Verso un'architettura digitale unica e sicura per la P.A.: il ruolo di AgID e Consip

Di **MARTA ZILIANTI**

SOMMARIO: – **1.** INTRODUZIONE. – **2.** AGID E CONSIP: DUE FACCE DELLA STESSA MEDAGLIA. – **3.** VERSO UN'ARCHITETTURA ISTITUZIONALE DI SICUREZZA CIBERNETICA. – **4.** POSSIBILI CRITICITA' E CONSIDERAZIONI CONCLUSIVE.

Abstract

This paper presentation explores the development of the new relationship between the public administration and the cyber security in light of the defense of the IT heritage, taking into consideration the key role of AgID and Consip and the complex architecture of cyber security to be implemented by the public entities following the AgID resolutions and the rules adopted during the last few years.

1. Introduzione. Non si ravvisa una normativa copiosa circa il rapporto tra pubblica amministrazione e cyber security. Le prime fonti si individuano infatti nel Codice dell'amministrazione digitale[1] e, ancora prima, nel Codice in materia di protezione dei dati personali[2]. Successivamente, il tema in questione è stato preso in esame dal legislatore con il Decreto Sviluppo del 2012[3] e il Decreto Crescita del medesimo anno[4], fino a giungere al d.p.c.m. del 24 gennaio 2013 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, abrogato recentemente da un analogo decreto che si esaminerà nel prosieguo.

La disciplina normativa, inizialmente scarna, quindi si è evoluta nel tempo. L'art. 51 del Codice dell'amministrazione digitale sopra citato ha introdotto delle regole di sicurezza dei dati, dei sistemi e delle infrastrutture

1 Art. 51 del d.lgs. 7 marzo 2005, n. 82.
2 Allegato B, Disciplinare tecnico in materia di misure minime di sicurezza del d.lgs. 30 giugno 2003, n. 196.
3 Art. 20, comma 3, lett. b), del d.l. 22 giugno 2012, n. 83, convertito con modificazioni dalla l. 7 agosto 2012, n. 134, concernente misure urgenti per la crescita del Paese.
4 Art. 33-septies del d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221, recante ulteriori misure urgenti per la crescita del Paese.

delle pubbliche amministrazioni. In particolare, sono state adottate soluzioni tecniche per la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati detenuti dalla P.A.. L'art. 51, comma 2, stabilisce in proposito che «I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta».

Il rischio cyber nei sistemi informatici delle P.A. è esploso negli ultimi anni, grazie all'esigenza di superare le criticità sorte con lo sviluppo tecnologico e per porre fine alle insidie alla sicurezza informatica[5]. In particolare, le amministrazioni possono essere facilmente esposte ad una serie di pericoli quali, la sottrazione, l'alterazione o la distruzione delle informazioni dalle stesse conservate. I servizi delle P.A. possono essere degradati, alterati o bloccati e le fonti possono essere confuse o alterate, inoltre, possono subire alterazioni le autorizzazioni o essere manomessi o distrutti i sistemi di controllo e di monitoraggio dalle stesse utilizzate.

Tali insidie avvengono tramite strumenti quali il contagio da malware (virus, botnet, phishing) o attacchi cibernetici (cybercrime, cyber war, activisms). Molto comuni sono anche il furto di credenziali o di identità, mediante la personificazione di un soggetto, una organizzazione o un servizio e il degrado, l'interruzione o la distruzione di un servizio.

Ne consegue che, con l'incremento delle potenzialità di internet, la criminalità informatica ha costituito una rete volta a scambiare informazioni e commercializzare prodotti e servizi funzionali al compimento di reati[6]. La possibilità di ricorrere a un mercato internazionale che possa gestire un sistema informatico vasto, ha esteso lo scenario del cyber-crime a qualsiasi tipologia di organizzazione criminale o terroristica.

5 Cfr. RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, (a cura di R. BALDONI e L. MONTANARI), 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security, in http://www.cybersecurityframework.it.
6 Cfr. AGENZIA PER L'ITALIA DIGITALE, (a cura di A. RAGOSA), La strategia e le azioni AgID per la gestione della sicurezza informatica delle P.A., in http://www.agid.gov.it.

In tale contesto, sono state rilevate ampie lacune nei sistemi utilizzati dalle P.A.[7], che hanno reso opportuna la costituzione di autorità ed enti ad hoc. È sorta, quindi, la necessità di incrementare e migliorare la protezione informatica delle P.A., con l'obiettivo di ridurre la vulnerabilità dei sistemi, nonché di diffondere la conoscenza delle norme a tutela della cyber security. Inoltre, sono stati definiti in maniera più attenta gli scenari di valutazione del rischio, coinvolgendo strutture adeguate e creandole laddove non esistenti, e costruendo una vera e propria cultura di monitoraggio e aggiornamento costante delle procedure, delle prassi e degli strumenti utilizzati.

È sufficiente verificare i rapporti tecnici di pochi anni fa per notare che la situazione della pubblica amministrazione è evoluta e si sta adeguando agli obiettivi europei. A titolo esemplificativo, il rapporto annuale del CIS (Centro di Ricerca Cyber Security della Università La Sapienza di Roma) fornisce un'idea chiara delle mancanze delle amministrazioni, anche delle più importanti e complesse[8].

2. AGID e CONSIP: due facce della stessa medaglia. Per comprendere la complessa architettura istituzionale che è stata creata dal legislatore nazionale, occorre definire due degli attori principali che operano all'interno di questa struttura: AgID e Consip.

L'Agenzia per l'Italia Digitale o AgID è stata istituita nel 2012 (art. 19 del Decreto Sviluppo) ed è sottoposta alla vigilanza del Presidente del Consiglio dei ministri o di un ministro delegato. Si tratta di un ente pubblico non economico avente il compito di fornire alle amministrazioni il supporto conoscitivo essenziale per l'attività amministrativa, che opera sulla base dei principi di autonomia organizzativa, tecnico-operativa, gestionale, di trasparenza e di

7 Le pubbliche amministrazioni, anche ai sensi della legge sul procedimento amministrativo (l. 7 agosto 1990, n. 241, art. 3-bis), incentivano l'uso della telematica nei rapporti interni tra le diverse amministrazioni e tra queste e i privati, al fine di conseguire una maggiore efficienza nella loro attività.

8 Cfr. RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, 2014 Italian Cyber Security Report, Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, in http://www.agid.gov.it.

economicità e «persegue gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e partecipazione dei cittadini e delle imprese».

Come espressamente stabilito dall'art. 14-bis del Codice dell'amministrazione digitale[9], la sua funzione principale è quella di essere preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana e dell'Agenda digitale europea, promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della P.A. e nel rapporto tra questa, i cittadini e le imprese[10].

9 Norma inserita dal d.lgs. 26 agosto 2016, n. 179.

10 Ai sensi dell'art. 14-bis, comma 2, del Codice dell'amministrazione digitale, le specifiche funzioni dell'AgID sono le seguenti: «a) emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea; b) programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella pubblica amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AgID, anche sulla base dei dati e delle informazioni acquisiti dalle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno; c) monitoraggio delle attività svolte dalle amministrazioni in relazione alla loro coerenza con il Piano triennale di cui alla lettera b) e verifica dei risultati conseguiti dalle singole amministrazioni con particolare riferimento ai costi e benefici dei sistemi informatici secondo le modalità fissate dalla stessa Agenzia; d) predisposizione, realizzazione e gestione di interventi e progetti di innovazione, anche realizzando e gestendo direttamente o avvalendosi di soggetti terzi, specifici progetti in tema di innovazione ad essa assegnati nonché svolgendo attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale, anche a carattere intersettoriale; e) promozione della cultura digitale e della ricerca anche tramite comunità digitali regionali; f) rilascio di pareri tecnici, obbligatori e non vincolanti, sugli schemi di contratti e accordi quadro da parte delle pubbliche amministrazioni centrali concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati per quanto riguarda la congruità tecnico-economica, qualora il valore lordo di detti contratti sia superiore a euro 1.000.000,00 nel caso di procedura negoziata e a euro 2.000.000,00 nel caso di procedura ristretta o di procedura aperta. […]; g) rilascio di pareri tecnici, obbligatori e non vincolanti, sugli elementi essenziali delle procedure di gara bandite, ai sensi dell'articolo 1, comma 512 della legge 28 dicembre 2015, n. 208, da Consip e dai soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66, concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e definiti di carattere strategico nel piano triennale. Ai fini della presente lettera per elementi essenziali si intendono l'oggetto della fornitura o del servizio, il valore economico del contratto, la tipologia di procedura che si intende adottare, il criterio di aggiudicazione e relativa ponderazione, le principali clausole che caratterizzano le prestazioni contrattuali. Si applica quanto previsto nei periodi da 2 a 5 della lettera f); h) definizione di criteri e modalità per il monitoraggio sull'esecuzione dei contratti da parte dell'amministrazione interessata ovvero, su sua richiesta, da parte della stessa AgID; i) vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del regolamento UE 910/2014 in qualità di organismo a tal fine

Per quanto concerne Consip S.p.A., si tratta di un modello societario particolare e innovativo. Essa è stata la prima centrale di committenza pubblica in Italia specializzata nella gestione di tutte le fasi del processo di approvvigionamento, con le funzioni di pianificazione strategica degli acquisti e di supporto nella gestione del procedimento di acquisizione. Consip ha svolto tali funzioni attraverso l'ausilio delle moderne tecnologie informatiche ed è stata in grado di rendere trasparente e celere il complesso meccanismo burocratico concernente l'approvvigionamento di beni e servizi pubblici (GIARDETTI, 2015)
Consip, costituita prima dell'AgID (nell' agosto 1997), è divenuta uno strumento di cambiamento della gestione delle tecnologie dell'informazione nell'allora Ministero del Tesoro, del Bilancio e della Programmazione Economica. Successivamente, mediante d.m. del 24 febbraio 2000 è stato conferito a Consip l'incarico di stipulare convenzioni e contratti quadro per l'acquisto di beni e servizi per conto delle Pubbliche Amministrazioni. Consip è stata, pertanto, garante dell'effettivo ed efficiente impiego delle tecnologie informatiche nel settore pubblico.

A partire dal 2012[11] le funzioni di supporto alle amministrazioni pubbliche in materia informatica sono state trasferite da Consip a Sogei S.p.A.[12], attraverso l'attribuzione delle attività informatiche riservate allo Stato e dello sviluppo e della gestione dei sistemi informatici destinati al settore pubblico. Consip continua, invece, a gestire l'attività di acquisizione dei beni e servizi per

designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'articolo 44-bis, nonché sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza; l) ogni altra funzione attribuitale da specifiche disposizioni di legge e dallo Statuto».

11 D.l. 27 giugno 2012 , n. 87, concernente misure urgenti in materia di efficientamento, valorizzazione e dismissione del patrimonio pubblico, di razionalizzazione dell'amministrazione economico-finanziaria, nonché misure di rafforzamento del patrimonio delle imprese del settore bancario.

12 Sogei (Società Generale d'Informatica S.p.A.) è la società di Information Technology totalmente controllata dal Ministero dell'Economia e delle Finanze e opera sulla base del modello organizzativo dell'in house providing. È partner tecnologico unico del citato Ministero, ha progettato e realizzato il Sistema informativo della fiscalità, del quale segue conduzione ed evoluzione e sviluppa sistemi, applicazioni e servizi per le esigenze di automazione e informatizzazione dei processi operativi e gestionali del Ministero, della Corte dei conti, delle Agenzie fiscali e di altre pubbliche amministrazioni.

Sogei e opera anche al servizio dell'AgID, svolgendo funzioni relative alle Reti telematiche della pubblica amministrazione, al Sistema pubblico di Connettività o SPC, alla Rete internazionale della P.A. e ai contratti quadro finalizzati alla rimozione delle duplicazioni amministrative di carattere informatico[13].

Dall'altro lato della medaglia, l'AgID interagisce con Consip mediante il rilascio di pareri tecnici, obbligatori e non vincolanti, sugli elementi essenziali delle procedure di gara bandite da Consip concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e di carattere strategico nel piano triennale[14].

La funzione che aveva originariamente Consip, quale affidataria delle procedure informatiche riservate allo Stato è stata fortemente riformulata e considerata funzionale esclusivamente per l'espletamento delle attività collegate al proprio ruolo di centrale di committenza nazionale per l'acquisto di beni e servizi per il settore amministrativo pubblico[15].

Con particolare riferimento alla sicurezza cibernetica, a Consip, in collaborazione con l'AgID, viene affidato il compito di gestire e indirizzare le richieste del settore pubblico al fine di rendere il sistema informatico della P.A. più efficiente e sicuro.

Vediamo ora come si intersecano i ruoli dei due attori AgID e Consip con le recenti direttive normative in tema di cyber security.

13 Ai sensi dell'art. 4, comma 3-ter, del d.l. 6 luglio 2012, n. 95, convertito dalla l. 7 agosto 2012, n. 135, è stabilito 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. Ferme restando le disposizioni di cui all'articolo 12, commi da 2 a 10, del decreto-legge 6 luglio 2011, n. 98, convertito, con modificazioni, dalla legge 15 luglio 2011, n. 111, gli strumenti di acquisto e di negoziazione messi a disposizione da Consip S.p.A. possono avere ad oggetto anche attività di manutenzione. La medesima società svolge, inoltre, le attività ad essa affidate con provvedimenti amministrativi del Ministero dell'economia e delle finanze. Sogei S.p.A., sulla base di apposita convenzione disciplinante i relativi rapporti nonché i tempi e le modalità di realizzazione delle attività, si avvale di Consip S.p.A, nella sua qualità di centrale di committenza, per le acquisizioni di beni e servizi».

14 Cfr. supra art. 14-bis, comma 2, del Codice dell'amministrazione digitale.

15 Cfr. M. DE BENEDETTI, Public procurement e cyber sicurezza nella P.A., in www.sicurezzanazionale.gov.it.

3. Verso un'architettura istituzionale di sicurezza cibernetica. Come anticipato, ogni amministrazione presenta caratteristiche differenti, per dimensioni, complessità organizzativa, tipologia di dati trattati. Il livello di esposizione ai rischi cibernetici aumenta e dipende anche da fattori ambientali e politici e ciò ha portato a prevedere una differenziazione nella disciplina della sicurezza, istituendo un'architettura distinta su tre livelli di intervento che vedremo più avanti nel dettaglio.

Con la legge di stabilità del 2016[16] il legislatore ha inteso porsi quale obiettivo principale il risparmio di spesa annuale della pubblica amministrazione per la gestione del settore informatico, mediante le seguenti modalità: (i) redazione di un Piano Triennale per l'informatica nella pubblica amministrazione da parte dell'AgID, contenente, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica; (ii) programmazione di acquisti di beni e servizi per l'informatica da parte di Consip o del soggetto aggregatore interessato e previa consultazione con l'AgID in merito ai beni e servizi strategici individuati nel citato Piano triennale; e (iii) risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, pari al 50 per cento della spesa annuale media per la gestione corrente sostenuta da ciascuna amministrazione per il solo settore informatico nel triennio 2013-2015.

Nelle more della definizione del Piano triennale, con circolare del 24 giugno 2016[17], l'AgID ha fornito le modalità con cui le amministrazioni pubbliche e le società inserite nel conto economico consolidato della P.A. individuate dall'ISTAT possono procedere agli acquisti di beni e servizi ICT (Information Communication Technology).

16 Art. 1, commi da 512 a 516, della l. 28 dicembre 2015, n. 208, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
17 Circolare AgID n. 2 del 24 giugno 2016, «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)».

La circolare in questione si inserisce nel più ampio contesto dei poteri conferiti all'AgID dal nuovo Codice dei Contratti Pubblici (d.lgs. 18 aprile 2016, n. 50) che, all'art. 58, comma 10, stabilisce che l'AgID «deve emanare le regole tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra i sistemi telematici di acquisto e negoziazione». Regole tecniche che sono state definite con la successiva circolare del 6 dicembre 2016[18] e che individuano le modalità con cui possono interoperare le piattaforme telematiche di e-procurement, stabilendo i riferimenti per l'utilizzo condiviso dei dati scambiati tra le piattaforme. L'obiettivo perseguito è quello di contribuire alla trasparenza delle fasi del processo e alla maggiore competitività tra fornitori di beni e servizi, nonché alla salvaguardia della spesa pubblica.

Contestualmente il legislatore europeo ha emanato una direttiva di notevole impatto sul tema oggetto di esame: la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza informatica nazionali (la c.d. Direttiva NIS). Si tratta di una normativa estesa a tutti gli Stati membri dell'Unione, che dovrà essere recepita entro maggio 2018. In Italia non è stata ancora emanata la relativa legge di attuazione, la quale indicherà nel dettaglio le specifiche azioni da intraprendere. Tra le disposizioni di maggiore rilevanza, la Direttiva NIS prevede (i) il miglioramento della capacità di cyber security dei singoli Stati dell'Unione mediante l'adozione di specifiche misure di sicurezza a carico dei settori interessati, (ii) l'aumento del livello di cooperazione tra gli Stati membri, (iii) l'obbligo per gli operatori di servizi essenziali e dei fornitori di servizi digitali di adottare un approccio basato sulla gestione dei rischi, nonché di riportare ad un'apposita autorità (e in ultima analisi all'Agenzia europea ENISA) tutti gli incidenti di una certa entità, e (iv) la designazione da parte di ogni Stato membro di un'autorità apposita che sia il punto di contatto per gli scambi

18 Circolare AgID n. 3 del 6 dicembre 2016, «Regole Tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra sistemi telematici di acquisto e di negoziazione».

internazionali, nonché la dotazione di una strategia cyber e la costituzione di uno o più CERT e CSIRT[19].

Occorre notare che l'Italia, in linea con le linee tracciate dalla Direttiva NIS, si è portata avanti emanando il 17 febbraio 2017 un decreto contenente gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali[20]. Il decreto ha permesso la riorganizzazione dell'architettura istituzionale della cyber security nazionale[21], già disciplinata peraltro nel previgente e analogo decreto del 24 gennaio 2013[22], rendendola più snella ed efficace. Tra le linee di intervento più innovative, si ravvisa il rafforzamento del ruolo del CISR (Comitato interministeriale per la sicurezza della Repubblica), che potrà emanare direttive con l'obiettivo di incrementare il livello di sicurezza informatica sul territorio nazionale e si avvarrà del supporto del CISR tecnico, ossia del coordinamento interministeriale delle amministrazioni CISR e del Dipartimento delle informazioni per la sicurezza (DIS). Inoltre, il nuovo decreto attribuisce al Direttore generale del DIS il compito di definire le linee di azione per la sicurezza cibernetica che dovranno assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati,

19 Per completezza, si segnala che l'acronimo inglese CERT sta per Computer Emergency Response Team, ossia squadra per la risposta ad emergenze informatiche, mentre CSIRT (Computer Security Incident Response Team) è la squadra preposta a rispondere in caso di incidenti informatici.

20 D.p.c.m. 17 febbraio 2017, n. 110835 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», pubblicato in Gazzetta Ufficiale n. 87 del 13 aprile 2017.

21 L'art. 1 del d.p.c.m. del 17 febbraio 2017 citato supra, fa riferimento alla «architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali».

22 D.p.c.m. 24 gennaio 2013, n. 67251 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», abrogato dall'art. 13, comma 4, del d.p.c.m. 17 febbraio 2017 citato supra. Rispetto a tale decreto, con il d.p.c.m. del 17 febbraio 2017 viene ampliata la definizione di sicurezza cibernetica, aggiungendo il termine controllo indebito. Ora la sicurezza cibernetica è definita pertanto quale: «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 o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi». Stessa estensione è stata data dal legislatore anche alle definizioni di minaccia cibernetica ed evento cibernetico (art. 2 del d.p.c.m. del 17 febbraio 2017).

verificandone ed eliminandone le vulnerabilità[23]. Ancora, con il decreto del 17 maggio 2017, il Nucleo sicurezza cibernetica o NSC viene ricondotto all'interno del DIS con l'obiettivo di fornire risposte agli eventi cibernetici significativi in raccordo con le strutture dei ministeri competenti per materia. Con particolare riferimento all'AgID, è prevista una forte interazione dell'agenzia con il Dipartimento della funzione pubblica e con alcuni ministeri (MiSE, Ministero dell'interno, Ministero della difesa e MEF). La ratio di tale intervento normativo è stata quella di raggiungere una maggiore semplificazione e razionalizzazione dell'impianto di cyber security, migliorando anche le funzioni di coordinamento e raccordo delle attività di prevenzione, preparazione e gestione delle crisi cibernetiche.

Con il decreto del 17 febbraio 2017 permangono in capo al Presidente del Consiglio dei ministri i poteri previsti in precedenza quale, a titolo esemplificativo, quello di adottare, su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali[24], e le linee d'azione da porre in essere per realizzare il quadro strategico nazionale[25].

A valle del decreto sinora esaminato, l'AgID, in attuazione del d.l. 22 giugno 2012, n. 83[26] e della direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015, che ha imposto l'adozione di standard minimi di prevenzione e reazione agli eventi cibernetici[27], ha emanato le Misure minime di sicurezza ICT

23 Art. 6 del d.p.c.m. 17 febbraio 2017 citato supra.
24 L'ultimo Piano nazionale è stato adottato il 31 marzo 2017: stabilisce gli obiettivi da perseguire e individua la roadmap per l'adozione da parte di soggetti pubblici e privati delle misure prioritarie per l'implementazione del quadro strategico nazionale (cfr. infra), sulla base di un dialogo attivo e interattivo (in particolare, prevede ben undici indirizzi operativi, tra i quali, ad esempio, la promozione e diffusione della cultura della sicurezza informatica, l'implementazione di un sistema di cyber risk management nazionale).
25 Quadro Strategico Nazionale adottato dalla Presidenza del Consiglio dei ministri nel dicembre 2013. Cfr. anche l'art. 3 del d.p.c.m. 17 febbraio 2017 citato supra.
26 L'art. 20, comma 3, lett. b) del d.l. 22 giugno 2012, n. 83, identifica nell'AgID l'organismo che «detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica».
27 La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri ha individuato l'AgID quale organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento in linea con quelli dei maggiori Stati partners e delle organizzazioni internazionali di cui l'Italia è parte. Si legge nella direttiva: «è emersa innanzitutto l'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di

per le Pubbliche Amministrazioni. Tali misure sono contenute nella circolare AgID n. 1 del 17 marzo 2017 e sono entrate in vigore con la pubblicazione in Gazzetta Ufficiale il 4 aprile 2017. Tuttavia le misure sono state rese pubbliche dall'AgID già un anno prima (i.e. il 26 aprile 2016): si è trattato di un'anticipazione della regolamentazione che è stata ufficializzata in seguito e che ha fornito alle P.A. dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento. La strategia adottata dall'AgID è stata certamente utile per le amministrazioni, specie in ragione della scadenza del 31 dicembre 2017, entro la quale dovranno essere attuati gli adempimenti previsti dalla circolare.

Con riferimento al contenuto delle misure anzidette, si rileva che l'AgID prevede tre livelli di attuazione: un livello minimo contenente i criteri di base cui la P.A. indipendentemente dalla sua dimensione o natura dovrà conformarsi in termini tecnologici, organizzativi e procedurali; altri due livelli che rappresentano standard di protezione più completi ed evoluti, che dovrebbero essere adottati dalle organizzazioni maggiormente esposte a rischi, specialmente se trattano informazioni o prestano servizi di particolare complessità e criticità.

L'AgID, con le misure in esame, intende fornire delle linee guida operative per proteggere i sistemi informativi e i dati delle pubbliche amministrazioni, permettendo una autovalutazione delle esigenze operative e delle mancanze della struttura ICT e l'individuazione delle azioni da intraprendere per il relativo adeguamento.

Per la tutela del proprio patrimonio informatico, le pubbliche amministrazioni hanno la possibilità di accedere a servizi in grado di mantenere il personale aggiornato sui rischi e sulle lacune della sicurezza cibernetica. Le P.A. dovrebbero, perciò, essere in grado di valutare e correggere le problematiche riscontrate e attuare policies idonee alla tipologia di struttura che è propria di un ente pubblico.

---

eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi».

Ultimo tassello del mosaico sopra rappresentato è la recente adozione del Piano Triennale per l'informatica nella pubblica amministrazione 2017-2019, predisposto dall'AgID (in collaborazione con, tra gli altri, Consip) e firmato dal Presidente del Consiglio dei ministri il 31 maggio 2017. È un documento di programmazione che definisce il percorso di attuazione nel modello strategico di evoluzione del sistema informativo della P.A., preventivando le spese per singola amministrazione o categoria di amministrazione in coerenza con gli obiettivi da raggiungere. Con questo documento l'AgID intende guidare da un punto di vista operativo la trasformazione digitale delle pubbliche amministrazioni, definendo le linee guida della strategia di sviluppo dell'informatica pubblica e fissando i principi e le regole per perseguire tale sviluppo.

Come rilevato anche dalla stessa AgID, il Piano Triennale non funge da libretto di istruzioni definitivo e completo; risulterebbe, infatti, difficile pianificare gli investimenti caso per caso. Pertanto è stato ideato un processo che sia di supporto all'interpretazione del Piano stesso e che integri in una fase successiva il documento. Al riguardo, si segnala che il Piano Triennale pubblicato il 31 maggio 2017 definisce le azioni per l'anno 2018, tuttavia, a settembre 2018 (e a settembre di ogni anno) verrà pubblicata una versione aggiornata del testo contenente le azioni previste per l'anno successivo, su proposta dell'AgID e previa approvazione del Presidente del Consiglio dei ministri o del Ministro delegato. In altre parole, si tratta di un piano in continua evoluzione.

Il lavoro svolto dall'AgID prosegue non solo nell'aggiornamento e integrazione del Piano Triennale ma anche nella predisposizione di una serie di linee guida contenente le specifiche tecnologiche e le scelte di indirizzo. A titolo esemplificativo, entro il mese di gennaio 2018 è previsto il rilascio di Linee guida per la razionalizzazione del patrimonio ICT delle P.A..

Il Piano Triennale prevede, inoltre, una specifica sezione dedicata alla sicurezza, rilevandone l'importanza per garantire la disponibilità, l'integrità e la riservatezza delle informazioni proprie del sistema informativo della P.A.[28]
L'AgID si occuperà del monitoraggio e del controllo dell'applicazione del Piano Triennale da parte delle amministrazioni, all'interno delle quali dovrà essere individuato un Responsabile della Trasformazione Digitale, preposto al confronto e al dialogo con l'AgID. Al riguardo, si è posta la domanda sulle possibili conseguenze in caso di ritardo nell'adeguamento da parte di un'amministrazione alle azioni descritte nel Piano Triennale. L'AgID ha fornito in merito una risposta piuttosto generica, senza individuare le relative sanzioni: «Ogni ritardo […] è da considerarsi come un costo non necessario per lo Stato, che deve essere ostacolato con i necessari strumenti di controllo della spesa pubblica».

4. Possibili criticità e considerazioni conclusive. Se per decenni la questione della sicurezza informatica era celata ed accessibile solo agli addetti ai lavori, oggi si discute apertamente e in maniera approfondita sulle minacce cibernetiche e su argomenti che erano ritenuti troppo tecnici.
Ne deriva una forte convinzione che sia necessario dotarsi di norme e strutture condivise che coordinino la materia complessiva della cyber security per i sistemi nazionali e sovranazionali in un'ottica di collaborazione: tutti devono partecipare e coadiuvare le proprie risorse, informazioni, capacità ed esperienze.

Non possono, tuttavia, nascondersi le criticità che derivano dalla implementazione dell'architettura di sicurezza cibernetica qui esaminata, specie con riferimento all'attuazione delle misure minime di sicurezza da parte della P.A. di cui alla circolare AgID n. 1 del 17 marzo 2017 sopra citata.

28 Sono previsti obiettivi strategici e linee di azione tra cui risulta, a titolo esemplficativo, (i) la realizzazione e gestione di un catalogo delle vulnerabilità informatiche (National Vulnerability Database - NVD), che va ad integrare i cataloghi disponibili a livello internazionale, con le vulnerabilità riscontrate in ambito nazionale, (ii) la realizzazione della Cyber Security Knowledge Base nella quale sono raccolte le informazioni sulle infrastrutture realizzate nel dominio della P.A. e sugli eventi di sicurezza occorsi nel tempo al loro interno.

La principale problematica è la mancanza di risorse della P.A.. Occorrono adeguate dotazioni finanziarie e l'adozione di tali misure è eccessivamente onerosa, specie se si tratta di implementare il terzo livello di applicazione, che consiste in un livello costoso, suggerito per le amministrazioni più grandi e più complesse, che erogano servizi aventi un maggiore livello di criticità. Dovranno essere fatti inevitabilmente degli investimenti.

Inoltre, non è da sottovalutare, la formazione adeguata del personale dipendente delle Pubbliche Amministrazioni, che si troveranno di fronte a novità di rilievo, con un notevole impatto sull'attività lavorativa dagli stessi svolta. Occorrerà sensibilizzare i dipendenti pubblici affinché siano evitati errori e siano diminuiti i rischi di condotte incaute o erronee di soggetti che non hanno dimestichezza con tale settore.

Riferimenti bibliografici

AGENZIA PER L'ITALIA DIGITALE (a cura di A. RAGOSA), La strategia e le azioni AgID per la gestione della sicurezza informatica delle P.A., in http://www.agid.gov.it.

E. CASETTA- F. FRACCHIA, Compendio di diritto amministrativo, Giuffrè Editore, Milano, 2016.

M. DE BENEDETTI, Public procurement e cyber sicurezza nella P.A., in www.sicurezzanazionale.gov.it

A. GIARDETTI, Il modello Consip evoluzione e funzioni della centrale di committenza nazionale, Key Editore, Vicalvi, 2015.

RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, (a cura di R. BALDONI e L. MONTANARI), 2015 Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security, in *http://www.cybersecurityframework.it*.

RESEARCH CENTER OF CYBER INTELLIGENCE AND INFORMATION SECURITY - SAPIENZA UNIVERSITÀ DI ROMA, 2014 Italian Cyber Security Report, Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, in http://www.agid.gov.it.