MINISTERO DELLA DIFESA

LINEE GUIDA

DEL RESPONSABILE PER LA TRANSIZIONE DIGITALE DELLA DIFESA

Edizione 2023

INDICE

ATTO DI APPROVAZIONE

Approvo il presente documento "*Linee Guida del Responsabile per la Transizione Digitale della Difesa*" .

Il presente documento abroga e sostituisce la "SMD-I-020 - *Direttiva per l'attuazione delle Disposizioni del Dirigente Generale Responsabile per i sistemi informativi dell'Amministrazione della Difesa (D.G.Re.S.I.A.D.) in aderenza alle politiche governative in materia di informatizzazione della pubblica amministrazione e norme applicative in materia di trattamento dei dati personali*", ed. 2009.

Roma, li 04 maggio 2023

IL MINISTRO

ELENCO DI DISTRIBUZIONE

COMANDI / ENTI

Diramazione Esterna:

UFFICI DI DIRETTA COLLABORAZIONE DEL MINISTRO DELLA DIFESA
UFFICIO CENTRALE DEL BILANCIO E DEGLI AFFARI FINANZIARI
SEGRETARIATO GENERALE DELLA DIFESA/DNA
STATO MAGGIORE ESERCITO
STATO MAGGIORE MARINA
STATO MAGGIORE AERONAUTICA
CENTRO ALTI STUDI PER LA DIFESA
COMANDO OPERATIVO DI VERTICE INTERFORZE
COMANDO PER LE OPERAZIONI DELLE FORZE SPECIALI
COMANDO PER LE OPERAZIONI IN RETE
UFFICIO PER LA TUTELA DELLA CULTURA E DELLA MEMORIA
ORGANISMO INDIPENDENTE DI VALUTAZIONE DELLA PERFORMANCE
UFFICIO CENTRALE PER LE ISPEZIONI AMMINISTRATIVE
CONSIGLIO DELLA MAGISTRATURA MILITARE
PROCURA GENERALE MILITARE PRESSO LA CORTE SUPREMA DI CASSAZIONE
CORTE MILITARE DI APPELLO
PROCURA GENERALE MILITARE PRESSO LA CORTE MILITARE DI APPELLO
TRIBUNALE MILITARE DI VERONA-ROMA-NAPOLI
PROCURA MILITARE DELLA REPUBBLICA PRESSO IL TRIBUNALE MILITARE DI VERONA-ROMA-NAPOLI
TRIBUNALE MILITARE DI SORVEGLIANZA

Diramazione Interna:

STATO MAGGIORE DELLA DIFESA
- Ufficio Generale del Capo di SMD
- Ufficio del Sottocapo di SMD
- Ispettorato Generale per la Sanità Militare
- I Reparto Personale
- II Reparto Informazioni e Sicurezza
- III Reparto Politica Militare e Pianificazione
- IV Reparto Logistica e Infrastrutture
- V Reparto Affari Generali
- VI Reparto C4I e Trasformazione
- Ufficio Generale Affari Giuridici
- Ufficio Generale Pianificazione Programmazione e Bilancio
- Ufficio Generale Responsabilità Amministrativa
- Ufficio Protocollo Unico
- Ufficio PRE.V.A.T.A.
- Ufficio Generale Spazio
- Ufficio Generale Innovazione Difesa
- Raggruppamento Autonomo Ministero della Difesa

REGISTRAZIONE DELLE AGGIUNT E VARIANTI

1	
2	
3	
4	
5	
6	
7	
8	

RIFERIMENTI NORMATIVI

Rif. [1] D.Lgs. 7 marzo 2005 n. 82 recante "Codice dell'Amministrazione Digitale" e s.m.i., in particolare le modifiche di cui al D.Lgs. 26 agosto 2016, n. 179 e D.Lgs. 13 dicembre 2017, n. 217.

Rif. [2] D.Lgs. 15 marzo 2010 n. 66 recante "*Codice dell'ordinamento militare*" (COM).

Rif. [3] D.P.R. 15 marzo 2010 n. 90 recante "*Testo unico delle disposizioni regolamentari in materia di ordinamento militare, a norma dell'art. 14 della Legge 28 novembre 2005 n. 246*" (TUOM).

Rif. [4] D.M. 18 settembre 2020 del Ministro della Difesa concernente l'individuazione dell'Ufficio dirigenziale generale responsabile per la transizione al digitale e del Dirigente generale Responsabile per la Transizione Digitale dell'A.D., ai sensi dell'art. 17 commi 1 e 3 del CAD.

Rif. [5] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (c.d. Regolamento Generale sulla protezione dei dati o *General Data Protection Regulation – GDPR*).

Rif. [6] D.Lgs. 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*", come modificato dal D.Lgs. 10 agosto 2018, n. 101, in recepimento del Regolamento (UE) 2016/679.

Rif. [7] Direttiva (UE) 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.

Rif. [8] Legge 9 gennaio 2004 n. 9 "*Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*" (c.d. "Legge Stanca"), come modificata dal D.Lgs. 10 agosto 2018 n. 106, in recepimento della Direttiva (UE) 2016/2102.

Rif. [9] D.L. 21 settembre 2019 n. 105, come convertito con Legge 18 novembre 2019 n. 133, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*".

Rif. [10] D.L. 14 giugno 2021, n. 82 "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", come convertito con la L. 4 agosto 2021, n. 109.

DIRETTIVE E CIRCOLARI DELLA DIFESA

Rif. [11] Direttiva SMD-I-003 "*Disciplinare per l'utilizzo dei servizi informatici non classificati erogati in ambito Difesa, quali i servizi di posta elettronica, instant messaging ed accesso ad internet*" - ed. 2017.

Rif. [12] Direttiva SMD-I-020 "*Direttiva per l'attuazione delle disposizioni del Dirigente Generale Responsabile per i Sistemi Informativi dell'Amministrazione della Difesa (Responsabile della Trasformazione Digitale dell'A.D.) in aderenza alle politiche governative in materia di informatizzazione della Pubblica Amministrazione e norme applicative in materia di trattamento dei dati personali*" – ed. 2009.

Rif. [13] Direttiva SMD-I-024 "*Procedure sulla gestione in sicurezza dei servizi informatici non-classificati dell'Amministrazione Difesa*" – ed. 2017.

Rif. [14] "*Direttiva sul trattamento e protezione dei dati personali del Ministero della Difesa*" - edizione 2021, del Responsabile della Protezione dei Dati personali dell'A.D. (diramata

con f. n. M_D SSMD REG2021 0039603 in data 2 marzo 2021 da SMD I Reparto – Referente del Titolare del trattamento per l'AOO dello SMD.

Rif. [15] Direttiva SMD "*La strategia di trasformazione digitale del Comparto Difesa*" – ed. 2021.

DIRETTIVE DELLA PCM E ALTRI DICASTERI

Rif. [16] Direttiva "*2025 - Strategia per l'innovazione tecnologica e la digitalizzazione del Paese*" ed. 2019 – emanata dal Ministro per l'Innovazione Tecnologica e la Digitalizzazione.

Rif. [17] Circolare 18 aprile 2017, n. 2/2017 - "*Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni*", dell'Agenzia per l'Italia Digitale (AgID) in recepimento della Direttiva PCM 1 agosto 2015, recante l'attuazione, da parte delle pubbliche amministrazioni, delle disposizioni in materia di protezione cibernetica e sicurezza informatica nazionale.

Rif. [18] Documento "*Piano Triennale per l'Informatica nella Pubblica Amministrazione*", di AgID e Dipartimento per la Trasformazione Digitale, ai sensi dell'art. 14-bis, comma 2, let. b) del CAD.

Rif. [19] Circolare del 1 ottobre 2018, n. 3 del Ministro della Pubblica Amministrazione "*Responsabile per la transizione digitale – art. 17 decreto legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale*".

Rif. [20] "*Linee Guida – La sicurezza nel procurement ICT*" – ed. 2020, di AgID.

Rif. [21] Circolare 20 gennaio 2021, n. 1 dell'AgID "*Monitoraggio sull'esecuzione dei contratti*" - (ai sensi dell'art.14 bis, comma 2, lettera h) del CAD), come modificato dal D.Lgs. 16 luglio 2020, n.76)".

1. PREMESSA

1.1 La trasformazione digitale della Pubblica Amministrazione e la Difesa.

La trasformazione digitale della Pubblica Amministrazione (PA) è un complesso ed articolato processo di rinnovamento organizzativo, oltre che di aggiornamento tecnologico, in continua e rapida evoluzione, in linea con le strategie politiche europee e nazionali che vedono nell'innovazione digitale della PA l'elemento indispensabile per la ripresa economica e sociale dei paesi dell'Unione Europea. Tale processo ha visto diverse fasi evolutive, spesso spontanee e influenzate dai vari mutamenti comportamentali della società e dei cittadini, che richiedono servizi informatizzati sempre più agili, efficaci e sicuri, in linea con i servizi rilasciati da organizzazioni private che puntano alla semplificazione e coinvolgimento. In tale contesto basta evidenziare l'enorme semplificazione di servizi bancari, assicurativi e di comunicazione.

Ad oggi, il quadro normativo si è modificato notevolmente e il Codice dell'Amministrazione Digitale (CAD, o Codice)[1], recependo anche le linee di indirizzo introdotte dai regolamenti e dalle direttive emanate dalla Commissione Europea, rimane il principale riferimento del settore. Il Codice riunisce, oggi, in un solo contesto aggiornato, tutte le disposizioni emanate dalle singole leggi nazionali al riguardo, abrogando quelle obsolete.

Per gli aspetti di specifico interesse del presente documento, si vuole sottolineare il radicale cambiamento dei contenuti del Codice, in particolare nell'art. 17 che prescrive alle pubbliche amministrazioni di garantire "*…l'attuazione delle linee strategiche per la digitalizzazione dell'amministrazione definite dal Governo, in coerenza con le Linee guida…*" dettate dall'Agenzia per l'Italia Digitale (AgID), quale Organismo di *governance* nazionale[2]. A tal fine, ciascuna pubblica amministrazione[3] "*…affida a un* ***unico ufficio dirigenziale generale*** *… la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità…*", in linea con i compiti indicati nello stesso articolo. La stessa disposizione normativa, altresì definisce che il responsabile del suddetto Ufficio generale è ***Responsabile per la Transizione Digitale*** (RTD)[4], e gli attribuisce competenze (manageriali, tecniche e di informatica giuridica) e funzioni di rilevanza strategica, necessarie per guidare il complesso processo di trasformazione digitale della propria amministrazione[5].

1.2 Scopo del documento.

La presente Direttiva definisce i compiti e le responsabilità dell'RTD. La sua corretta applicazione consentirà di:

- armonizzare e seguire costantemente lo sviluppo dell'informatica gestionale della Difesa;
- monitorare ed effettuare la verifica dei risultati ottenuti sui programmi relativi ai sistemi informativi dell'Amministrazione;
- porre le condizioni per gli interventi migliorativi necessari, anche in attuazione delle linee strategiche definite dal Governo in materia di trasformazione digitale della PA;
- garantire, conseguentemente, l'ottimizzazione delle risorse disponibili.

---

1 D.Lgs. 7 marzo 2005, n. 82 e successive modifiche e integrazioni (s.m.i.).

2 Ai sensi dell'art. 14-*bis*, comma 1 del CAD, l'AgID "*…è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato, e con l'Agenda digitale europea…*" e, per il comma 2, svolge le funzioni di "*…a) emanazione delle Linee guida contenenti regole, standard e guide tecniche , nonché di indirizzo, vigilanza e controllo sull'attuazione e rispetto delle norme di cui al presente Codice…*".

3 Le amministrazioni soggette all'applicazione del Codice sono individuate all'art. 2, comma 2.

4 La figura del RTD sostituisce quella del *Dirigente generale responsabile per i sistemi informativi automatizzati* di cui all'art. 10 del D.Lgs. 39/93. In esito alle s.m.i. del CAD introdotte dal D.Lgs. 176/2016, l'art. 10 del D.Lgs. 39/93 è stato abrogato.

5 Tale aspetto è particolarmente rimarcato nella Circolare 1 ottobre 2018, n. 3, del Ministro della Pubblica Amministrazione "*Responsabile per la Transizione Digitale – art. 17 decreto legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale*".

Nella considerazione che la maggior parte dei sistemi informativi automatizzati riguarda anche la trattazione dei dati del personale a vario titolo, viene dedicato un apposito capitolo in tema di "*privacy*", nel contesto informatico.

2. FUNZIONI, COMPITI E ORGANIZZAZIONE

2.1 Il Responsabile della Transizione Digitale dell'A.D.

Il Responsabile per la Transizione Digitale, come accennato in generale nella *Premessa*, opera per l'attuazione delle linee strategiche emanate dal Governo in materia di trasformazione digitale della PA e per i compiti e le responsabilità definite dal CAD[6].

Egli rappresenta, come spesso rimarcato in molteplici ambiti, l'elemento cardine nella definizione unitaria delle linee di indirizzo, della pianificazione, dello sviluppo, del coordinamento e verifica delle attività volte alla riorganizzazione dei processi interni, per la realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, in un'ottica di maggiore efficienza ed economicità. In virtù di tali oneri, il Responsabile è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice politico[7].

In tale contesto, fatte salve le disposizioni dettate dall'Ordinamento militare[8], l'RTD opera per il riordino, in chiave digitale, dei processi tecnico amministrativi interni all'A.D. sviluppando programmi che implementano sistemi informativi gestionali/servizi correlati all'applicazione delle disposizioni del Codice, al fine di migliorare l'efficacia e la fruibilità dei servizi.

Tutto ciò in aderenza alle linee guida del settore emanate dall'AgID e in coordinamento con le peculiarità della Difesa.

La trasformazione digitale implica un profondo cambiamento, principalmente di carattere gestionale piuttosto che tecnologico, che impatta sul modo di lavorare. Affinché tutti, nell'ambito dell'A.D., siano in grado di comprendere, accettare e adottare non solo i nuovi strumenti tecnologici ma anche i cambiamenti nei processi di lavoro, quindi consentire l'adattamento dell'Amministrazione all'era digitale, l'RTD dirama alle Aree Organizzative Omogenee/Unità Organizzative (AOO/UO) interessate dell'Area Interforze e agli SM di F.A., per gli aspetti di propria competenza, disposizioni o linee guida in merito agli indirizzi e ai relativi settori d'intervento definiti dal Governo, agli obiettivi prioritari per l'ICT e la sicurezza *cyber*; altresì, divulga le norme, le direttive tecniche e gli *standard* elaborati da AgID, armonizzandone la relativa applicazione con l'emanazione di appositi documenti.

Al fine di ottenere una risposta univoca da tutto il Comparto, l'RTD promuove le iniziative impartite dal Governo o dall'AgID per la formazione/informazione del personale militare e civile della Difesa impiegato nel settore l'ICT/*Cyber* e concorre anche nel fornire, agli organismi della Difesa preposti, gli indirizzi per l'aggiornamento delle offerte formative sotto gli aspetti della normativa e delle tecnologici emergenti.

Inoltre, per il ruolo di coordinamento che riveste, l'RTD ha la facoltà, peraltro richiamata dalle citate norme, di costituire tavoli di lavoro/coordinamento sia con gli altri dirigenti/figure di riferimento[9] del Comparto Difesa, sia con altre amministrazioni relativamente ai progetti di interesse comune.

L'RTD, in sintesi, garantisce una visione unitaria nel continuo processo di digitalizzazione dell'A.D., nel rispetto del CAD e dei dettami emanati dall'AgID, che recepisce come dirigente generale della pubblica amministrazione, alla luce delle esigenze e delle specificità del Dicastero.

2.2 Compiti ed attribuzioni derivanti dal D.Lgs. 7 marzo 2005 n. 82 del CAD.

L'art. 17 del CAD attribuisce *all'Ufficio dirigenziale generale* di ogni amministrazione e, quindi, anche all'RTD quale responsabile dell'Ufficio, specifici compiti per attuare la transizione alla

6 D.Lgs. 7 marzo 2005, n. 82 e s.m.i., art. 17 "*Responsabile per la transizione digitale e difensore civico digitale*".

7 Ai sensi dell'art. 17, comma 1-*ter* del CAD.

8 D.P.R. 15 marzo 2010 n. 90, con specifico riferimento al Titolo II - *Norme di coordinamento dei sistemi informativi automatizzati delle amministrazioni pubbliche con le esigenze di difesa nazionale*.

9 Ad esempio, il Responsabile per la Protezione dei dati personali/DPO, il Responsabile per la Prevenzione della Corruzione e della Trasparenza, Responsabile per la Conservazione della documentazione, ecc… (cfr. Circ. 1 ottobre 2018 n. 3 del Ministro della PA).

modalità operativa digitale della propria amministrazione, secondo le linee strategiche definite dal Governo, dettagliate nello stesso Codice e nelle linee guida attuative dell'AgID.

Detti compiti, attualizzati nelle varie s.m.i. della norma[10], prevedono in particolare:

- coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del CAD;
- accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
- analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla precedente alinea;
- indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis del CAD[11];
- pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 14-bis comma 2, let. b) del CAD.

2.3 Attribuzioni introdotte dalla Circolare 1 ottobre 2018, n. 3, del Ministro della PA.

Il Ministro della PA, con la Circolare in argomento, ha inteso evidenziare la particolare importanza che riveste la figura dell'RTD ai fini della trasformazione digitale della PA. A tal fine, il Ministro richiama l'attenzione su alcuni aspetti di particolare rilevanza connessi alla nomina della figura, ferma restando l'autonomia organizzativa riconosciuta dall'ordinamento giuridico delle singole amministrazioni centrali e locali.

Nell'elencare le responsabilità afferenti all'RTD sull'attuazione dei compiti che il CAD attribuisce all'Ufficio dirigenziale generale preposto, l'Autorità precisa che l'elenco di tali compiti deve ritenersi esemplificativo e non esaustivo, in quanto alla figura "…*competono tutti i poteri di impulso e coordinamento finalizzati alla piena transizione verso la modalità operativa digitale…*". A tal riguardo, "…*al fine di garantire la piena operatività del predetto Ufficio, si raccomanda di prevedere, nell'atto di conferimento dell'incarico o di nomina, nel caso di incarico*

[10] Ultime integrazioni introdotte dalla variante di cui al D.L. 31 maggio 2021 n. 77, convertito con L. 108/2021.

[11] Il *Punto di accesso telematico* ai servizi in rete delle PA, attivato preso la Presidenza del Consiglio dei Ministri (PCM).

in essere, oltre che i compiti espressamente previsti, anche quelli sotto indicati in ragione della trasversalità della figura:

a) il potere del RTD di costituire tavoli di coordinamento con gli altri dirigenti dell'amministrazione e/o referenti nominati da questi ultimi;

b) il potere del RTD di costituire gruppi tematici per singole attività e/o adempimenti (ad esempio: pagamenti informatici, piena implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.);

c) il potere del RTD di proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT);

d) l'adozione dei più opportuni strumenti di raccordo e consultazione del RTD con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali);

e) la competenza del RTD in materia di predisposizione del Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale;

f) la predisposizione di una relazione annuale sull'attività svolta dall'Ufficio da trasmettere al vertice politico o amministrativo che ha nominato il RTD. …".

In conclusione, sebbene gli atti abbiano origini da fonti diverse e contesti dissimili, si trova una correlazione fra quando disposto dall'Ordinamento militare e la Circolare stessa, nel ricordare "… *che il RTD rappresenta il punto di contatto con l'Agenzia per l'Italia Digitale e la Presidenza del Consiglio dei Ministri per le questioni connesse alla trasformazione digitale delle pubbliche amministrazioni, nonché per la partecipazione a consultazioni e censimenti previsti dal Piano triennale per l'informatica della pubblica amministrazione…*".

2.4 Coordinamento dei sistemi informativi delle PA con le esigenze della difesa nazionale.

L'azione dell'RTD si estende esclusivamente sulla parte ICT/*Cyber* gestionale della Difesa, sia dell'Area Tecnico Operativa (T/O) che Tecnico Amministrativa (T/A)[12], strettamente correlata con i sistemi informativi gestionali della PA, laddove intervengono e sono applicabili le disposizioni normative del CAD. A tal riguardo, il TUOM, nel Titolo II, definisce le "*Norme di coordinamento dei sistemi informativi automatizzati delle amministrazioni pubbliche con le esigenze di difesa nazionale*"[13], tutelando le particolari esigenze della Difesa che necessita di sistemi informativi[14]:

- a carattere prettamente operativo, concernenti o connessi con l'esplicazione dei compiti specifici della difesa dello Stato;
- aventi implicazioni di carattere operativo;
- appartenenti all'Arma dei Carabinieri ricadenti sotto la responsabilità della Difesa.

I citati sistemi perseguono peculiari finalità indicate nel TUOM[15] e rispettano le strategie e le linee d'indirizzo fissate dal Ministro della Difesa, anche in accordo con le intese raggiunte nell'ambito dell'Alleanza Atlantica.

In tale contesto, il monitoraggio dei programmi relativi allo sviluppo dei predetti sistemi resta attribuito al Capo del VI Reparto "*C4I e Trasformazione*" dello Stato Maggiore Difesa (SMD VI) e non ricadono nelle *policy* regolamentate dal CAD.

[12] Con esclusione per l'Arma dei Carabinieri che, in ragione dei compiti istituzionali, nomina un proprio RTD e individua un proprio Ufficio che svolge i compiti attribuiti all'*Ufficio dirigenziale generale*.

[13] Il Titolo II comprende gli artt. dal 542 al 551.

[14] Cfr. art. 544, comma 1 del TUOM.

[15] Cfr. art. 545 del TUOM.

2.5 I Referenti dell'RTD.

In ragione della complessità della struttura e delle molteplici articolazioni che compongono l'A.D., al fine di consentire al RTD di esercitare la *governance* verso tutte le AOO/UO dell'A.D. ed ottenere puntuale riscontro sull'andamento delle iniziative intraprese nel settore ICT e sicurezza informatica, è necessario individuare, presso gli Enti dello SMD e gli Stati Maggiori di F.A., dei referenti incaricati di espletare le funzioni di supervisione, controllo e consulenza per conto del RTD nell'ambito della propria organizzazione.

In tal senso, ferme restando le responsabilità e le attribuzioni del Capo di SM della Difesa e dei Capi di SM delle F.A., ogni AOO di vertice Interforze, nonché ogni SM di F.A. individua, con apposito atto interno, un proprio Referente che rappresenti l'interfaccia verso l'RTD per tutti gli aspetti afferenti al settore ICT e sicurezza informatica. Detto Referente, in particolare:

- recepisce le norme, le disposizioni/indicazioni tecniche, elaborate dall'RTD e le dirama, anche mediante apposite direttive/circolari interne, verso per tutte le articolazioni interessate della propria area di competenza;
- verifica la corretta applicazione delle disposizioni ricevute dall'RTD ed impartite alle discendenti articolazioni proponendo, eventualmente, interventi migliorativi necessari o opportuni;
- riferisce/relaziona direttamente al vertice gerarchico della propria organizzazione (Ca./SCa. di SM, Cte Vertice Operativo, Direttore Generale, ecc…) e all'RTD, sullo stato di situazione dei programmi di informatizzazione avviati;
- segue le problematiche attinenti ai progetti interministeriali ed intersettoriali limitatamente alle attribuzioni assegnate alla propria area di competenza;
- fornice consulenza nei confronti del rispettivo vertice gerarchico relativamente ai programmi di informatizzazione della propria organizzazione, in coordinamento con le *policies* e le linee d'azione stabilite dall'RTD;
- funge da punto di contatto per l'RTD per questioni connesse a progetti, soluzioni tecniche ed attività avviate/da avviare da parte della propria organizzazione e ne coordina le linee d'azione.

Considerata la complessità dello specifico settore, dovuta sia alla crescente ed inarrestabile evoluzione tecnologica, sia dal mutevole e variegato quadro giuridico-normativo, è indispensabile che il Referente, oltre al legame tecnico-funzionale con l'RTD, possieda competenze tecnologiche, di informatica giuridica, nonché un appropriato livello gerarchico per esercitare le sue funzioni nei confronti dell'AOO/UO di appartenenza. La struttura organizzativa tiene conto sia degli assetti interni alla Difesa ed individua i vari Referenti fra:

- Capi/Vice Capi dei Reparti C4I[16] degli SM di F.A.;
- Direttore/Vice Direttore di SGD/DNA V Reparto[17];
- Capi/Vice Capi Reparto di Comandi/Enti di vertice dello SMD, qualora il grado e le attribuzioni siano compatibili al ruolo rivestito, ovvero da un Capo Ufficio designato.

Per l'espletamento delle attribuzioni di supporto all'RTD, il Referente si avvale della collaborazione del Comando C4/Centro di Esercizio/struttura di supporto informatico della propria UO, ovvero del Referente Informatico Locale di ciascun EDR della propria UO.

[16] Ovvero denominazione analoga.
[17] V Reparto "*Innovazione Tecnologica*" del Segretariato Generale della Difesa/Direzione Nazionale Armamenti.

3. PROCEDURE

3.1 Il processo di *eGovernment* – Generalità.

Il Governo definisce le strategie per la trasformazione digitale della PA e l'AgID, in ambito nazionale, è l'organismo deputato alla realizzazione di dette strategie, con l'attuazione degli obiettivi del programma noto come *Agenda Digitale Italiana*[18]. Detto programma, in linea con le analoghe strategie e i principi guida della Comunità Europea, definisce i criteri e le azioni per l'evoluzione in chiave digitale della PA, fattore considerato di fondamentale importanza per rilancio dell'economia del mercato comune e dello sviluppo sociale del Paese e degli Stati membri.

In aderenza a tale linea, le Amministrazioni attuano la riorganizzazione del proprio settore, per la "*…realizzazione un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità…*", ricorrendo a progettualità che utilizzano le soluzioni e gli strumenti dell'informazione e della comunicazione disposte dal CAD, in conformità alle linee d'azione definite dall'AgID e dal Dipartimento per la Trasformazione Digitale (DTD) che sono indicate nel Piano Triennale per l'Informatica della PA (PT)[19]. Tale processo passa attraverso un percorso che deve essere adeguatamente pianificato in tutte le sue fasi e che si associa a varie procedure/buone pratiche[20] consolidate; questo consente sia alle amministrazioni, sia all'Agenzia e al Dipartimento, di delineare un chiaro punto di situazione delle attività programmate/in itinere, nonché delle risorse finanziarie impiegate a livello nazionale.

La Difesa, da sempre allineata alle regole dell'informatizzazione/digitalizzazione della PA[21], segue le predette procedure per gli aspetti connessi alla realizzazione di sistemi gestionali interoperabili e tecnologicamente all'avanguardia. Peraltro, il *modus operandi* sopra accennato risulta allineato con quanto disposto dall'ordinamento militare, che fissa le norme di coordinamento dei sistemi informativi della PA con le esigenze dei sistemi connessi alla difesa nazionale/orientati all'impiego dello strumento militare, le cui strategie sono fissate dal Ministro della Difesa.

Si riportano, di seguito, le principali procedure di riferimento in linea con le prescritte normative.

3.2 Piano Triennale per l'Informatica della PA.

Il Piano Triennale per l'Informatica della PA (PT) è un documento di indirizzo strategico ed economico, elaborato dall'AgID e dal DTD, che nasce per guidare operativamente la trasformazione digitale del Paese e le amministrazioni centrali e locali nello sviluppo dei propri servizi/sistemi informativi. Il PT definisce il modello di riferimento per lo sviluppo dell'informatica pubblica italiana fissando i principi architetturali fondamentali, le regole di usabilità e interoperabilità e precisando la logica di classificazione delle spese ICT, secondo cui:

- il livello nazionale definisce regole, *standard* e realizza piattaforme abilitanti che ottimizzano investimenti;
- le amministrazioni centrali e locali sviluppano servizi secondo le proprie specificità utilizzando competenze interne e/o di mercato;
- il privato, compresa la strategia di paese, programma investimenti di medio/lungo periodo e sfrutta nuove opportunità di mercato creando soluzioni che si integrino con le piattaforme nazionali;

---

[18] Il Programma ha origine con il documento "*Strategie per la crescita digitale 2014-2020*" della PCM, che ha definito i criteri generali e gli obiettivi a lungo termine da perseguire per l'evoluzione della digitalizzazione della PA. Successivamente, il documento è stato via via aggiornato e sostituito da indirizzamenti sempre più attuali che, sulla base degli orientamenti politici, economici e sociali del momento, recepiscono le esigenze di nuovi servizi digitali più efficienti, sicuri e di qualità.

[19] Ai sensi dell'art. 14-*bis*, comma 2, let b) del CAD.

[20] La terminologia è sovente usata nell'ambito della PA, ove per *buona prassi* o *buona pratica*, talvolta anche *miglior pratica* o *migliore prassi* (c.d. *best practice*), si intendono le esperienze, le procedure o le azioni più significative, o comunque quelle che hanno permesso di ottenere i migliori risultati, relativamente a svariati contesti e obiettivi preposti.

[21] Art. 528 del D.Lgs. 15 marzo 2010, n. 66 "*Codice dell'ordinamento militare*" (COM).

quanto sopra, al fine di focalizzare la spesa delle amministrazioni, migliorare la qualità dei servizi offerti a cittadini e imprese e mettere a disposizione degli strumenti efficaci per gli operatori della PA. Nella valutazione dei progetti di investimento in materia di innovazione tecnologica, le Amministrazioni tengono conto dei pareri e delle prescrizioni di AgID/DTD, nonché dei costi effettivi e delle economie derivanti dalla razionalizzazione del proprio settore.

Il documento, approvato dal Presidente del Consiglio dei Ministri o dal Ministro delegato entro il 30 settembre di ogni anno[22], viene redatto e aggiornato in conformità alle leggi che regolano la stabilità e gli investimenti dell'economia nazionale e sulla base delle informazioni/dati/proposte avanzate dalle amministrazioni. In particolare, la raccolta dei dati da parte delle amministrazioni avviene tramite una rilevazione annuale condotta da AGID sulla spesa ICT effettuata o programmata delle principali amministrazioni centrali e da Regioni, Province Autonome, città metropolitane e relativi comuni capoluogo, in qualità di soggetti aggregatori territoriali.
Il Piano è pubblicato sulla piattaforma nazionale per la *governance* della trasformazione digitale[23] e sul sito dell'Agenzia.

La Difesa pianifica le proprie progettualità e programma gli investimenti per le proprie esigenze (relative ai sistemi gestionali) anche sulla base delle linee d'azione dettate dal PT. L'RTD, per il tramite di SMD VI, partecipa alla rilevazione annuale della spesa ICT, collezionando i dati di interesse di AgID e li trasmette all'Agenzia tramite procedura telematica, nelle modalità e nei tempi che AgID di volta in volta comunica a tutte le amministrazioni.

3.3 Rilevazione annuale sulla spesa ICT delle PA.

L'attività, condotta dall'AgID nei confronti delle amministrazioni, rientra nel quadro più generale delle azioni di monitoraggio previste dal PT sullo stato della trasformazione digitale della PA.
La Difesa partecipa alla rilevazione avvalendosi dei Referenti dell'RTD delle Aree T/O e T/A., al fine di redigere un documento di raccolta dei dati unitario per tutto il Comparto, da sottoporre all'approvazione dell'RTD. I dati sono comunicati ad AgID, a cura dell'RTD, con procedura telematica e nelle scadenze fissate dall'Agenzia stessa.
La procedura finalizzata alla preparazione del suddetto documento è la seguente:

- l'RTD, in base delle scadenze/disposizioni determinate di volta in volta dall'AgID, comunica ai Referenti le tempistiche e le eventuali modalità per comunicare i dati richiesti;
- i Referenti, per la propria area di competenza, organizzano la raccolta dei dati che gli Enti periferici trasmettono ai rispettivi SM, Comandi o SGD (se trattasi di DG o Enti dell'area T/A);
- gli SM, Comandi dell'Interforze e SGD V, tramite i propri Referenti, inoltrano i propri consuntivi nei termini e con le modalità indicate da SMD VI nella comunicazione preventiva;
- l'RTD provvede ad elaborare un resoconto unitario che sarà comunicato all'AgID, tramite inserimento dei dati sull'apposito portale telematico predisposto dall'Agenzia.

Qualora necessario, può essere convocato il Comitato Coordinamento Informatica[24] (CCI) a cura di SMD VI, per l'esame congiunto del consuntivo generale o dirimere problematiche ad esso connesse.

3.4 Piano Triennale per l'Informatica della Difesa (PTD).

In analogia a quanto viene elaborato, a fattor comune, da AgID e dal DTD per le amministrazioni, anche la Difesa redige un Piano Triennale per l'Informatica per il proprio Comparto (PTD). L'elaborazione del PTD mira alla definizione di un documento che raccolga la situazione

[22] Art. 14-bis, comma 2, let. b) del CAD.
[23] Ai sensi dell'art. 18, comma 3 del CAD, il *link*: https://docs.italia.it.
[24] Il Comitato Coordinamento Informatica è un organo permanente interforze che opera per la Difesa nell'ambito dello SMD VI, con i compiti di esaminare, valutare, coordinare le principali problematiche a carattere interforze nel settore dell'informatica. E' presieduto dal VCR di SMD VI delegato per l'informatica e mantiene un legame funzionale con l'RTD per quanto attiene le problematiche relative all'informatica gestionale.

complessiva dei programmi ICT dell'A.D., già avviati o in fase di avvio, per la realizzazione dei sistemi informativi non classificati a carattere gestionale.

In relazione alle disposizioni che sono indicate:

- nel CAD e nel suddetto PT, per quanto attiene ai sistemi esclusivamente gestionali di varia natura, interconnessi o interoperabili con quelli della PA;
- nel TUOM e in relazione al documento di visione strategica di trasformazione digitale della Difesa, per quanto attiene ai sistemi di specifico interesse dell'A.D.;

l'RTD individua e predispone la pianificazione triennale delle specifiche azioni progettuali del settore Interforze e delle F.A., dando direttive alle predette Aree T/O e T/A tramite i rispettivi Referenti, affinché esplicitino la propria pianificazione e comunichino propri i fabbisogni finanziari.

In tale contesto, l'RTD:

- verifica che tale pianificazione sia in linea con gli obiettivi nazionali e coerenti alle esigenze stesse dell'A.D., evidenziando progetti che non siano perfettamente allineati con le strategie;
- verifica che la pianificazione non comporti duplicazioni e, in caso di proposte tra di loro conflittuali, propone eventuali soluzioni;
- assicura, in base alle priorità rappresentate, il soddisfacimento delle diverse esigenze, sulla base della valutazione tecnico-amministrativa e delle soluzioni tecniche di costruzione/produzione ed approvvigionamento di beni e servizi IT convalidate dal CCI;
- redige ed approva il PTD, quale documento programmatico e di indirizzo della Difesa.

Il PTD così redatto è sottoposto all'approvazione dell'RTD. Il documento viene aggiornato annualmente entro il 30 novembre.

3.5 Realizzazione dei progetti del settore ICT.

La riorganizzazione digitale dei processi interni all'A.D. si estrinseca con la realizzazione di progetti ICT aderenti alle esigenze delle AOO/UO della Difesa e in linea con le *policy* strategiche del settore. Peraltro, tutte le attività afferenti alla corretta realizzazione dei progetti, dalla pianificazione iniziale alla chiusura delle attività contrattuali, non possono prescindere da una costante azione di controllo/monitoraggio nelle loro varie fasi da parte dell'RTD, cui compete l'azione di indirizzo e coordinamento strategico dell'ICT gestionale della Difesa, nonché la responsabilità dei risultati derivanti dalla digitalizzazione dei processi.

3.5.1 Richiesta del parere obbligatorio di aderenza ai processi di digitalizzazione e standardizzazione in ambito Difesa.

Ferme restando le competenze e le responsabilità del SGD/DNA sullo sviluppo dell'iter tecnico amministrativo attraverso la competente Direzione Generale (DG), è necessario consentire all'RTD le verifiche preventive sugli atti progettuali e il monitoraggio delle attività tecnico-amministrative per ciascun progetto informatico relativo all'ICT gestionale.

A tal riguardo, gli Enti dell'Interforze delegati all'impiego operativo dei fondi e gli SM di F.A., trasmettono allo SMD VI la documentazione relativa alla realizzazione dei singoli progetti per la verifica di aderenza fra:

- le esigenze manifestate dall'Ente/F.A. nei programmi relativi alla digitalizzazione dei processi e gli obiettivi/finalità dei progetti;
- le tecnologie/misure di sicurezza informatiche utilizzate e le linee guida/disposizioni tecniche emanati dall'AgID e dall'Agenzia per la Cybersicurezza Nazionale (ACN).

In caso di esito positivo delle verifiche, l'RTD rilascerà un formale parere di rispondenza per ogni singolo progetto che verrà trasmesso all'Ente/SM interessato.

Analogamente, l'Ente/SM trametterà la documentazione relativa ad ogni progetto a SGD/DG competente per il rilascio del parere di congruità tecnico-economica e l'avvio dell'*iter* tecnico-amministrativo.

Nei casi previsti dal CAD, laddove sia obbligatorio il rilascio del parere tecnico da parte dell'AgID[25]:

- l'RTD, previa verifica, invierà all'Agenzia tutta la documentazione tecnico-amministrativa del progetto, comprensiva del parere di congruità tecnico-economica della DG, degli schemi di contratto/accordi quadro relativi all'acquisizione di beni e servizi e degli elementi essenziali delle procedure di gara bandite, dandone conoscenza all'Ente/SM di F.A. interessato e a SGD V[26] se trattasi di progetti dell'area T/A;
- l'AgID, effettuate le verifiche e, salvo eventuale richiesta di elementi integrativi, comunicherà all'RTD il parere tecnico di competenza;
- a procedura ultimata, l'RTD trasmetterà all'Ente/SM di F.A. interessato e alla DG il parere di AgID per il proseguo dell'*iter* tecnico amministrativo e l'emissione del previsto modello di finanziamento.

Nell'ambito del consuntivo annuale[27], ciascuna Ente/SM di F.A. dovrà riportare un punto di situazione sui progetti avviati e su quelli la cui realizzazione è ancora in corso.

3.5.2 Monitoraggio dei processi di digitalizzazione in ambito Difesa.

Il monitoraggio è un'attività che mira a verificare, in ogni momento, e assicurare il corretto sviluppo dei procedimenti tecnico-amministrativi dei progetti avviati, in una cornice di costante aderenza ai processi di digitalizzazione della Difesa. L'attività, contemplata dal CAD, oltre a rappresentare una precisa responsabilità per l'RTD[28], è volta a conferire solidità e completezza all'intera strategia ICT dell'amministrazione.

L'A.D., quale Amministrazione centrale, è tenuta a rispettare la normativa sui pubblici appalti[29] e, pertanto, ad effettuare le attività di monitoraggio anche sui contratti del settore ICT, in aderenza sia alle disposizioni amministrative emanate nell'ambito del Comparto, sia a quelle dell'AgID emanate con la Circolare 20 gennaio 2021, n. 1 "*Monitoraggio sull'esecuzione dei contratti*" [30].

In linea con la Circolare, l'Amministrazione deve porre in essere vari adempimenti, fra i quali nominare, con atto formale, un *Responsabile del Monitoraggio* (RdM) e comunicarne il nominativo all'AgID[31]. Detto Responsabile, di norma, è un dirigente o un funzionario apicale appartenente all'Ufficio dell'RTD, a cui viene affidata la gestione delle attività di monitoraggio sull'esecuzione dei contratti della propria Amministrazione.

L'RdM, quale interfaccia unica verso l'AgID, è posto a capo di un'attività complessa che prende origine dalla fase pre-contrattuale e termina con la chiusura degli oneri contrattuali; per tale motivo, dovrebbe essere coadiuvato da un apposito *team* di risorse (o *Gruppo di Monitoraggio*), appositamente costituito in seno all'amministrazione, con competenze e conoscenze necessarie[32] per adempiere a tutti i compiti definiti nella Circolare.

Al fine di supportare adeguatamente l'RTD, specialmente per le progettualità articolate in più fasi, l'attività di monitoraggio si basa su azioni pianificate (*piano di monitoraggio*), condotte

---

[25] Art. 14-*bis*, comma 2, lett. f), g), del CAD individua i casi in cui il parere tecnico dell'AgID è obbligatorio e:
a. non vincolante, sugli schemi di contratto e accordi quadro concernenti l'acquisizione di beni e servizi relativi ai sistemi informativi, qualora il valore lordo sia superiore a 1M€ nel caso di procedura negoziata e a 2M€ nel caso di procedura ristretta o aperta;
b. vincolante, sugli elementi essenziali delle procedure di gara bandite da Consip e soggetti aggregatori.

[26] SGD V Reparto – Innovazione Tecnologica.

[27] In ambito CCI e/o programmazione finanziaria.

[28] Art. 549 del TUOM "*Monitoraggio dei programmi relativi ai sistemi informativi automatizzati*".

[29] In particolare, le procedure e gli ambiti di applicazione o di esclusione espressamente indicati, sono definiti da:
- D.Lgs. 18 aprile 2016, n. 50, relativo all'attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE e il riordino della disciplina vigente in materia di aggiudicazione di appalti pubblici e contratti pubblici di lavori, forniture e servizi;
- D.Lgs. 15 novembre 2011, n. 208, relativo ai contratti pubblici per lavori, servizi e forniture nei settori della difesa e sicurezza, in attuazione della direttiva 2009/81/CE.

[30] Il monitoraggio dei contratti è stato introdotto con l'art.13, comma 2, del D.Lgs. 39/1993 e successivamente novellato nell'art. 14-*bis*, comma 2, let. h) del CAD, che attribuisce all'AgID le funzioni di definire criteri e modalità per regolamentare le attività di monitoraggio. L'Agenzia, inoltre, svolge azioni di verifica sulla conduzione del monitoraggio effettuato dalle PA.

[31] La nomina è obbligatoria; le caratteristiche e le funzioni della figura sono descritte nella citata Circ. n. 1/2021 (cfr. para 3.1. e 5.1.).

[32] In particolare, la Circolare specifica competenze nel contesto normativo, *best practise*, in ambito dell'IT e della qualità dei servizi, *project management*, sicurezza delle informazioni, *data protection*, qualità e metriche del *software*.

con una metodologia strutturata in relazione allo sviluppo contrattuale e rendicontate all'AgID nelle modalità e nei termini prescritti dalla Circolare, alla quale si rinvia per tutti gli approfondimenti sulle procedure attuative. In linea generale, i principali adempimenti che riguardano l'amministrazione possono essere di seguito riassunti:

- nomina del RdM e comunicazione all'AgID;
- approntamento della lista dei contratti da sottoporre al monitoraggio (da pubblicarsi sul sito dell'Amministrazione), del documento di *screening* e relative comunicazioni all'AgID;
- preparazione del *piano di monitoraggio* e comunicazione all'AgID;
- esecuzione delle azioni del piano, relazionando periodicamente l'RTD sullo stato dell'arte con rapporti periodici sul monitoraggio effettuato;
- segnalazione al Responsabile Unico del Procedimento/Direttore di Esecuzione Contrattuale delle informazioni ritenute utili, ovvero rilievi e misure correttive eventualmente da applicare nei confronti dei fornitori;
- se richiesto, trasmettere all'AgID, in qualità di Organismo verificatore, le informazioni sul monitoraggio in corso o concluso. In tale contesto, l'AgID potrà fornire adeguato supporto tecnico e formativo per il personale che l'Amministrazione impiega nel monitoraggio.

3.6 Implementazione delle misure minime di sicurezza ICT in ambito A.D. (MMS).

L'AgID, con la Circolare 18 aprile 2017, n. 2 "*Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015)*»"[33], in ottemperanza a quanto disposto dalla Direttiva della PCM in titolo, ha emanato le disposizioni per l'immediata implementazione di varie misure di sicurezza informatica da parte di tutte le PA. Vista l'elevata frequenza a cui i sistemi informatici delle PA sono bersaglio di eventi di natura cibernetica[34], la Circolare intende fornire alle amministrazioni delle misure/controlli tecnici, per verificare ed eventualmente irrobustire, la cornice di sicurezza dei propri sistemi ICT e scongiurare l'accadimento dei più tipici eventi informatici.

L'RTD, in esito ad una serie di tavoli tecnici condotti congiuntamente ai Referenti del settore Interforze e delle F.A., ha definito un *iter* procedurale per l'applicazione della Circolare e ha emanato le *Linee guida per l'implementazione delle misure minime di sicurezza ICT in ambito A.D.* (LG), documento che armonizza il processo di implementazione delle MMS in tutto il Comparto.

Le attività e le procedure relative all'implementazione delle MMS sono descritte sia nella Circolare di AgID, sia nelle LG di SMD VI.

In generale, i Referenti delle AOO del settore Interforze e delle F.A. sono responsabili nei confronti dell'RTD per l'implementazione delle MMS sui sistemi ICT della propria area di competenza (cfr. LG), che avviene tramite i propri Centri di Esercizio/Reparti C4, sia per i sistemi a gestione centralizzata che per i sistemi in gestione locale. Analogamente, gli Enti/UO delle predette AOO che gestiscono localmente sistemi informativi dedicati a specifiche esigenze sono responsabili, nei confronti dell'RTD e del Referente dell'area, per l'implementazione delle misure tramite il loro referente informatico locale/responsabile EAD locale (o figura analoga) dell'Ente/UO. A tal riguardo, i Referenti delle AOO, acquisiscono dagli Enti/UO della propria area le informazioni sullo stato di implementazione delle misure per quei specifici sistemi gestiti localmente, al fine di avere un quadro completo sulla sicurezza ed eventualmente individuare, in un'ottica di razionalizzazione delle risorse, criticità e possibili interventi a fattor comune.

Le AOO/UO/Enti, secondo le modalità indicate nelle LG, almeno annualmente, sono tenuti alla compilazione o aggiornamento della documentazione prescritta dalla Circolare di AgID e redigono una relazione sullo stato dell'implementazione delle MMS da inoltrare all'RTD.

---

[33] A causa di varianti normative occorse durante il procedimento di approvazione e pubblicazione in Gazzetta Ufficiale, la Circolare 17 marzo 2017, n. 1 "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*" è stata sostituita, quasi immediatamente, dalla Circolare n. 2/2017, aggiornata.

[34] Intesi come incidenti, attacchi, malfunzionamenti.

Per garantire un maggiore rispondenza al quadro normativo in vigore, soprattutto nell'attuazione dei controlli relativi alla valutazione delle vulnerabilità[35], le LG contemplano l'esecuzione di attività di *vulnerability assessment* e *penetration test* ove, queste ultime, sono generalmente effettuate dal Comando per le Operazioni in Rete (COR), quale organismo di riferimento per la cybersicurezza in ambito Difesa. Ciò consente alle MMS di allinearsi alle norme concernenti il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), in considerazione che determinati sistemi/servizi potrebbero rientrare nell'annovero dei cosiddetti "*beni ICT*", considerati fondamentali per l'esercizio di funzioni/servizi essenziali per gli interessi dello Stato (vds. paragrafo seguente).

Si precisa che, in esito all'andamento delle nuove minacce emergenti, le MMS sono costantemente suscettibili di revisione e aggiornamento sia da parte dell'AgID, sia dalle disposizioni che, eventualmente, potrebbero essere emanate dall'ACN[36], al fine di garantire una migliore sicurezza per i sistemi e i dati in essi contenuti.

3.7 Perimetro di sicurezza nazionale cibernetica (PSNC).

Il PSNC nasce per garantire una solida cornice di sicurezza agli assetti ICT denominati *beni*[37], gestiti sia delle PA/Enti pubblici sia operatori privati, che consentono lo svolgimento di funzioni o servizi ritenuti essenziali per gli interessi dello Stato e, dal cui malfunzionamento, interruzione o compromissione, ne deriverebbe un pregiudizio per la sicurezza nazionale. Il PSNC è stato istituito con la norma generale del D.L. n. 105/2019[38] (c.d. *Decreto perimetro*) che rimanda ad apposite disposizioni in materia, veicolate da Decreti della PCM e da apposito D.P.R., con cui vengono definite, fra l'altro:

- le modalità e i criteri per l'individuazione dei soggetti e relativi beni da includere nel Perimetro;
- le procedure per l'acquisizione e le verifiche tecniche per la validazione e certificazione dei beni;
- le particolari misure di sicurezza da applicare al perimetro;
- la costituzione della rete di organismi preposti alle attività di certificazione.

L'A.D., quale Dicastero operante nel settore governativo della difesa:

- rientra fra i *soggetti* inclusi nel PSNC[39];
- partecipa, con i rappresentanti dell'Ufficio di Gabinetto del Ministro della Difesa e di SMD VI, al Tavolo Interministeriale istituito a supporto del Comitato Interministeriale per la Cybersicurezza[40] per l'attuazione delle attività previste dal Perimetro.

In tale contesto, l'RTD per gli aspetti di sua competenza, in coordinazione con le strutture del COR relativamente alla gestione della sicurezza *cyber*[41], è la figura deputata a supportare il CHOD nella centralità del ruolo assegnato e nelle responsabilità che ne derivano[42]. Infatti,

---

35 Cfr. misura ABSC 4 "*Valutazione e correzione continua della vulnerabilità*".

36 Con il D.L. 14 giugno 2021, n. 82, convertito in L. 4 agosto 2021, n. 109, viene costituita l'Agenzia per la Cybersicurezza Nazionale, quale Ente responsabile per tutte le attività concernenti la cybersicurezza in ambito nazionale. Con apposito regolamento sono definite le competenze che rimangono attestate alla diretta responsabilità dell'ACN e quelle che resteranno in capo all'AgID.

37 Ai sensi dell'art. 1, comma 1, del D.L. 21 settembre 2019, n. 105 (convertito dalla L. 133/2019), si intendono quegli assetti ICT (reti, sistemi, servizi) "*…da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale* …". Si rinvia alla specifica normativa di settore (DPCM e Regolamento attuativo).

38 D.L. 21 settembre 2019, n. 105, convertito dalla L. 133/2019.

39 Con la comunicazione della PCM - Dipartimento delle Informazioni per la Sicurezza (DIS), prot. n. 0187669 D002/V4000/4.1.13 in data 21/12/2020, il Capo di SMD nella sua veste di Autorità responsabile della pianificazione, della predisposizione e dell'impiego delle F.A. nel loro complesso (art. 26 del COM), è stato nominato quale "*Soggetto*" per l'esercizio delle funzioni essenziali assolte dalla Difesa.

40 Art.4 del D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109.

41 In esito alla *vision* espressa dal Capo di SMD (cfr. f.n. 1/193 del 21 luglio 2020 "*Relazioni funzionali fra il Comando per le Operazioni in Rete (CORDIFESA) e le corrispondenti articolazioni di F.A.*"), rappresenta il principale riferimento dell'A.D. per gli aspetti *cyber* militari, svolgendo anche le funzioni di *CERT Difesa*.

42 Art. 1, commi 9, 14, del D.L. 105/2019.

l'implementazione del perimetro necessita un'azione di direzione delle attività e armonizzazione delle procedure, non soltanto sull'area di Vertice Interforze, ma anche sugli SM di F.A..

In esito alle disposizioni del CAD, in ordine all'indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica[43], l'RTD ha:

- disposto l'attivazione di un Tavolo Tecnico con la partecipazione di tutte le articolazioni Referenti del Comparto, per curare gli approfondimenti specifici riguardanti le incombenze relative all'implementazione del Perimetro e in relazioni alle diverse competenze coinvolte;
- integrato le procedure delle LG per l'implementazione delle MMS, sulla base delle disposizioni tecniche di sicurezza da applicare ai *beni ICT*, introducendo anche indirizzamenti generali relativi allo svolgimento delle attività di *vulnerability assessment* e *penetration testing*. Tali attività sono svolte, rispettivamente, le prime sotto la responsabilità del COR e delle F.A. per ciascun ambito di competenza, mentre le seconde ricadono sotto la responsabilità del COR per tutto l'ambito Difesa, ovvero delle F.A. qualora ne abbiano le capacità tecniche per attuarle;
- costituito punto di contatto verso l'ACN, divulgando ai Referenti interessati tutte le comunicazioni e le disposizioni dell'Agenzia relative all'implementazione del perimetro.

Infine, si precisa che, in esito a recenti modifiche introdotte al *Decreto perimetro*, l'ACN assume tutte le funzioni in materia di cybersicurezza relative al PSNC[44].

3.8 Accessibilità agli strumenti informatici.

Fra i compiti attribuiti all'RTD troviamo le incombenze relative all'*accessibilità* agli strumenti informatici dell'amministrazione di appartenenza, ove per accessibilità si intende la capacità dei sistemi informatici di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

In attuazione delle normative del settore europee e nazionali[45], AGID ha emanato le *Linee Guida sull'Accessibilità degli strumenti informatici* (LGA)[46] che indirizzano le PA all'erogazione di servizi sempre più accessibili ed inclusivi. Per quanto sopra, le amministrazioni hanno l'obbligo di compilare e pubblicare:

- entro *il 31 marzo di ogni anno*, gli *obiettivi di accessibilità* (OdA) relativi all'anno corrente e lo stato di attuazione del piano per l'utilizzo del telelavoro[47];
- entro *il 23 settembre di ogni anno*, la *Dichiarazione di Accessibilità* (DdA) per ogni sito *web* e applicazione mobile.

3.8.1 Obiettivi di Accessibilità.

Detti obiettivi si estrinsecano come interventi/azioni/provvedimenti che ogni amministrazione deve intraprendere al fine di rendere i propri siti *web* accessibili, in tutte sezioni e nei contenuti pubblicati; fra questi, sono contemplati anche gli interventi tecnici volti al mantenimento, revisione o rifacimento completo dell'architettura del sito o di parti di esso, adeguamento strutturale o riscrittura dei contenuti, nonché le attività rivolte alla formazione/informazione del personale impiegato nella pubblicazione dei contenuti o nella gestione dei portali. Al fine di supportare le PA nell'attività di definizione e pubblicazione degli OdA, sul sito dell'AgID è disponibile l'apposita applicazione "Obiettivi di accessibilità" che consente di redigere l'elenco da pubblicare secondo le norme vigenti. A tal riguardo:

- il *Webmaster* dall'Ufficio Pubblica Informazione e Comunicazione (UPICOM) dell'Ufficio di diretta collaborazione del Ministro della Difesa, in qualità responsabile supervisore e promotore delle attività relative alla pubblicazione dei contenuti su tutti i portali dell'A.D.,

[43] Art. 17, comma 1, let. c).

[44] Ai sensi dell'art. 7, commi 1, let. f), h), i), l), del D.L. 14 giugno 2021, n. 82, convertito con L. 4 agosto 2021, n. 109.

[45] Direttiva UE 2016/2102 elativa all'*accessibilità dei siti web e delle applicazioni mobili degli enti pubblici*, recepita con il D.Lgs. 10 agosto 2018, n. 106 "*Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici*".

[46] In vigore dal 10 gennaio 2020.

[47] Come stabilito dalle LGA, cap. 4, para. 2, e D.L. n. 179/2012, art. 9, comma 7, convertito dalla L. 221/2012.

colleziona le esigenze, in termini di OdA, dell'Uff. di Gabinetto, degli UPICOM del settore Interforze e delle F.A., ne definisce le priorità d'intervento in un Requisito Tecnico Operativo che trasmette al RTD annualmente per l'approvazione/finanziamento;
- la Sez. Supporto RTD provvede a redigere un punto di situazione per l'RTD sui risultati finora raggiunti e sulle attività dell'anno in corso che, come OdA, si intendono pubblicare ed attuare;
- a seguito dell'approvazione da parte dell'RTD si avvierà l'iter tecnico-amministrativo volto all'individuazione della Ditta aggiudicataria per le attività di assistenza sistemistica dei portali.

Successivamente, la Sezione Supporto RTD:
- provvede a registrare gli OdA sul portale di AgID;
- riceve, a seguito delle verifiche effettuate dall'Agenzia, un *link* di collegamento necessario alla pubblicazione e visualizzazione degli OdA;
- inoltra la richiesta per la pubblicazione sul sito *web* dell'A.D. del *link* inviato dall'AgID al Webmaster e, per conoscenza, alla struttura preposta alla Prevenzione della Corruzione e Trasparenza (PCT) presso BILANDIFE[48].
  In esito al benestare formulato da parte della citata struttura per PCT[49], il *Webmaster* provvederà alla pubblicazione e ad informare la Sezione Supporto RTD.

3.8.2 Dichiarazione di Accessibilità.

La DdA è lo strumento attraverso il quale le Amministrazioni rendono pubblico lo stato di conformità ai requisiti di accessibilità di ciascun sito *web* e applicazione mobile di cui sono titolari; la sua pubblicazione rappresenta un preciso obbligo di legge[50]. La DdA viene redatta, oppure aggiornata, e pubblicata entro il 23 settembre di ogni anno, a seguito di una analisi effettuata dalle amministrazioni sulle condizioni di accessibilità dei propri siti *web* e applicazioni mobili. Analogamente a quanto avviene per gli OdA, la procedura di pubblicazione viene eseguita e validata esclusivamente in modalità telematica su un portale di AgID[51], che rilascia la dichiarazione compilata in maniera conforme ai disposti normativi.

A tal riguardo, l'RTD ha già emanato disposizioni[52] al fine di coordinare ed uniformare la procedura in parola per tutti gli UPICOM dell'A.D. Dette disposizioni contemplano, in linea generale, l'attuazione delle alcune attività:
- a monte della pubblicazione, gli UPICOM, dovranno:
  - effettuare preventivamente le verifiche di accessibilità dei siti *web* e delle applicazioni mobili adottando le metodologie, i criteri di valutazione e le verifiche tecniche di conformità ai requisiti di accessibilità[53];
  - implementare e rendere disponibile sul sito un *Meccanismo di feedback*[54], che dovrà essere indicato all'interno della Dichiarazione, per consentire agli utenti di segnalare eventuali casi di inaccessibilità;
  - redigere la bozza della DdA[55] con i dati richiesti da AgID, per ciascun sito *web* o applicazione mobile di responsabilità, ed inviarla allo SMD VI;

---

48 Ufficio Centrale del Bilancio e degli Affari Finanziari della Difesa.

49 Gli OdA si collocano nell'ambito delle misure che favoriscono la trasparenza degli enti pubblici, ai sensi del D.Lgs. 14 marzo 2013. n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da patte delle pubbliche amministrazioni*", e sono pubblicati nella sezione dei siti: "*Amministrazione Trasparente\Altri contenuti\accessibilità e dati aperti*".

50 Art. 3-*quater*, della L. 9 gennaio 2004, n. 4 "*Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*" e s.m.i., apportate dal D.Lgs. 106/2018.

51 Il portale è raggiungibile all'indirizzo: https://form.agid.gov.it/.

52 Con lettera prot. n. M_D SSMD REG2021 0020736 del 3 febbraio 2021.

53 L'AgID, per agevolare il lavoro alle PA, mette a disposizione il *Modello di Autovalutazione di accessibilità*, in Allegato 2 alle LGA, utile per determinare lo stato di conformità di ogni sito *web* e/o applicazione mobile per i quali la dichiarazione viene redatta e il cui esito può determinare una situazione di *conformità*, *parziale conformità* o *non conformità*.

54 Il Meccanismo di feedback può essere una *mail* o un *form online* che si è scelto di utilizzare per consentire agli utenti di segnalare eventuali casi di inaccessibilità. Per maggiori approfondimenti (https://www.agid.gov.it/it/design-servizi/accessibilita).

55 In allegato 1 alle LGA è riportato il *Modello di dichiarazione di accessibilità*, da utilizzare come guida.

– la Sezione Supporto RTD, provvede a:
  · raccogliere le bozze delle dichiarazioni dagli UPICOM, entro i termini stabiliti dalle disposizioni emanate;
  · compilare sul portale telematico dell'AgID le rispettive DdA, sulla base dei dati pervenuti;
  · ricevere i *link* di pubblicazione ed inoltrarli ai referenti dei rispettivi UPICOM, che provvederanno a inserirli sui siti/applicazioni;
  · accertarsi dell'avvenuta pubblicazione ed informare l'RTD.

L'AgID notifica le comunicazioni istituzionali e i *link* di collegamento solo all'RTD, sulla casella di posta elettronica registrata sull'IPA[56].

[56] Indice delle Pubbliche Amministrazioni, ai sensi della citata Circ. n. 3/2018.

4. SISTEMI INFORMATICI E TRATTAMENTO DEI DATI PERSONALI

4.1 Introduzione.

A decorrere dal 25 maggio 2018, il *Regolamento (UE) 2016/679 del 27 aprile 2016 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (Regolamento), anche noto come *General Data Protection Regulation* (GDPR), trova integrale applicazione nei Paesi membri dell'Unione europea, con contestuale abrogazione della previgente Direttiva 95/46/CE del 24 ottobre 1995, che aveva costituito, fino ad allora, la base giuridica di riferimento per le legislazioni nazionali nella materia.

Pertanto, al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento, in attuazione dell'art. 13 della L. 25 ottobre 2017 n. 163 (legge di delegazione europea), sono stati adottati provvedimenti volti ad adattare il diritto interno al citato Regolamento, con l'emanazione del D.Lgs. 10 agosto 2018, n. 101, che modifica ed integra il Codice nazionale in materia di *privacy* (D.Lgs. 30 giugno 2003 n. 196).

Analogamente alle altre PA, anche la Difesa si è conformata alla nuova legislazione e, tenendo conto anche dei chiarimenti espressi dall'autorità Garante, ha posto in essere vari adempimenti che hanno portato a definire un nuovo assetto dispositivo e organizzativo in materia di *privacy*, ridisegnato secondo i principi del nuovo Regolamento. Per tali aspetti, si rimanda alle norme e alle disposizioni generali emanate nell'ambito del Comparto Difesa e a quelle dei singoli Titolari che trattano dettagliatamente la materia[57].

4.2 Utilizzo dei sistemi informatici nel trattamento dei dati personali.

Le attività di trattamento dei dati personali che avvengono con modalità informatiche e/o per via telematica, utilizzano sistemi informatici/servizi telematici che, sia nelle fasi di progettazione e sviluppo, sia in quelle di utilizzo e gestione, devono tener conto di:

- valutazioni d'impatto sui trattamenti effettuate dal Titolare[58], specialmente se utilizzano tecnologie di nuova introduzione, che devono essere partecipate ai responsabili del settore ICT per la corretta messa a punto dello strumento informatizzato;
- rischi che possono derivare, in modo accidentale o doloso, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione o dall'accesso non autorizzati, dei dati personali trasmessi, conservati o comunque trattati.

Fatti salvi gli obblighi prescritti dalle norme di legge e le disposizioni interne alla Difesa, i sistemi informatici/telematici che trattano dati personali devono poter consentire:

- l'esercizio dei diritti degli interessati, nei limiti stabiliti dal Regolamento[59];

---

[57] In particolare, si citano le seguenti normative valide per l'A.D. e le disposizioni dell'AOO del Titolare di SMD:
- Decreto Ministro della Difesa 28 marzo 2018 recante la nomina del Responsabile per la Protezione dei Dati della Difesa (RPD). Trattasi del primo Decreto istitutivo e di nomina del RPD;
- Decreto Ministro della Difesa 18 novembre 2020 recante l'individuazione dei soggetti Titolari per il trattamento dei dati personali e dei loro compiti;
- Direttiva sulla protezione dei dati personali del RPD, diramata allo SMD con lettera prot. n. M_D SSMD REG2021 0039603 in data 2 marzo 2021;
- Ordine di Servizio n. I/001 in data 8 luglio 2021 del Capo di SMD, diramato con lettera n. M_D SSMD REG2021 0131113 in data 14 luglio 2021;
- Manuale "Misure di sicurezza tecniche e organizzative, con valutazione d'impatto sulla protezione dei dati personali", emanato dal Titolare di SMD in data 7 ottobre 2021;
- Manuale "Procedura da adottare in caso di violazione di dati personali (*data breach*)", del Titolare di SMD in data 7 ottobre 2021.

[58] Art. 35 del Regolamento (UE) 2016/679.

[59] Gli artt. da 15 a 22 del Regolamento (UE) 2016/679 elencano i diritti degli interessati, mentre l'art. 23 tratta delle limitazioni sulla portata degli obblighi e dei diritti anzidetti.

- l'accesso ai dati personali sia agli interessati che ai soli autorizzati, tramite sistemi di accesso/autenticazione protetti e restrittivi, in ragione delle rispettive funzioni istituzionali secondo una la visione dei dati "a cono d'ombra" su quanto di reale interesse;
- l'acquisizione dei soli dati necessari e finalizzati allo specifico trattamento (minimizzazione);
- l'utilizzo di funzioni di controllo automatizzato che assicurino la correttezza e la validità dei dati già in fase di inserimento/acquisizione;
- l'integrità per il tempo necessario al conseguimento delle finalità di trattamento, ovvero durante il periodo di conservazione nei limiti indicati dall'informativa;
- l'applicazione delle misure di protezione informatica e di quelle indicate dal Titolare;
- l'acquisizione e la suddivisione dei dati secondo categorie, per una migliore ottimizzazione delle risorse ed interoperabilità fra applicativi gestionali;
- il ripristino tempestivo della disponibilità e dell'accesso al dato in caso di incidente fisico o tecnico.

Unitamente ai suddetti aspetti, strettamente connessi alla progettazione, sviluppo, gestione del sistema ai vari livelli/settori di competenza, l'impiego dello strumento informatizzato deve essere supportato anche da ulteriori attività da parte dell'organizzazione preposta, fra le quali:

- definizione delle politiche di gestione ed utilizzo in sicurezza dei sistemi/servizi informatici non classificati e revisione periodica delle direttive emanate al riguardo[60], attività di *policy* univoca per tutto il Comparto, a cura dell'RTD;
- preparazione dei piani atti a garantire la continuità di funzionamento dei sistemi/servizi informatici deputati ad assicurare l'operatività dei processi vitali dell'Amministrazione (*business continuity plan* e *disaster recovery plan*), a cura del COR e Centri C4 di esercizio;
- predisposizione per l'attuazione delle procedure, emanate dai Titolari, relative alla gestione degli incidenti della sicurezza informatica, che possono causare violazione/*data breach*[61], a cura del COR e Centri C4 di esercizio;
- verifica e aggiornamento periodico delle misure di sicurezza informatiche adottate, a cura del COR e Centri C4 di esercizio, sotto monitoraggio da parte del RTD;
- definizione dei piani di formazione del personale autorizzato e dei gestori dei sistemi informativi, limitatamente all'utilizzo degli applicativi, a cura del RTD, per i sistemi a fattor comune dell'A.D. e dell'interforze, a cura degli SM di F.A./Centri C4, per le attività specialistiche dell'area di competenza.

4.3 Misure di sicurezza, tecniche ed organizzative relative ai sistemi ICT.

I dati costituiscono un patrimonio fondamentate per tutte le organizzazioni e in particolare, per gli aspetti relativi alla salvaguardia dei diritti e della libertà delle persone fisiche, lo sono quelli personali, specialmente se messi a sistema fra loro, in quanto costituiscono informazioni da tutelare. I sistemi informatici non classificati in esercizio presso l'A.D., attraverso i quali vengono effettuate molteplici attività di trattamento dei dati personali, debbono pertanto:

- garantire, in una cornice di sicurezza intesa come riservatezza, integrità ed affidabilità, il dato in tutte le sue forme di rappresentazione (analogica e digitale) e durante tutto il suo ciclo di vita[62];
- consentire la disponibilità dei dati agli interessati e a quanti necessitano di accedervi.

Stante la necessità, ai sensi del Regolamento, di identificare e valutare le minacce e i rischi che possono compromettere la protezione dei dati personali, sussiste l'obbligo da parte del Titolare[63] di implementare misure tecniche ed organizzative per assicurare un adeguato livello di sicurezza

[60] In particolare, le Direttive SMD-I-024 – ed. 2021, SMD-I-003 – ed. 2017.
[61] Per l'AOO dello SMD, cfr. il citato *Manuale "Procedura da adottare in caso di violazione di dati personali (data breach)"*, emanato dal Titolare di SMD
[62] Acquisizione, trattamento/elaborazione, conservazione/archiviazione, cancellazione o trasferimento ad altro Titolare.
[63] Art. 24, comma 1, del Regolamento *Responsabilità del titolare del trattamento*.

e limitare i rischi connessi al trattamento in modalità informatica/telematica/automatica, secondo i principi di *security by design/by default*.

Sebbene l'identificazione delle minacce, la valutazione dei rischi e l'implementazione delle misure tecniche ed organizzative[64] siano responsabilità afferenti al Titolare, nell'ambito di un trattamento eseguito con modalità informatica/telematica/automatizzata, appare plausibile ed auspicabile che venga stabilito un canale collaborativo fra il Titolare stesso e l'RTD in merito alle caratteristiche funzionali e di sicurezza informatica del sistema da utilizzare, soprattutto se il trattamento implica l'utilizzo di un nuovo sistema in fase di progettazione/sviluppo o implichi l'utilizzo di tecnologie di nuova introduzione.

Ciò è motivato delle responsabilità attribuite all'RTD, fra cui quelle relative a:

- la definizione delle linee di indirizzo per lo sviluppo e l'impiego della rete e dei sistemi non classificati dell'A.D.;
- le attività di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica su dati, sistemi e infrastrutture;
- la pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione[65].

In virtù delle predette responsabilità, al fine di garantire il corretto utilizzo e gestione dei sistemi/servizi informatici, sia da parte degli utenti, sia da parte degli amministratori o dai responsabili preposti ai vari livelli, l'RTD ha diramato una serie di disposizioni indispensabili a fornire la corretta cornice di protezione all'intera info-struttura dell'A.D. Tali disposizioni sposano gli indirizzi indicati dal Regolamento e dalle Direttive interne sul trattamento, costituendo una base stabile per la definizione delle misure di sicurezza tecniche e organizzative a cui il Titolare può riferirsi. In particolare:

- Direttiva SMD–I–024 "*La gestione in sicurezza dei servizi informatici non-classificati dell'Amministrazione Difesa*" – ed. 2021. Scopo del documento è quello di delineare, a beneficio degli amministratori dei sistemi informatici non classificati dell'A.D., i criteri organizzativi, procedurali e tecnici fondamentali da porre in essere, al fine di conseguire un livello di sicurezza adeguato all'attuale minaccia cibernetica. Il documento è corredato da Appendici, a firma del Comandante del COR, alla luce della loro spinta caratterizzazione tecnica e dei frequenti aggiornamenti cui sono soggette. La Direttiva, inoltre, tiene conto delle determinazioni dell'Autorità Garante sui ruoli del personale impiegato come amministratore di sistema[66];
- Direttiva SMD-I-003 "*Disciplinare per l'utilizzo dei servizi informatici non classificati erogati in ambito Difesa, quali i servizi di posta elettronica, instant messaging ed accesso ad Internet*", ed. 2017. Il Disciplinare è uno strumento finalizzato ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT e definisce:
  - le modalità di utilizzo dei servizi informatici non classificati cui gli utenti devono attenersi, con particolare riferimento a quelli di accesso ad *Internet*, ai servizi di posta elettronica e di *instant messaging*;
  - le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità delle informazioni trattate con i servizi anzidetti;

---

64 Per gli approfondimenti sull'argomento si rimanda alle specifiche disposizioni emanate dai Titolari di ogni AOO/UO; es. il Manuale "*Misure di sicurezza tecniche e organizzative, con valutazione d'impatto sulla protezione dei dati personali*" – ed. 2021, emanato dal Titolare dello SMD.

65 Fermo restando quanto indicato dal Regolamento UE 2019/881 del 17 aprile 2019 *relativo all'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione*, gli acquisti del materiale informatico per la PA sono regolamentati anche dalle Linee Guida di AgID "*La sicurezza nel procurement*" – ed. 2020, che definiscono indicazioni tecnico-amministrative per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.

66 Provvedimento del 27 novembre 2008, "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", modificato con provvedimento del 25 giugno 2009, "*Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento*".

– *Linee Guida per l'implementazione delle "Misure Minime di Sicurezza ICT" in ambito A.D. - ai sensi della Circolare 18 aprile 2017, n. 2 di AgID*, con le quali è stata diramata la Circolare di AgID (trattata nella Parte Terza "Procedure" del presente documento). Le misure elencate nella Circolare di AgID, armonizzate dalle LG ed implementate in tutta l'A.D., rispondono a molte indicazioni dettate dal Regolamento e costituiscono un fondamento imprescindibile ed efficace da applicare per la sicurezza comune. Per quanto non possa essere considerata una soluzione esaustiva per tutte le tipologie di trattamenti, rappresenta comunque, uno strumento certificato per garantire un consapevole livello di sicurezza dei sistemi informatici preposti al trattano dati personali[67].

4.4 Le figure di riferimento dell'ICT nel trattamento e protezione dei dati personali.

a. Il Responsabile della Transizione Digitale dell'A.D.

L'RTD definisce le procedure per l'utilizzo e la gestione in sicurezza anche per i sistemi ICT non classificati della Difesa che trattano dati personali. In tale contesto, di concerto con il COR quale organismo deputato alla implementazione della cornice di cybersicurezza dell'A.D.:

- recepisce le direttive/circolari in materia di trattamento dei dati personali emanate dal RPD e da SMD in qualità di Organismo Titolare;
- definisce, in termini concettuali e di esigenza, gli strumenti informatici in attuazione a quanto previsto dal Regolamento e dalle Direttive interne;
- analizza i sistemi informativi gestionali che trattano dati personali, al fine di verificarne la *compliance* al Regolamento, individuarne le criticità e favorirne il processo di adeguamento;
- stabilisce, anche sulla base dell'analisi del rischio effettuata dal Titolare, gli indirizzamenti sulle misure di sicurezza informatica (fisiche, logiche e procedurali) da adottare sui sistemi informativi, al fine di garantire ai Titolari un livello di sicurezza adeguato per ciascun trattamento, nonché prevenire e contrastare eventi informatici che possano portare alla sottrazione, alterazione, cancellazione dei dati o interruzione del servizio[68];
- fornisce, eventualmente se richiesto dal Titolare, consulenza sulle caratteristiche e sulla configurazione dei sistemi, sulle misure tecniche di sicurezza informatica applicate o da implementare relativamente ai sistemi che gestiscono dati personali;
- approva le procedure di controllo, elaborate dal COR per l'Area Interforze, tese a verificare e valutare periodicamente:
  - l'efficacia e la resilienza delle misure di sicurezza informatica adottate sui sistemi informativi gestionali che trattano dati personali[69];
  - la capacità di ripristinare tempestivamente la continuità operativa dei sistemi, nonché il mantenimento dell'integrità e l'accesso ai dati personali a seguito di incidente informatico;
  - la predisposizione degli elementi necessari a comunicare al Titolare (o a più Titolari in caso di sistema condiviso), con la dovuta tempestività, eventuali violazioni o sospette violazioni dei dati personali[70].

b. I Referenti dell'RTD.

Il Referente, in virtù dei compiti attribuiti:

[67] A tal riguardo, l'applicazione della Circolare è richiamata anche nelle disposizioni diramate dal Titolare di SMD.
[68] Ai sensi degli artt. 32 e 35 del Regolamento (UE) 2016/679.
[69] *Vulnerability assessment* e *penetration test* – cfr. Parte 3 – Procedure.
[70] Cfr. le procedure indicate nel *Manuale "Procedura da adottare in caso di violazione di dati personali (data breach)"*, emanato dal Titolare di SMD in data 7 ottobre 2021.

- è garante, all'interno della propria AOO/UO, dell'applicazione delle disposizioni di cui alle Direttive del RPD e del Titolare ai fini dell'implementazione, sviluppo e gestione dei sistemi/servizi di propria competenza;
- attua le disposizioni emanate dal RTD, in particolare:
  - la citata Direttiva SMD-I-024;
  - la Circolare 18 aprile 2017 n. 2/2017 di AgID "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni", secondo le procedure indicate dalle LG di SMD VI;
- dirama, se necessario, ulteriori disposizioni di dettaglio al personale con le funzioni di amministratore di sistema, o che riveste funzioni chiave nella gestione dei sistemi/servizi di rete[71] in conformità alle Direttive predette;
- verifica che, in caso di variazioni organizzative, siano adottate le procedure indicate dalla suddetta Direttiva, in particolare per le nomine d'incarico;
- riceve, dal rispettivo Comando C4/Centro di Esercizio/Referente Informatico locale, le comunicazioni relative ad ogni violazione o sospetta violazione per la protezione dei dati personali e la segnala al Titolare, ovvero ai Titolari qualora la violazione o la sospetta violazione interessi l'ambito di un sistema informatico utilizzato da più AOO/UO.

Per lo svolgimento dei suoi compiti, il Referente si avvale della collaborazione del Comando C4/Centro di Esercizio relativo alla propria AOO/UO e del Referente informatico locale di ciascun EDR dipendente.

c. Il Referente Informatico locale.

Il *Referente Informatico locale* è il responsabile del funzionamento e gestione dei sistemi informatici in uso presso l'UO di appartenenza e rappresenta l'interfaccia della struttura nei confronti del Referente.

Svolge i compiti generali conferiti con l'atto di nomina[72] nel rispetto delle disposizioni emanate dal Referente e delle procedure definite dal proprio Comando C4/Centro di Esercizio. In particolare:

- controlla, sotto il profilo tecnico, il corretto funzionamento della rete e dei servizi/applicativi di sua competenza, specie quelli preposti al trattamento dei dati personali;
- assicura l'implementazione delle misure di sicurezza informatica, di cui alla Circolare di AgID, dandone periodico riscontro al Referente nelle modalità indicate dalle LG del RTD;
- adotta, compatibilmente con le risorse a sua disposizione, tutte le misure idonee per prevenire l'utilizzo illecito della rete e dei servizi di rete, salvaguardando opportunamente i *server* e le postazioni di lavoro/strumenti informatici ed effettuando un costante monitoraggio degli stessi;
- implementa, sulla base delle procedure definite dal Comando C4/Centro di Esercizio, le procedure di controllo sulle proprie strutture di competenza;
- segnala al Referente ogni violazione o sospetta di violazione della sicurezza informatica.

d. L'Amministratore di Sistema.

Gli Amministratori di Sistema (Amministratori) sono figure professionali essenziali per la sicurezza e la corretta gestione dei sistemi informatici. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere ai dati personali trattati con strumenti elettronici. Per tale motivo la figura di Amministratore di Sistema è stata regolamentata anche da specifico Provvedimento dell'Autorità Garante[73], che individua gli

[71] Ai sensi della Direttiva SMD – I – 024 – Annesso 1 "*Procedura per la gestione in sicurezza dell'attuale architettura dei sistemi ICT non classificati*".

[72] Per gli approfondimenti si rimanda agli Allegati/Appendici della Direttiva SMD-I-024.

[73] Provvedimento del Garante del 27 novembre 2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", come modificato dal provvedimento del 25 giugno 2009,

Amministratori di Sistema, non solo le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, altresì quelle figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di *database*, di sistemi di *networking*, di sistemi di sicurezza informatica, di sistemi *SW* complessi, ecc...
Gli Amministratori sono nominati mediante apposito atto di nomina. I requisiti, i compiti e le modalità di nomina degli Amministratori di Sistemi sono regolamentati dalle prescrizioni indicate nella Direttiva SMD-I-024, eventualmente integrate da specifiche disposizioni in materia di *privacy* emanate dal Titolare del trattamento.