decreto n. 83 del 2012, l'Agenzia è responsabile della predisposizione delle linee guida operative utili allo sviluppo ed alla promozione dei processi di digitalizzazione della vigilanza e controllo sul rispetto delle norme[23], assorbendo anche i compiti attribuiti in capo all'Agenzia per la diffusione delle tecnologie per l'innovazione ed al Dipartimento per la digitalizzazione per la Pubblica Amministrazione e l'innovazione tecnologica; alla Consip viene, invece, affidata la responsabilità circa le attività amministrative, contrattuali e strumentali allo scopo di realizzare gli obiettivi indicati dalla disposizione di legge, con primaria attenzione sull'attività di consulenza riguardante gli acquisti di beni e servizi della Pubblica Amministrazione, anche in virtù del proprio ruolo di aggregatrice della domanda tramite gara che la rende la società pubblica più adatta alla gestione degli acquisti utili alla sicurezza dei sistemi informatici perché ottima conoscitrice del mercato.

Ad essa, più precisamente, è affidato il compito di gestire ed indirizzare, in collaborazione con l'Agenzia, le richieste del settore pubblico anche in materia di sicurezza cibernetica al fine di rendere il sistema informatico della Pubblica Amministrazione più sicuro ed efficiente. A dare manforte alla partnership tra Consip e AgID interviene una Convenzione quadriennale, firmata nel marzo del 2013, che riguarda misure concernenti la stipula di Contratti ed Accordi quadro per l'acquisto di beni e servizi di *Information e Communication Technology* relativamente a: progetti (sistemi informativi gestionali, sistemi informativi verticali); *commodity* (servizi di telecomunicazioni, contratti quadro applicativi); infrastrutture/applicazioni cross (sistema pubblico di connettività, servizi cloud).

In questo contesto opera una funzione di altissima importanza la recentissima stipula dei Contratti quadro relativi alla fornitura di servizi di connettività del Sistema Pubblico di Connettività, oggetto della gara che Consip ha indetto su indicazioni di AgID[24], allo scopo di rendere effettivi i progetti riguardanti la 'Crescita Digitale' della Pubblica Amministrazione italiana.

Il secondo lotto di contratti, in particolare, riguarda i servizi inerenti la gestione delle identità digitali, l'autenticazione per l'accesso ai servizi e la sicurezza applicativa[25]. I servizi forniti secondo le modalità previste dai Contratti quadro sono funzionali all'attuazione del «Piano triennale per l'informatica nella Pubblica Amministrazione», il documento che predisporrà una visione sistemica unitaria attraverso cui realizzare l'allocazione ottimale delle risorse impiegate per lo sviluppo dei sistemi informativi dell'Amministrazione Pubblica italiana.

Il Piano triennale opera nel contesto normativo predisposto dalla legge di stabilità 2016[26] la quale si pone l'obiettivo di raggiungere il risparmio di spesa annuale nelle tecnologie informatiche delle Pubbliche Amministrazioni ammontante al 50 per cento della spesa annuale media per la gestione corrente del solo settore informatico, relativa al triennio 2013-2015, da realizzare entro la fine del triennio 2016-2018: esso deve essere predisposto da AgID ed approvato dal Presidente del consiglio dei ministri o dal Ministro delegato, come previsto all'art. 1, comma 513, della legge di stabilità.

A Consip, o al soggetto aggregatore interessato[27], viene affidata la programmazione degli acquisti di beni e servizi per l'informatica, sentita preventivamente AgID per l'acquisizione di beni e servizi strategici. Il Piano è un documento di importanza ambivalente: da un lato serve a predisporre il prospetto, per ciascuna amministrazione, dei beni e servizi informatici e di connettività (unitamente ai servizi di particolare importanza strategica), compresi i relativi costi, suddivisi in spese destinate all'innovazione e spese destinate alla gestione corrente; dall'altro, è cruciale nel processo di strutturazione ed implementazione del «Modello strategico di evoluzione del sistema informativo della Pubblica Amministrazione», strutturato in tre livelli, per i quali il Piano provvederà ad indicare obiettivi strategici, costi e modalità di risparmio.

Nel primo livello tra questi, 'Infrastrutture materiali', sono inserite le infrastrutture fisiche che erogano i servizi informativi applicativi della Pubblica Amministrazione: *data center*, servizi di connettività, *disaster recovery*, *business continuity*, *cybersecurity*. Il Piano servirà da volano per la riduzione del numero di *data center*, allo scopo di garantire elevati standard di sicurezza e perseguire obiettivi di efficienza e razionalizzazione della spesa: a questo scopo, le infrastrutture verranno classificate e suddivise in *cluster* corrispondenti ai servizi erogati ed ai dati gestiti, per ognuno dei quali verranno individuati gli obiettivi da conseguire in termini di sicurezza, performance e relativi costi[28].

Di recente, l'AgID ha provveduto ad inviare a tutte le amministrazioni e società pubbliche inserite nel conto economico consolidato della Pubblica Amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT), la circolare n. 2 del 24 giugno del 2016 recante «Modalità di acquisizione di beni e servizi ICT nelle more della definizione del "Piano triennale per l'informatica nella pubblica amministrazione" previsto dalle disposizioni di cui all'art.1, comma 513 e seguenti della legge 28 dicembre 2015, n.208 (legge di stabilità 2016)» che, in attesa dell'attuazione del Piano triennale, elenca le indicazioni utili alla programmazione delle spese in beni e servizi informatici dei destinatari, in coerenza con gli obiettivi dell'Agenda digitale, oltre che a fornire le linee guida che saranno di ausilio alle Pubbliche Amministrazioni per adeguare i propri sistemi informativi al Modello strategico, allo scopo di non pregiudicare la piena attuazione del Piano triennale a partire dal 2017.

In particolare, secondo il disposto del paragrafo 4, che richiama le previsioni della circolare del Ministero dell'Economia e delle Finanze del 17 maggio 2016, n. 16, le Pubbliche Amministrazioni possono effettuare acquisti per approvvigionamenti ai sensi del dettato della Legge di Stabilità 2016, art. 1, c. 516, utilizzando gli strumenti di acquisto forniti da Consip (o dalle centrali di committenza o altri soggetti aggregatori) secondo i seguenti principi*:* a) predisposizione e trasmissione ad AGID di un piano di integrazione alle infrastrutture immateriali affinchè sia attuato il pieno utilizzo di tutte le infrastrutture disponibili e non ancora utilizzate (SPID, ANPR, PagoPA e NoiPA), entro dicembre 2017, al fine di consentire, entro il 2018, il perseguimento degli obiettivi di risparmio di spesa previsti dal comma 515 della Finanziaria per il 2016; b) impossibilità di effettuare acquisti di beni e servizi informatici, anche se per innovazione, se entrano in contrasto con i principi generali definiti nel paragrafo 3 della circolare in questione, né sostenere spese destinate alla istituzione di nuovi data center, oltre che le spese per l'implementazione delle applicazioni in dotazione nelle infrastrutture immateriali, quali il potenziamento di soluzioni di pagamento locale o di infrastrutture per l'autenticazione ai servizi online.

In riferimento alla infrastruttura immateriale 'ComproPA', nelle more dell'emanazione delle Regole tecniche aggiuntive, di cui all'art. 58 del d.lgs. n. 50 del 2016 (nuovo Codice degli Appalti), per garantire la trasmissione e la condivisione dei dati tra i sistemi telematici di acquisito e di negoziazione, è sottolineato che le amministrazioni che siano prive di piattaforme telematiche per le negoziazioni, non potranno effettuare investimenti per la creazione di nuove piattaforme, ma potranno comunque utilizzare le piattaforme di negoziazione rese disponibili da CONSIP o dalle centrali di committenza, oppure impiegare 'servizi di piattaforma di *e-procurement*' (pubblicazione, negoziazione, aggiudicazione) erogati in modalità *Application Service Provider*[29]; le centrali di committenza già fornite di una piattaforma di negoziazione, preso atto sia degli obblighi di adeguamento al nuovo Codice degli appalti sia degli obblighi relativi all'uso di dispositivi di comunicazione elettronici nello svolgimento di procedure di aggiudicazione, possono realizzare gli investimenti previsti per il biennio 2016/2017; c) verifica preliminare, ai fini della realizzazione degli acquisti di beni e servizi informatici e di connettività, fatti salvi «gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente» (ai sensi del c. 512 della Legge di stabilità 2016), della sussistenza, per le Amministrazioni Pubbliche e le società del conto economico consolidato ISTAT, di obblighi di utilizzo di strumenti di acquisto e strumenti di negoziazione centralizzata.

Sarà necessario verificare la sussistenza dell'obbligo di ricorso alle Convenzioni CONSIP (art. 1, comma 449, della legge n. 296/2006), al Mercato elettronico della pubblica amministrazione (art. 1, comma 450, della legge n. 296/2006), agli Accordi quadro, al Sistema pubblico di connettività o alle gare su delega individuati con decreto ministeriale (art. 2, comma 574, della legge n. 244/2007), oltre che l'obbligo di ricorso a strumenti di acquisto e negoziazione telematici forniti da CONSIP o dalle centrali di committenza regionali di riferimento (art. 15, comma 13, lettera d) , d.l. n. 95/2012)[30].

Le amministrazioni e le società pubbliche interessate dal documento in questione, che non siano obbligate a ricorrere agli strumenti di negoziazione e di acquisto di cui sopra, devono comunque ricorrere, in base alla disposizione del summenzionato comma 512, agli strumenti forniti da Consip e dagli altri soggetti aggregatori; inoltre, le stesse possono procedere autonomamente alle acquisizioni di beni e servizi informatici in seguito alla verifica dell'assenza di strumenti di aggregazione, verificabili sul sito della stessa Consip S.p.A.

Note

[1] Decreto legislativo 19 novembre 1997, n. 414, "Attività informatiche dell'Amministrazione statale in materia finanziaria e contabile", http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:1997-11-19;414!vig= .

[2] Legge 3 aprile 1997, n. 94, recante modifiche alla Legge 5 agosto 1978, n. 468 e successive modificazioni e integrazioni, recante norme di contabilità generale dello Stato in materia di bilancio. Delega al Governo per l'individuazione delle Unità Previsionali di Base del bilancio dello Stato»., http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1997-04-03;94.

[3] A. GIARDETTI, *Il modello Consip. Evoluzione e Funzioni della centrale di committenza nazionale*, Key Editore, 2015.

[4] D. BROGGI, *Consip: una novità nella Pubblica Amministrazione*, Franco Angeli, 2006.

[5] Il progetto nato all'inizio del nuovo millennio ad opera della Legge Finanziaria per il 2000 e denominato «Programma di razionalizzazione della spesa pubblica per gli acquisti di beni e servizi», si situa all'interno di un processo volto alla modernizzazione della Pubblica Amministrazione, nell'ottica di sviluppare modelli di approvvigionamento basati sull'impiego di processi e tecnologie ICT. Questo si basa su: a) aggregazione della domanda, al fine di conseguire economie di scala e ridurre i costi di beni e servizi; b) rafforzamento del potere negoziale della Pubblica Amministrazione, che porta all'aumento dei volumi di beni e servizi richiesti con conseguente possibilità di acquisto dei medesimi a prezzi unitari più vantaggiosi; c) riduzione delle tempistiche richieste per l'accesso al mercato da parte delle amministrazioni pubbliche; d) individuazione di nuovi sistemi di razionalizzazione della spesa; e) promozione di strumenti innovativi di *procurement* telematico; f) semplificazione delle procedure gestite da Consip. Tramite essa, vengono introdotte nel settore pubblico nuove metodologie di gestione dei processi di approvvigionamento, rappresentate dalle tecniche di *E-procurement*, come il sistema delle Convenzioni e degli Accordi Quadro o il Mercato elettronico della Pubblica Amministrazione per gli acquisti sotto la soglia comunitaria, strumenti da tempo utilizzati nel settore privato, a cui si affianca il Sistema dinamico di acquisizione.

[6] Gli interventi normativi in materia più rilevanti sono: il d.l. n. 52 del 7 maggio 2012, il d.l. 6 luglio 2012 n. 95 (Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini nonché misure di rafforzamento patrimoniale delle imprese del settore bancario) e la legge di stabilità 2013, i quali hanno istituzionalizzato l'obbligo di approvvigionamento attraverso le Convenzioni-quadro Consip S.p.A. per tutte le tipologie di beni e servizi che devono essere acquistati dalle Amministrazioni statali, centrali e periferiche.

[7] Sogei S.p.A. è la Società di *Information & Communication Technology* del Ministero dell'Economia e delle Finanze, costituita nella seconda metà degli anni '70 del secolo scorso, in esecuzione di una specifica esecuzione normativa nell'ambito delle iniziative dell'Istituto per la Ricostruzione Industriale (IRI), le cui azioni appartengono interamente al suddetto Ministero, classificandosi, così, come società *in house* del Mef stesso.

[8] L'Agenzia per l'Italia digitale, già Digit PA, è stata istituita dal d.l. n. 83 del 2012 allo scopo di dirigere le attività finalizzate all'innovazione ed alla promozione delle tecnologie ICT a sostegno della Pubblica Amministrazione, in attuazione degli obiettivi dell'Agenda digitale italiana coordinati, a loro volta, con quelli fissati dall'Agenda digitale europea. Coordina inoltre le attività dell'amministrazione centrale, regionale e periferica, progettando e monitorando l'attuazione del 'Sistema Informativo della Pubblica Amministrazione', anche attraverso l'adozione di infrastrutture e standard che riducano i costi sostenuti dalle singole amministrazioni e migliorino i servizi erogati ai privati.

[9] Comma 3 quater del d.l. n. 95 del 2012: a) le Reti telematiche delle amministrazioni pubbliche sono lo strumento che interconnette le Pubbliche Amministrazioni sia tra loro, sia con i privati (art. 12, c. 4, d.lgs. n. 82 del 2005; b) il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche per la diffusione e lo sviluppo del patrimonio informativo e dei dati nel settore amministrativo pubblico, necessario a garantire la sicurezza, la salvaguardia e la riservatezza delle informazioni in possesso della Pubblica Amministrazione (art. 83, d.lgs. n. 82 del 2005); c) la Rete internazionale, interconnessa al SPC, è l'infrastruttura che mette in collegamento le amministrazioni pubbliche italiane con i propri uffici all'estero (art. 85, d.lgs.. n. 82 del 2005).

[10] Il c. 3 ter del Decreto Legge n. 95 del 2012 enuclea gli ambiti di competenza di Consip in qualità di centrale di committenza, stabilendo che: «fermo restando lo svolgimento da parte di Consip S.p.A. delle attività ad essa affidate con provvedimenti normativi, le attività di realizzazione del Programma di razionalizzazione degli acquisti, di centrale di committenza e di E-procurement continuano ad essere svolte dalla Consip S.p.A.».

[11] Direttiva recante «Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale».

[12] «Spazio cibernetico: l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi», DPCM 23 gennaio 2013, art. 2, c.1, lett. h).

[13] Tale bagaglio di informazioni deve essere tutelato per mantenere integre e, perciò, affidabili le informazioni pubbliche; prevenire gli attacchi e gli abusi informatici; evitare che queste informazioni vengano diffuse senza autorizzazione; permettere ai servizi *on* line dell'apparato burocratico di poter funzionare senza interruzioni.

[14] *Il futuro della Cyber security in Itala*, a cura d R. Baldoni e R. De Nicolai, Laboratorio Nazionale di Cyber Security, ottobre 2015.

[15] *2015 Italian Security Report*, a cura di R. Baldoni e L. Montanari, Roma, febbraio 2016.

[16] «Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture».

[17] Comma 1: «L'architettura di sicurezza del SPC è volta a consentire: a. lo sviluppo del SPC come dominio affidabile (trusted), costituito da una federazione di domini di sicurezza in cui diversi soggetti si impegnano reciprocamente ad adottare le misure minime definite nell'ambito del SPC, atte a garantire i livelli di sicurezza necessari all'intero sistema"; Comma 2: "La Commissione, sulla base dell'analisi dei rischi cui sono soggetti il patrimonio informativo ed i dati della pubblica amministrazione, emana le linee guida riguardanti le misure di sicurezza e gli standard da adottare».

[18] Decreto Sviluppo 2012: «Misure urgenti per l'Agenda digitale e la Trasparenza nella Pubblica Amministrazione».

[19] «L'Agenzia per l'Italia digitale, con l'obiettivo di razionalizzare le risorse e favorire il consolidamento delle infrastrutture digitali delle pubbliche amministrazioni, avvalendosi dei principali soggetti pubblici titolari di banche dati, effettua il censimento dei Centri per l'elaborazione delle informazioni (CED) della pubblica amministrazione, come definiti al comma 2, ed elabora le linee guida, basate sulle principali metriche di efficienza internazionalmente riconosciute, finalizzate alla definizione di un piano triennale di razionalizzazione dei CED delle amministrazioni pubbliche che dovrà portare alla diffusione di standard comuni di interoperabilità, a crescenti livelli di efficienza, di sicurezza e di rapidità nell'erogazione dei servizi ai cittadini e alle imprese».

[20] A. RAGOSA, *La strategia e le azioni AgID per la gestione della sicurezza informatica delle PA*, Agenzia per l'Italia digitale, Roma, 10 luglio 2013.

[21] Nel dicembre 2013, a completamento dell'opera iniziata con il DPCM 24 gennaio 2013, il Consiglio dei Ministri ha adottato due documenti di importanza cruciale ai fini della definizione di procedure coordinate necessarie alla prevenzione ed arginamento delle minacce cibernetiche alla Pubblica Amministrazione: il «Quadro strategico nazionale per la sicurezza dello spazio cibernetico» ed il «Piano nazionale per la protezione cibernetica e la sicurezza informatica». Entrambi pubblicati in Gazzetta Ufficiale n. 41 del 19 febbraio 2014 operano congiuntamente ai fini della realizzazione di cui sopra. Il Quadro strategico individua sei indirizzi principali: 1) Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati; 2) Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema Paese;– Incentivazione della cooperazione tra istituzioni ed imprese nazionali; 4) Promozione e diffusione della cultura della sicurezza cibernetica; 5) Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali on-line; 6) Rafforzamento della cooperazione internazionale. Questi dovranno essere conseguiti operando congiuntamente con gli 11 indirizzi operativi indicati nel Piano nazionale: 1) Potenziamento capacità di intelligence, di polizia e di difesa civile e militare; 2) Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati; 3) Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento; 4) Cooperazione internazionale ed esercitazioni; 5) Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali; 6) Interventi legislativi e *compliance* con obblighi internazionali; 7) *Compliance* a standard e protocolli di sicurezza; 8) Supporto allo sviluppo industriale e tecnologico; 9) Comunicazione strategica; 10) Risorse; 11) Implementazione di un sistema di Information *Risk*

Management nazionale. In questo prospetto, il Governo italiano ha voluto innestarsi definitivamente nel quadro già delineato a livello internazionale, introducendo quei principi strategici comuni che costituiscono le fondamenta del sistema di conservazione delle informazioni dagli attacchi derivanti dal Cyberspazio.

[22] Ragosa, *La strategia e le azioni AgID per la gestione della sicurezza informatica delle PA*, cit.

[23] La disposizione cita testualmente che l'Agenzia: «…a) contribuisce alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, allo scopo di favorire l'innovazione e la crescita economica, anche mediante lo sviluppo e l'accelerazione della diffusione delle Reti di nuova generazione (NGN); b) detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità dei linguaggi, delle procedure e degli standard, anche di tipo aperto, in modo da assicurare anche la piena interoperabilità' e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione europea; c) assicura l'omogeneità, mediante il necessario coordinamento tecnico, dei sistemi informativi pubblici destinati ad erogare servizi ai cittadini ed alle imprese, garantendo livelli uniformi di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo; d) supporta e diffonde le iniziative in materia di digitalizzazione dei flussi documentali delle amministrazioni, ivi compresa la fase della conservazione sostitutiva, accelerando i processi di informatizzazione dei documenti amministrativi e promuovendo la rimozione degli ostacoli tecnici, operativi e organizzativi che si frappongono alla realizzazione dell'amministrazione digitale e alla piena ed effettiva attuazione del diritto all'uso delle tecnologie, previsto dall'articolo 3 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni; e) vigila sulla qualità dei servizi e sulla razionalizzazione della spesa in materia informatica, anche in collaborazione con CONSIP Spa e SOGEI Spa; f) promuove e diffonde le iniziative di alfabetizzazione informatica rivolte ai cittadini, nonché di formazione e addestramento professionale destinate ai pubblici dipendenti, anche mediante intese con la Scuola superiore della pubblica amministrazione e il Formez, e il ricorso a tecnologie didattiche innovative, nell'ambito delle dotazioni finanziarie disponibili, senza nuovi o maggiori oneri per la finanza pubblica; g) effettua il monitoraggio, anche a campione, dell'attuazione dei piani di Information and Communication Technology (ICT) delle pubbliche amministrazioni, redatti in osservanza delle prescrizioni di cui alla lettera b), sotto il profilo dell'efficacia, economicità e qualità delle realizzazioni, proponendo agli organi di governo degli enti e, ove necessario, al Presidente del Consiglio dei Ministri, le conseguenti misure correttive, nonché segnalando alla Corte dei conti casi in cui si profilino ipotesi di danno erariale; h) svolge attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale, anche a carattere intersettoriale, per la più efficace erogazione di servizi in rete della pubblica amministrazione a cittadini e imprese; i) costituisce autorità di riferimento nazionale nell'ambito dell'Unione europea e internazionale; partecipa all'attuazione di programmi europei al fine di attrarre, reperire e monitorare le fonti di finanziamento finalizzate allo sviluppo della società dell'informazione; l) adotta indirizzi e formula pareri facoltativi alle amministrazioni sulla congruità tecnica ed economica dei contratti relativi all'acquisizione di beni e servizi informatici e telematici, anche al fine della piena integrazione dei sistemi informativi; m) promuove, anche a richiesta di una delle amministrazioni interessate, protocolli di intesa e accordi istituzionali finalizzati alla creazione di strutture tecniche condivise per aree omogenee o per aree geografiche, alla risoluzione di contrasti operativi e al più rapido ed effettivo raggiungimento della piena integrazione e cooperazione applicativa tra i sistemi informativi pubblici, vigilando sull'attuazione delle intese o degli accordi medesimi».

[24] Gara *SPC Cloud,* del 24 maggio 2016, composta da due lotti: lotto n. 1, riguardante servizi di *cloud computing* nelle modalità: *Infrastructure As A Service* (IAAS), in cui i clienti possono dotarsi di capacità elaborativa, storage, reti ed altre risorse di base sulle quali i clienti possono caricare ed eseguire software di base e applicativi. I clienti gestiscono i sistemi operativi, lo storage e le applicazioni caricate; *Platform As A Service* (PAAS), in cui i clienti possono sviluppare proprie applicazioni cloud basate su strumenti e linguaggi di programmazione supportati dal Provider, oppure possono utilizzare applicazioni compatibili reperibili sul mercato. I clienti hanno il controllo sulle applicazioni e sulle configurazioni degli ambienti di hosting; *Software As A Service* (SAAS), tramite cui i clienti possono utilizzare le applicazioni dell'infrastruttura cloud fornite dal Provider, accessibili da qualsiasi dispositivo tramite l'interfaccia a sua disposizione. I clienti non gestiscono l'infrastruttura, né le componenti di rete. Il lotto è stato aggiudicato al Raggruppamento Temporaneo di Imprese di Telecom Italia, Poste Italiane, Postel, Postecom e HPE

Service Italia; lotto n. 2, aggiudicato al RTI di cui fanno parte Leonardo Finmeccanica, IBM Italia, Fastweb e Sistemi Informativi**.** Il *cloud computing* indica una serie di tecnologie che permettono l'elaborazione, l'archiviazione e la memorizzazione dei dati mediante l'utilizzo di risorse hardware e software che forniscono servizi *on demand* (su richiesta) attraverso Internet.

[25] I servizi di sicurezza, verranno erogati sia in modalità *as a service*, sia in modalità *on premise*, e saranno finalizzati a garantire la sicurezza applicativa ed il supporta alle Amministrazioni Pubbliche nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità hardware e software dei sistemi informativi; tali servizi includeranno anche servizi professionali a supporto delle attività delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni. I servizi in modalità *as a service* vengono erogati attraverso il Centro Servizi del Fornitore (l'impresa o RTI vincitrice della fornitura di servizi), coadiuvato dagli strumenti hardware e software che il Fornitore stesso mette a disposizione. In fase di attivazione, l'Amministrazione interessata ed il Fornitore concordano strategie, policy di sicurezza per arginare le minacce ed i livelli di criticità dei servizi erogati, siano essi critici o meno. La gestione delle minacce avviene in funzione delle policy predefinite e dei relativi livelli di criticità. È prevista l'emissione di report periodici. I servizi in modalità *on premise* vengono erogati impiegando strumenti già in uso presso le Amministrazioni Pubbliche stesse mediante l'impiego di figure professionali messe a disposizione dal Fornitore.

[26] Legge n. 208 del 28 dicembre 2015, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-12-28;208!vig=.

[27] La figura dei soggetti aggregatori per l'acquisto di beni e servizi, è stata istituita con d.l. n. 66 del 2014, art. 9, convertito, con modificazioni, in legge n. 89 del 23 giugno 2014. Ne fanno parte: Consip; una centrale di committenza per ciascuna Regione 'qualora costituita ai sensi dell'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296'; altri soggetti, diversi dai precedenti, che siano in possesso dei requisiti di stabilità dell'attività di centralizzazione, di valori di spesa ritenuti significativi per le acquisizioni di beni e di servizi, con riferimento ad ambiti, anche territoriali, da ritenersi ottimali ai fini dell'aggregazione, della centralizzazione della domanda. Con questi requisiti è possibile richiedere l'iscrizione in un apposito Elenco e partecipare alle attività del Tavolo dei soggetti aggregatori, oltre che ad attingere al Fondo per l'aggregazione degli acquisti di beni e di servizi.

[28] Il secondo livello, 'Infrastrutture immateriali', concerne le piattaforme applicative, nazionali o locali, che erogano servizi condivisi, razionalizzando la spesa pubblica. Tra essi sono compresi: 'Spid' (Sistema pubblico di identità digitale), 'PagoPA' (nodo dei pagamenti per la gestione elettronica di tutti i pagamenti della PA), la fatturazione elettronica, 'ANPR' (Anagrafe unica della popolazione residente), 'ComproPA' (sistema delle piattaforme negoziali per gli acquisti della PA) e 'NoiPA' (sistema di gestione del trattamento giuridico ed economico dei dipendenti della PA). Il terzo livello, 'Ecosistemi', comprende i domini applicativi verticali, come individuati dal «Documento di Strategia per la Crescita Digitale 2014-20» (Sanità digitale, Scuola digitale, Giustizia digitale, Turismo digitale, Agricoltura digitale, Smart cities & communities), cui si aggiungono quelli operanti negli ambiti applicativi verticali (il public procurement, il fisco e tributi, i servizi alle imprese, il lavoro, l'edilizia e i lavori pubblici, ecc.).

[29] Modalità di erogazione di servizi informatici che consente la gestione centralizzata dell'*hardware* e del *software* ad un Provider, consentendo all'utente finale la piena discrezionalità sulla scelta di tempi e modi per l'utilizzazione del servizio.

[30] Circolare AgID n. 2 del 24 giugno del 2016, http://www.agid.gov.it/sites/default/files/documentazione/circolare_piano_triennale_24.6.2016._def.pdf.

Bibliografia

2015 Italian Security Report, a cura di R. Baldoni e L. Montanari, CIS Sapienza, Roma, febbraio 2016, http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

D. BROGGI, *Consip: una novità nella Pubblica Amministrazione*, Franco Angeli, 2006

Circolare AgID n. 2 del 24 giugno 2016, recante modalità di acquisizione di beni e servizi ICT nelle more della definizione del "Piano triennale per l'informatica nella pubblica amministrazione" previsto dalle disposizioni di cui all'art.1, comma 513 e seguenti della legge 28 dicembre 2015, n. 208 (legge di stabilità 2016), http://www.agid.gov.it/sites/default/files/documentazione/circolare_piano_triennale_24.6.2016._def.pdf

CONSIP, *Contratto Quadro Servizi di identità digitale e sicurezza applicativa*, aprile 2016, http://www.consip.it/opencms/export/sites/consip/news_ed_eventi/2016/4/Gara-1403-Lotto-2-Servizi-di-sicurezza.pdf

Decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetice e la sicurezza informatica nazionale, https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-27-gennaio-2014-quadro-strategico-nazionale-cyber.html

A. GIARDETTI, *Il modello Consip. Evoluzione e Funzioni della centrale di committenza nazionale*, Key Editore, 2015

Il futuro della Cyber security in Itala, a cura di R. Baldoni, R. De Nicola, Laboratorio Nazionale di Cyber Security, ottobre 2015, https://www.consorzio-cini.it/index.php/it/component/attachments/download/416

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – Sistema di informazione per la sicurezza della Repubblica, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, Presidenza del Consiglio dei Ministri, dicembre 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – Sistema di informazione per la sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza*, 2015, febbraio 2016, http://sicurezzanazionale.pdc/relazione-annuale/relazione-al-parlamento-2015.html

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – Sistema di informazione per la sicurezza della Repubblica, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Presidenza del Consiglio dei Ministri, dicembre 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

A. RAGOSA, *La strategia e le azioni AgID per la gestione della sicurezza informatica delle PA*, Agenzia per l'Italia digitale, Roma, 10 luglio 2013, http://www.agid.gov.it/sites/default/files/documentazione/strategia_sicurezza_informatica.pdf