queste istituzioni

Procurement di beni e servizi ICT in ambito pubblico e normative regolamentari in tema di digitalizzazione della PA, *privacy* e *cybersecurity*.

Luca Tufarelli

Numero 2/2021
30 luglio 2021

Procurement di beni e servizi ICT in ambito pubblico e normative regolamentari in tema di digitalizzazione della PA, *privacy* e *cybersecurity*

di Luca Tufarelli*

Sommario

Sintesi

L'approvvigionamento di beni e servizi nel settore dell'*information and communications technology* ("ICT") in ambito pubblico deve avvenire nel rispetto del D.Lgs. n. 50/2016 e ss.mm.ii ("Codice dei contratti pubblici" o "CCP") oltre che in conformità con gli obiettivi definiti dal Piano triennale per l'informatica nella P.A. ("Piano triennale"), nonché alla normativa in materia di *e-government*, privacy e cybersecurity.
Il presente contributo, senza alcuna pretesa di esaustività, offre una breve rassegna degli obblighi e *constraints* che i soggetti pubblici devono rispettare nell'acquisto e nella gestione delle risorse informatiche in ambito pubblico. L'ultimo paragrafo fornisce un contributo conclusivo come proposta operativa per semplificare l'impianto normativo e garantire i risultati attesi in termini di semplificazione e digitalizzazione della azione amministrativa.

Abstract

The procurement of goods and services in the Information and Communications Technology sector (ICT) within the public sphere must follow the Legislative Decree no. 50/2016 and the subsequent amendments ("Code of public contracts" or "CCP"). It should be also in accordance with the objectives defined by the three-year plan for information technology in the Public Administration ("Three-year plan"), as well as the legislation on e-government, privacy, and cybersecurity.

* Avvocato, Foro di Roma.

This contribution offers a brief review of the obligations and constraints that the public entities must comply when purchasing and managing IT resources within the public sphere. The last paragraph provides a final contribution, as an operational proposal, aiming at simplifying the regulatory system and ensuring the expected results in terms of simplification and digitization of the administrative action.

Parole chiave
ICT; digitalizzazione; Public Procurement; e-government; cybersecurity.

1. *Procurement* di beni e servizi ICT.

1.1. Centralizzazione degli acquisti in ambito ICT.

Le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione[1]sono tenute ad acquisire beni e servizi informatici e di connettività esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip S.p.a. o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi. Sono fatti salvi «gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente[2]». Pertanto, qualora non sussistano obblighi specifici di acquisto centralizzato, le amministrazioni potranno ricorrere agli strumenti di acquisto e di negoziazione disponibili presso Consip ed i soggetti aggregatori. Fra i detti strumenti sono ricompresi le convenzioni-quadro, i contratti-quadro e gli accordi-quadro nonché il Mercato elettronico della pubblica amministrazione ("MEPA"), il Sistema Dinamico della Pubblica Amministrazione ("SDAPA") e le gare su delega che aggregano la domanda di più amministrazioni.

Il comma 516 dell'art. 1 della Legge di stabilità 2016 ammette la deroga ai suddetti obblighi solamente in casi tassativi ossia:

a) qualora il bene o il servizio non sia disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione, ovvero

b) in casi di necessità ed urgenza comunque funzionali ad assicurare la continuità della gestione amministrativa.

---

[1] Come individuate dall'Istituto nazionale di statistica ("ISTAT"), ai sensi dell'art. 1 commi 512-520 della l. 28 dicembre 2015, n. 208 ("Legge di stabilità 2016").

[2] Si veda, ad esempio, la disciplina dell'acquisto di beni e servici ICT in ambito sanitario di cui all'art. 1, co. 548-549 della Legge di stabilità. Sul punto si veda anche la Circolare AgID n. 1 del 26 giugno 2016. Più in generale in materia di contratti pubblici appare, qui, utile rinviare, *ex multis*, in dottrina alle recenti riflessioni sviluppate in A. MEALE (*a cura di*), *Manuale breve di diritto dei contratti pubblici*, Pacini Editore, Pisa, 2020, p. 7 ss.; F. ARMENANTE, *Le procedure di affidamento dei contratti pubblici*, Milano, Giuffrè, 2020, p. 3 ss.;D. BOLOGNINO - H. BONURA - A. STORTO (*a cura di*), *I contratti pubblici dopo il Decreto semplificazioni. Le principali novità in materia di contratti pubblici, responsabilità, controlli, procedimento e processo, tra emergenza e sistema "a regime"*, La Tribuna, Piacenza, 2020, p. 1 ss.; R. DIPACE, *Manuale dei Contratti Pubblici*, Giappichelli, Torino, 2021, p. 65 ss.; L. DELPINO, F. DEL GIUDICE, *Manuale di Diritto Amministrativo*, Edizioni Giuridiche Simone, Napoli, 2021, p. 623 ss.

Gli approvvigionamenti effettuati in deroga (*ex* comma 516) devono comunque essere autorizzati[3] dall'organo di vertice amministrativo nonché comunicati all'ANAC e all'Agenzia per l'Italia Digitale (di seguito "AgID" o "Agenzia") e la mancata osservanza delle disposizioni dettate in materia può rilevare ai fini della responsabilità disciplinare e per danno erariale (comma 517). Inoltre,ai sensi dell'art. 1, comma 1 del D.L. 6 luglio 2012, n. 95 s.m.i., i contratti stipulati in violazione degli obblighi di acquisto centralizzato sono nulli, salvo il conseguimento di un comprovato risparmio di spesa.

Ricordiamo, infatti, che l'obiettivo degli acquisti centralizzati è quello di «garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività» e di realizzare «un risparmio di spesa annuale»[4].

1.2. Art. 75 del Decreto "Cura Italia"[5].

Ulteriori deroghe, seppur temporanee, sono state introdotte in questo particolare periodo storico dalla disciplina emergenziale per agevolare la diffusione dello *smart-working* e favorire la fruibilità di servizi *online* a vantaggio di cittadini e imprese[6]. In particolare, fino al 31 dicembre 2021[7], l'art. 75 del Decreto Cura Italia consente alle amministrazioni aggiudicatrici (di cui all'art. 3 CCP), nonché alle autorità amministrative indipendenti, ivi comprese la CONSOB e COVIP, di acquistare beni e servizi informatici, preferibilmente basati sul modello *cloud SaaS* (*software as a service*),e servizi di connettività mediante procedura negoziata senza previa pubblicazione di un bando di gara *ex* art. 63, comma 2,lett. c), del Codice dei contratti pubblici,

---

[3] La Circolare n.2 del 26 gennaio 2016 chiarisce che tale autorizzazione motivata debba essere resa al momento dell'avvio della procedura di affidamento e, dunque, al momento dell'adozione della determina a contrarre. In tale momento andrà, pertanto, valutata la disponibilità o la compatibilità delle tempistiche preventivate da Consip e dai soggetti aggregatori per la messa a disposizione del bene/servizio rispetto ai fabbisogni della stazione appaltante, oltre ovviamente alla idoneità del bene/servizio. Le pubbliche amministrazioni, nell'ambito di tali acquisti di beni e servizi informatici, devono comunque adottare gli standard vigenti (in particolare: le Linee Guida di design per i siti web della PA, le regole di interoperabilità previste da SPC, le regole descritte al paragrafo 3, lett. c. Ecosistemi della Circolare) e attenersi a quanto disposto dal comma 516 per le comunicazioni, inviandole in via anticipata.

[4] Cfr. art. 1, co. 512-515, L. 28 dicembre 2015, n. 208. In dottrina si rimanda, *ex plurimis,* alle brillanti ricostruzioni recentemente sviluppate in C. BENETAZZO, *ANAC e sistema europeo dei Contratti Pubblici*, Torino, Giappichelli, 2020, p. 102 ss.

[5] D. L. 17 marzo 2020, n. 18 convertito con modificazioni dalla L. 24 aprile 2020, n. 27.

[6] Per utili riflessioni sul punto si leggano F. FRACCHIA, P. PANTALONE, *La fatica di semplificare: procedimenti a geometria variabile, amministrazione difensiva, contratti pubblici ed esigenze di collaborazione del privato responsabilizzato*,in *Federalismi.it,* n. 36/2020, pp. 33-70; A. CELOTTO, *Emergenza e pubblica amministrazione*, in *Rivista AIC,* n. 1/2021, pp. 422-432; F. CINTOLI, *Il decreto semplificazioni (decreto legge n. 76 del 2020), gli appalti pubblici e il riparto di giurisdizione*, in *Federalismi.it*, n. 7/2021, pp. 80-104; M.COZZIO - N. PARISI, *L'emergenza sanitaria causata dal COVID-19: l'impatto (attuale e futuro) sul sistema nazionale dei contratti pubblici*, in *Il diritto dell'economia,* n. 1/2021, pp. 37-73.

[7] Il termine inizialmente fissato al 31 dicembre 2020, è stato esteso al 31 dicembre 2021 dal D. L. 31 dicembre 2020, n. 183 convertito in legge dalla L. 26 febbraio 2021, n. 21 (cd. Decreto Mille proroghe).

selezionando l'affidatario tra almeno quattro operatori economici, di cui almeno una start-up o PMI innovativa.

In deroga al Codice dei contratti pubblici, l'art. 75 citato prevede inoltre che la verifica sul possesso dei requisiti in capo all'aggiudicatario sia sostituita da una autocertificazione dell'operatore economico e che il contratto sia stipulato immediatamente con contestuale avvio dell'esecuzione, senza necessità di rispettare il termine di *standstill*[8].

Gli acquisti effettuati tramite la predetta procedura negoziata«devono essere relativi a progetti coerenti con il Piano triennale per l'informatica nella pubblica amministrazione» e gli interventi di sviluppo e implementazione dei sistemi informativi devono prevedere, ove possibile, l'integrazione con le piattaforme abilitanti previste dal d. lgs. 7 marzo 2005, n. 82 ("Codice dell'Amministrazione Digitale" o "CAD")[9].

1.3. L'art. 53 del Decreto Semplificazioni-*bis*[10].

Il recente Decreto Semplificazioni-*bis* ha introdotto importanti novità in materia di procedure di *e-procurement* e acquisto di beni e servizi informatici al fine di realizzare gli obiettivi di trasformazione digitale previsti dal Piano Nazionale di Ripresa e Resilienza ("PNRR").[11]

In particolare, l'art. 53 prevede una serie di misure specifiche volte a semplificare e velocizzare i predetti acquisti di beni e servizi informatici.

1.3.1. Procedure d'acquisto semplificate.

Tra le misure di maggior rilievo si segnala innanzitutto che, in relazione ai predetti acquisti, è confermata la facoltà di ricorrere all'affidamento diretto per tutti gli appalti di valore inferiore alla soglia di rilevanza comunitaria[12]. In relazione agli appalti sopra soglia, invece, è previsto il ricorso alla procedura negoziata senza bando *ex* art. 63 del Codice dei Contratti Pubblici, richiamata dall'art. 48, comma 3, del medesimo decreto[13], per gli affidamenti finalizzati

[8] Il termine di *stand still* è previsto dall'art. 32, comma 9 del Codice dei contratti pubblici.

[9] Piattaforma tecnologica per l'interconnessione tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati (cfr. art. 5 del CAD); Anagrafe nazionale della popolazione residente – ANPR (cfr. art. 62 del CAD); Sistema pubblico per la gestione dell'identità digitale di soggetti giuridici – SPID (cfr. 64 del CAD) e Accesso telematico ai servizi della pubblica amministrazione (cfr. art. 64-bis del CAD).

[10] D.L. 31 maggio 2021, n. 77.

[11] Il PNRR all'interno della Missione 1, Componente 1 "Digitalizzazione, innovazione e sicurezza nella P.A.", reca tra le riforme 1.1., una specifica misura consistente nell'innovazione dell'impianto normativo per velocizzare gli appalti ICT, con specifico riferimento agli appalti strumentali alla realizzazione degli obbiettivi dello stesso PNRR. Per consultare il PNRR cfr. https://www.governo.it/sites/governo.it/files/PNRR.pdf.

[12] L'art. 53 rinvia all'art. 1, comma 2, lett. a) del D.L. 16 luglio 2020, n. 76 conv. nella Legge 11 settembre 2020, n. 120 che prevede la possibilità di ricorrere all'affidamento diretto per gli appalti di lavori, servizi e forniture inferiori alla soglia comunitaria individuata per il biennio 2020-2021 in 214.000 euro.

[13] L'art. 48, comma 3, statuisce che«Le stazioni appaltanti possono altresì ricorrere alla procedura di cui all'articolo 63 del decreto legislativo n. 50 del 2016, per i settori ordinari, e di cui all'articolo 125, per i settori

all'acquisto di beni e servizi informatici basati sulla tecnologia *cloud*, la cui determina a contrarre o altro atto di avvio del procedimento equivalente sia adottato entro il 31 dicembre 2026. Il ricorso a tale procedura è ammesso anche ove ricorra la rapida obsolescenza tecnologica delle soluzioni disponibili tale da non consentire il ricorso ad altra procedura di affidamento (comma 1).

È inoltre previsto che le amministrazioni possano stipulare il contratto e dare avvio all'esecuzione del servizio, previa acquisizione di un'autocertificazione dell'operatore economico aggiudicatario attestante il possesso dei requisiti, richiamando la previsione di cui all'art. 75 del Decreto Cura Italia, facendo tuttavia salvi gli obblighi eurounitari di *stand still* a cui invece la citata disposizione (al suo secondo comma) derogava.

1.3.2. Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri.

Infine, il citato art. 53 attribuisce al Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri il potere di coordinare gli acquisti ICT strettamente finalizzati alla realizzazione del PNRR, garantendo il rispetto del cronoprogramma dei singoli progetti della Missione 1[14],nonché la compatibilità tecnologica e infrastrutturale dei progetti di trasformazione digitale, mediante pareri obbligatori e vincolanti sugli elementi essenziali delle procedure di affidamento e potendo guidare le amministrazioni aggiudicatrici con prescrizioni riguardanti l'oggetto, le clausole principali, i tempi e le modalità di acquisto (commi 3 e 4).

1.3.3. Banca Dati dei Contratti Pubblici e pubblicazione degli atti delle procedure.

L'art. 53, comma 5 del Decreto Semplificazioni-*bis* apporta delle modifiche ad alcune disposizioni del Codice dei Contratti Pubblici.

Tra le modifiche apportate si segnala innanzitutto l'ampliamento dell'ambito di operatività degli obblighi di pubblicazione previsti dall'art. 29 del Codice dei Contratti Pubblici anche alla fase dell'esecuzione del contratto.

È previsto, inoltre, che tutte le informazioni relative alla programmazione, alla scelta del contraente, all'aggiudicazione ed esecuzione delle opere saranno gestite e trasmesse alla Banca Dati dei Contratti Pubblici dell'Autorità Nazionale Anticorruzione (ANAC) attraverso l'impiego di piattaforme informatiche interoperabili che le amministrazioni saranno obbligate ad

---

speciali, nella misura strettamente necessaria, quando, per ragioni di estrema urgenza derivanti da circostanze imprevedibili, non imputabili alla stazione appaltante, l'applicazione dei termini, anche abbreviati, previsti dalle procedure ordinarie può compromettere la realizzazione degli obiettivi o il rispetto dei tempi di attuazione di cui al PNRR nonché al PNC e ai programmi cofinanziati dai fondi strutturali dell'Unione Europea».

[14] In particolare la digitalizzazione, innovazione e sicurezza della PA (M1C1), unitamente alla semplificazione dell'azione amministrativa rappresenta una delle riforme centrali del PNRR (cfr. §2A le riforme) insieme ai temi della Innovazione, Competitività, Cultura e Turismo (Missione 1).

utilizzare. L'interscambio dei dati avverrà nel rispetto del principio di unicità del luogo di pubblicazione e di unicità di invio delle informazioni, in conformità alle Linee guida AgID in materia di interoperabilità[15].

All'interno della Banca Dati dei Contratti Pubblici verrà istituito il fascicolo virtuale dell'operatore economico, nel quale saranno conservati tutti i dati e le informazioni necessarie ai fini della partecipazione alle procedure di gara, rendendo in tal modo più semplice le attività di verifica e controllo *ex* artt. 80, 83 e 84 del Codice dei Contratti Pubblici, da parte delle stazioni appaltanti. Queste ultime dovranno avere requisiti di qualità in termini di esperienza pregressa documentata, personale qualificato e strumentazione tecnica adeguata.

1.4. Acquisti di servizi ICT tramite Sogei S.p.A.

L'art. 51 del D.L. 26 ottobre 2019, n. 124[16] consente ad alcune amministrazioni[17]di acquisire da Sogei S.p.A.,[18] sulla base di apposite convenzioni IT, i servizi informatici strumentali al raggiungimento dei rispettivi obiettivi, come meglio specificati dal secondo comma della disposizione in questione, al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, la sinergia tra processi istituzionali, il consolidamento delle infrastrutture, la razionalizzazione dei sistemi informativi e l'interoperabilità tra le banche dati.

1.5. *In House Providing.*

Tra le modalità di *procurement,* il CCP prevede l'*in house providing*, che consente alla pubblica amministrazione di affidare a proprie società *in house* beni, servizi e lavori (c.d. "autoproduzione"), anziché rivolgersi al mercato, in deroga alle regole sull'evidenza pubblica.

Ai sensi dell'art. 5 del CCP, il ricorso all'*in house providing* è consentito qualora

a) l'amministrazione aggiudicatrice o l'ente aggiudicatore esercita sulla persona giuridica di cui trattasi un controllo analogo a quello esercitato sui propri servizi;

b) oltre l'80% delle attività della persona giuridica controllata è effettuata nello svolgimento dei compiti ad essa affidati dall'amministrazione aggiudicatrice controllante o da

[15] Cfr. Circolare AgID n. 1 del 9 settembre 2020 recante «Linea di indirizzo sull'interoperabilità tecnica» e relativi allegati. Con Provvedimento dell'8 luglio 2021 [doc. web n. 9682994] si segnala che il Garante per la Protezione dei Dati Personali ha espresso parere favorevole sugli schemi, predisposti dall'AgiD, di Linee Guida sull'interoperabilità tecnica delle pubbliche amministrazioni e di Linee Guida su tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici.

[16] D.L. 26 ottobre 2019, n. 124 convertito in legge con L. 19 dicembre 2019, n. 157 recante: «Disposizioni urgenti in materia fiscale e per esigenze indifferibili».

[17] Ad oggi, Presidenza del Consiglio dei Ministri, Consiglio di Stato, Avvocatura dello Stato, INVIMIT S.p.A., PagoPA S.p.A., Comando generale del Corpo delle capitanerie di porto e Ministero dell'istruzione.

[18] Società di Information Technology interamente partecipata dal Ministero dell'Economia e delle Finanze.

altre persone giuridiche controllate dall'amministrazione aggiudicatrice o da un ente aggiudicatore di cui trattasi;

c) nella persona giuridica controllata non vi è alcuna partecipazione diretta di capitali privati, ad eccezione di forme di partecipazione di capitali privati (le quali non comportano controllo o potere di veto) previste dalla legislazione nazionale, in conformità dei trattati, che non esercitano un'influenza determinante sulla persona giuridica controllata.

Ai fini dell'affidamento *in house* di servizi disponibili sul mercato in regime di concorrenza, le stazioni appaltanti effettuano una valutazione preventiva sulla congruità economica dell'offerta dei soggetti *in house*, avuto riguardo all'oggetto ed al valore della prestazione. Nella motivazione del provvedimento di affidamento devono altresì dare atto delle ragioni del mancato ricorso al mercato, nonché dei benefici per la collettività della forma di gestione prescelta, anche con riferimento agli obiettivi di universalità e socialità, di efficienza, di economicità e di qualità del servizio, nonché di ottimale impiego delle risorse pubbliche[19].

1.6. Appalti innovativi.

Un particolare strumento di approvvigionamento di servizi ICT è costituito dai cd. "appalti innovativi"[20] che si distinguono a loro volta in (i) appalti pre-commerciali o *pre-commercial procurement*(PCP) e(ii) appalti di soluzioni innovative o *public procurement of innovation*.

Si tratta di procedure previste dalla legislazione comunitaria e nazionale con cui la P.A. esprime al mercato il proprio fabbisogno in termini funzionali, in modo che gli operatori interessati possano proporre la soluzione più in linea con le sue esigenze.

Gli "appalti innovativi" quindi consistono in:

a) Appalti pre-commerciali (PCP): prevedono l'acquisto da parte della PA del processo di innovazione, quindi di servizi di ricerca e sviluppo. In particolare,l'acquirente pubblico (i) acquista i servizi di ricerca e sviluppo di prodotti, servizi o processi non ancora esistenti, (ii) indica le sue esigenze e (iii) incoraggia le imprese e i ricercatori a sviluppare prodotti, servizi o processi innovativi che rispondano alle sue esigenze. L'appalto pre-commerciale è escluso dall'ambito di applicazione della direttiva 2014/24/UE[21].

b) Appalti di soluzioni innovative (PPI):prevedono l'acquisto da parte della PA di prodotti innovativi creati da terzi: l'acquirente pubblico, invece di acquistare un prodotto già

[19] Cfr. art. 192, comma 2, del Codice dei contratti pubblici.

[20] All'art. 3, lett. nnnn) del Codice dei Contratti pubblici "l'innovazione" è definita come: «l'attuazione di un prodotto, servizio o processo nuovo o che ha subito significativi miglioramenti, tra cui quelli relativi ai processi di produzione, di edificazione o di costruzione o quelli che riguardano un nuovo metodo di commercializzazione o organizzativo nelle prassi commerciali, nell'organizzazione del posto di lavoro o nelle relazioni esterne». Per un breve inquadramento sugli appalti innovativi cfr. https://www.agid.gov.it/it/agenzia/appalti-innovativi.

[21] Considerando (47) e art. 14 direttiva 2014/24/UE.

disponibile in commercio, assume il ruolo di utente pioniere e acquista un prodotto, un servizio o un processo ancora sconosciuto al mercato e contraddistinto da caratteristiche fondamentalmente innovative. La Direttiva 24/2014/UE disciplina integralmente il PPI, quindi per tali appalti può essere utilizzata qualsiasi procedura d'appalto prevista dalla disciplina europea.

Secondo le indicazioni della Commissione Europea[22], la PA può ricorrere agli "appalti per l'innovazione" per le seguenti finalità: acquisire servizi pubblici di migliore qualità ad un prezzo ottimale; far fronte a nuove esigenze; modernizzare i servizi pubblici; promuovere l'avvio e la crescita di start-up e di PMI innovative.

Un ruolo strategico nella promozione e nello sviluppo del *procurement* d'innovazione è affidato ad AgID che:

- promuove la definizione e lo sviluppo di grandi progetti strategici di ricerca e innovazione connessi alla realizzazione dell'Agenda digitale italiana;

- può svolgere il ruolo di stazione di committenza ausiliaria per l'esecuzione di appalti di innovazione, a favore delle Regioni e delle altre pubbliche amministrazioni che ne facciano richiesta;

- gestisce il centro di competenza territoriale sugli appalti di innovazione a supporto delle pubbliche amministrazioni italiane.

2. E-Government.

Il *procurement* di beni e servizi ICT è regolato, altresì, dalle norme in materia di *e-government*.

Il CAD[23] e la Legge di stabilità 2016 attribuiscono all'AgID il compito di definire il Piano triennale per l'Informatica nella Pubblica Amministrazione, che si propone principalmente di contribuire alla diffusione delle nuove tecnologie digitali incentivando l'innovazione dei servizi pubblici. A tal fine, il Piano triennale delinea una serie di azioni che le amministrazionie l'AgID, ognuno nell'ambito di rispettiva competenza,dovranno realizzare nel triennio di riferimento.

Per il raggiungimento di tali obiettivi, il CAD attribuisce all'AgID poteri necessari ad acquisire dalle amministrazioni i dati e le informazioni utili al monitoraggio sulla spesa in ambito ICT e alla razionalizzazione delle risorse informatiche nel settore pubblico. All'Agenzia è altresì attribuito il potere di adottare Linee Guida contenenti regole tecniche e di indirizzo per l'attuazione del CAD.

La disciplina dettata da AgID è rivolta a tutti gli enti che rientrano nel campo di applicazione del CAD, ossia:

---

[22] Comunicazione della Commissione "Orientamenti in materia di appalti per l'innovazione" C (2018) 3051 final del 15.5.2018.

[23] Cfr. artt. 14 e 14 bis comma 2, lettera b).

a) le pubbliche amministrazioni di cui all'articolo 1, comma 2,del D.lgs. 30 marzo 2001, n. 165[24], ivi comprese le autorità di sistema portuale, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;

b) i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;

c) le società a controllo pubblico, ossia le società in cui una o più amministrazioni pubbliche esercitano poteri di controllo i sensi dell'art. 2359 c.c. Il controllo può sussistere anche quando, in applicazione di norme di legge o statutarie o di patti parasociali, per le decisioni finanziarie e gestionali strategiche relative all'attività sociale è richiesto il consenso unanime di tutte le parti che condividono il controllo[25]. Sono escluse le società quotate a partecipazione pubblica che non rientrino nella categoria di cui alla lettera b).

Esulano dal campo di applicazione del CAD l'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché le comunicazioni di emergenza e di allerta in ambito di protezione civile.

2.1. Il *Cloud* della P.A.

In coerenza con gli obiettivi posti dal Piano triennale 2017-2019, l'AgID, in collaborazione con il *Team* per la Trasformazione Digitale, ha dato vita al progetto per il *Cloud* della P.A.[26]in merito all'uso di infrastrutture e servizi di *cloud computing* all'interno della Pubblica Amministrazione[27].

In tale ambito, l'AgID ha censito il patrimonio ICT della Pubblica Amministrazione, al fine di classificare le PA in base alle caratteristiche delle rispettive infrastrutture fisiche[28]. In particolare, sono stati individuate:

---

[24] Tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al d. lgs. 30 luglio 1999, n. 300.

[25] Art. 2, lett. b) e lett. m) del D.lgs. 19 agosto 2016, n. 175 (Testo unico in materia di società a partecipazione pubblica).

[26] Cfr. "Il Cloud della PA" AgID - Team Digitale del 19 novembre 2018.

[27] Per una più ampia ricostruzione si legga, in particolare, V. PAGNANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della "(big) data governance" pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto,* n. 1/2021, pp. 13-28.

[28] Al riguardo si leggano le più generali considerazioni maturate in C. BENETAZZO, *ICT [Information and communications technology - Tecnologie dell'informazione e della comunicazione] e nuove forme di interazione tra cittadino e Pubblica Amministrazione*, in *Rivista di diritto dei media,* n. 2/2020, pp. 262-273.

(i) le infrastrutture idonee ad essere elette dalla Presidenza del Consiglio dei Ministri come Poli Strategici Nazionali ("P.S.N.")[29],ossia soggetti giuridici controllati dallo Stato che hanno a disposizione un numero ridotto di *data center* nazionali in grado di garantire il funzionamento dei servizi cruciali del Paese attraverso standard di sicurezza, qualità ed efficienza;

(ii) i *data center* del Gruppo "A", ossia i *data center* che presentano requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo. Essi non potranno agire come P.S.N., ma potranno eventualmente proporre allo stesso P.S.N. di utilizzare le proprie risorse per gestire alcuni dei suoi servizi;

(iii) i *data center* del Gruppo "B", che includono i *data center* con carenze strutturali e/o organizzative o che non garantiscono la continuità dei servizi nonché le infrastrutture che non hanno partecipato al censimento e che devono essere dismessi per migrare al *Cloud* della P.A..

Quello della PA costituisce un modello *cloud* misto che include infrastrutture e servizi di tipo *private cloud*, *public cloud* e *community cloud*.

I P.S.N. sono in grado di erogare ad altre amministrazioni servizi di *private cloud* in maniera continuativa e sistematica, inclusi servizi infrastrutturali *on-demand*, *disaster recovery* e *business continuity*, ma anche di gestione della sicurezza IT e assistenza tecnica.

Per quanto riguarda i servizi di *public cloud*, con decorrenza dal 1° gennaio 2019 le amministrazioni possono acquisire esclusivamente i servizi *IaaS*, *PaaS* e *SaaS* resi da *cloud service provider* ("C.S.P."),qualificati da AgID[30] sulla base di specifici requisiti di sicurezza dei sistemi e delle informazioni e nella misura in cui offrano sufficienti garanzie di portabilità contro il rischio di *lock-in*. Una volta qualificati, tali servizi sono esposti sul*Marketplace Cloud*, una piattaforma che consente di visualizzare la scheda tecnica di ogni servizio mettendo in evidenza le caratteristiche, il costo e i livelli di servizio dichiarati dal fornitore in sede di qualificazione, nonché le modalità con cui uno specifico servizio potrà essere acquisito, rimandando allo strumento di *procurement* disponibile (ad esempio, il portale *acquistinretepa.it*).

L'infrastruttura di tipo *community cloud*, invece, è realizzata dal Raggruppamento Temporaneo d'Imprese aggiudicatario del Contratto Quadro Consip SPC Cloud - Lotto 1 nei confronti delle amministrazioni aderenti.

Anche il P.N.R.R., in linea con gli obiettivi perseguiti negli ultimi anni dall'AgID (e confluiti nei Piani triennali), pone l'accento sulla necessità di perseguire un approccio *cloud first* quale strumento di trasformazione digitale della P.A. In particolare,proseguirà il processo di razionalizzazione e consolidamento dei *data center* distribuiti sul territorio e la trasformazione sarà attuata secondo due modelli complementari: le amministrazioni centrali, infatti, in

[29] Circolare AgID n. 5 del 20 luglio 2018.
[30] Circolare AgID n. 2 del 9 aprile 2018Circolare AgID n. 3, del 9 aprile 2018.

funzione dei requisiti di *performance* e scalabilità e della sensibilità dei dati e dei servizi coinvolti, potranno migrare verso:

(i) un P.S.N., definito dal P.N.R.R. come «nuova infrastruttura dedicata cloud (completamente "privata" o "ibrida"), localizzata sul territorio nazionale e all'avanguardia in prestazioni e sicurezza»;

(ii) oppure sul *public cloud* di uno tra gli operatori di mercato precedentemente certificati.

Per facilitare il processo di migrazione al *cloud*, il P.N.R.R. prevede un programma di supporto e incentivo per trasferire basi dati e applicazioni secondo una logica definita «*migration as a service*».

Le amministrazioni saranno accompagnate sin dalla fase di analisi tecnica e di definizione delle priorità, con risorse specializzate nella gestione amministrativa, nonché nella contrattazione del supporto tecnico esterno necessario all'attuazione e, più in generale, saranno supportate nell'attività complessiva di *project management* per tutta la durata della trasformazione. A tal fine saranno predisposti dei "pacchetti" standard di supporto che ogni P.A. potrà combinare a seconda delle esigenze specifiche.

Per favorire la migrazione al *cloud* e conseguire i correlati risparmi di spesa in ambito ICT, il P.N.R.R. prevede disincentivi per le amministrazioni che non avranno effettuato la migrazione dopo un "periodo di grazia" predefinito e che siano riviste le regole di contabilità che attualmente scoraggiano e complicano la migrazione. L'obbiettivo primario del PNRR, e prim'ancora dei Piani Triennali, è quello di evitare spese in conto capitale per acquistare *data center*, macchinari e servizi correlati, ma di operare in flessibilità privilegiando spese operative scalabili a seconda della bisogna. Insomma, comprare risorse e servizi scalabili da chi fa della fornitura delle piattaforme il suo business principale[31].

2.2. Acquisti e investimenti sui *Data Center.*

Con Circolare n. 1 del 14 giugno 2019, l'AgID ha fornito indicazioni sugli specifici obblighi correlati agli acquisti IT in ambito pubblico.

Coerentemente con gli obiettivi di razionalizzazione del patrimonio ICT della P.A., l'Agenzia ha ribadito quanto già stabilito con la Circolare n. 2 del 26 giugno 2016, prevedendo che le amministrazioni non possono effettuare spese o investimenti in materia di *data center*, ma possono acquisire beni e servizi ICT per i *data center* già in uso,purché finalizzati esclusivamente ad (i) evitare problemi di interruzione di pubblico servizio (inclusi gli interventi

[31] Come precisato nel PNRR, al momento la migrazione al *cloud* comporta di "tradurre" l'investimento *capex* in *opex*, cioè spese operative flessibili e scalabili.

necessari a garantire la sicurezza dei dati e dei sistemi) e (ii) anticipare processi di dismissione dei propri *data center* per migrare al Cloud della P.A.

Tali acquisti sono soggetti ad un preciso obbligo di comunicazione ad AgID, declinato diversamente a seconda del valore dell'acquisto. In particolare:

- qualora il valore economico per la spesa o investimento in beni e servizi ICT sia pari o inferiore alla soglia comunitaria (fissata per il biennio 2020-2021 in 214.000,00 euro), le amministrazioni comunicano ad AgID il fabbisogno qualificato e il relativo valore economico, nonché le motivazioni a fondamento dell'acquisto;

- qualora tale valore superi la soglia comunitaria, la comunicazione dovrà essere altresì corredata da una specifica relazione contenente la puntuale descrizione tecnico-economica degli interventi che comportano la spesa e/o l'investimento sul *data center*. Se entro 30 giorni dal ricevimento della nota, l'amministrazione non riceve richieste di chiarimenti e/o integrazioni da parte dell'AgID, la spesa o l'investimento potranno ritenersi approvati.

2.3. Le Linee Guida AgID.

L'acquisto e la gestione di servizi e risorse ICT in ambito pubblico sono altresì soggetti al rispetto delle raccomandazioni e *best practices* definite dalle Linee Guida dell'AgID.

In particolare, a titolo esemplificativo:

- le Linee Guida su «La sicurezza nel procurement ICT» forniscono alle amministrazioni e ai fornitori indicazioni tecnico-amministrative per garantire che le procedure di *procurement* si svolgano nel rispetto di standard minimi in materia di *privacy* e di sicurezza cibernetica;

- il documento «Misure minime di sicurezza ICT per le pubbliche amministrazioni» fornisce alle amministrazioni un riferimento pratico per la valutazione e il miglioramento del livello di *cybersecurity*, mediante l'implementazione di controlli di natura tecnologica, organizzativa e procedurale per valutare il proprio livello di sicurezza informatica e prevenire le minacce più frequenti ai propri sistemi. Le misure sono diversificate seconda della complessità del sistema informativo e della realtà organizzativa dell'amministrazione interessata e possono essere implementate in modo graduale seguendo tre livelli di attuazione (minimo, standard e avanzato);

- le «Linee Guida su acquisizione e riuso di *software* per le pubbliche amministrazioni»danno attuazione alle previsioni degli artt. 68 e 69 del CAD, che incentivano l'utilizzo di soluzioni software *open source* in ambito pubblico, secondo la politica del "riuso", salvo che nei settori più delicati del governo digitale nazionale che potrebbero essere esposti a rischio dalla condivisione e gestione di soluzioni *software* di tipo aperto (ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali).

2.4. Il monitoraggio sull'esecuzione dei contratti IT.

Con la Circolare n. 1/2021, approvata con determinazione n. 79 del 20 gennaio 2021, l'AgID ha definito i criteri e le modalità con cui le amministrazioni effettuano il monitoraggio sull'esecuzione dei contratti.

Come chiarito dall'Agenzia, il monitoraggio consiste in un insieme di attività e processi finalizzato a supportare l'amministrazione nella gestione e nel miglioramento della *governance* dei contratti IT e che mira a costruire uno standard per la verifica e il controllo dei propri sistemi informativi. Secondo la recente circolare, il monitoraggio dovrà avere ad oggetto i contratti IT che:

a) abbiano un valore, al netto di IVA, superiore a 10 milioni di euro, ovvero, in caso di contratti con validità pluriennale, superiore a 2,5 milioni di euro in media ogni anno, incluse le relative proroghe e gli eventuali atti aggiuntivi;

b) si riferiscano a servizi che interessino la sicurezza dello Stato, la difesa nazionale, l'ordine e la sicurezza pubblica, lo svolgimento di consultazioni elettorali nazionali ed europee, indipendentemente dalle dimensioni economiche sopra indicate;

c) indipendentemente dalle dimensioni economiche, abbiano un rilevante impatto sotto il profilo organizzativo o dei benefici che si prefiggono di conseguire e che l'AgID ritenga necessario sottoporre a monitoraggio;

d) rientrino tra gli obiettivi ed i risultati attesi che le singole Amministrazioni sono invitate a realizzare per contribuire concretamente al Piano Triennale dell'Informatica per la PA.

e) in caso di adesione a contratti quadro, o altre procedure CONSIP, il monitoraggio si applica a tutti i piani dei fabbisogni richiesti dall'Amministrazione, se il valore complessivo di detti piani dei fabbisogni, al netto di IVA, è superiore a 10 milioni di euro;

f) in caso di affidamenti *in-house*, il monitoraggio si applica direttamente a tutti gli affidamenti, se il valore complessivo è superiore, al netto di IVA, a 5 milioni di euro annui.

In ogni caso, le amministrazioni possono sottoporre al monitoraggio anche ulteriori tipologie di contratti, in base alle proprie necessità, per una migliore *governance* complessiva delle proprie iniziative di informatizzazione.

La circolare ribadisce la necessità che le amministrazioni provvedano a nominare formalmente un Responsabile del Monitoraggio che operi a supporto dell'Ufficio del Responsabile della Transizione Digitale[32], con il compito di coordinare le attività di

[32] L' articolo 17 del CAD obbliga tutte le amministrazioni a individuare un ufficio per la transizione alla modalità digitale – il cui responsabile è il Responsabile della Transizione Digitale (RTD) – a cui competono le attività e i processi organizzativi ad essa collegati e necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità. Con la Circolare n. 3 del 1° ottobre 2018, adottata dal Ministro per

monitoraggio e di interfacciarsi con l'AgID e i fornitori, avvalendosi di un *team* di risorse con competenze specifiche.

È prevista la possibilità di esternalizzare le attività di monitoraggio mediante procedura di gara per l'affidamento del servizio a società esterne, fermo restando, in ogni caso, la direzione e la responsabilità delle attività in capo al Responsabile.

Le attività del Gruppo di monitoraggio si articolano in diverse fasi, finalizzate alla pianificazione del monitoraggio, alla rilevazione e valutazione delle criticità e alla rendicontazione delle attività svolte per la definizione di piani di rientro con i fornitori, al fine di risolvere le vulnerabilità eventualmente rilevate.

L'AgID effettuerà delle analisi a campione sul monitoraggio operato dalle amministrazioni, con possibilità di esprimere pareri, richiedere chiarimenti o formulare consigli nei casi in cui siano rilevate criticità o non conformità gravi, nonché su richiesta dell'amministrazione interessata.

3. Disciplina in materia di privacy e cybersecurity.

L'acquisto, lo sviluppo e l'implementazione di risorse ICT in ambito pubblico presuppongono il rispetto della normativa nazionale ed europea in materia di *privacy* e di *cybersecurity*[33].

3.1. Normativa privacy.

La disciplina di riferimento è costituita dal Regolamento generale per la protezione dei dati personali dell'Unione Europea 2016/679 ("G.D.P.R.") e dal d. lgs. n. 196/2003 e s.m.i. ("Codice Privacy"), nonché dalle indicazioni contenute nei provvedimenti e atti di indirizzo adottati dalle autorità nazionali ed europee competenti in materia.

In generale, il trattamento di dati personali in ambito pubblico può essere effettuato in base ad una norma di legge o, nei casi previsti dalla legge, di una fonte normativa secondaria, cioè un regolamento. Anche la comunicazione di tali dati tra diversi titolari[34], per l'esercizio di

---

la Pubblica Amministrazione, tutte le amministrazioni pubbliche sono state sollecitate a individuare al loro interno un RTD.

[33] *Ex multis*, in dottrina, C. BENETAZZO, *ICT [Information and communications technology - Tecnologie dell'informazione e della comunicazione] e nuove forme di interazione tra cittadino e Pubblica Amministrazione*, cit., pp. 262-273;G. PEROTTO, *La standardizzazione europea nel settore dell'ICT nell'era dell'"Internet of Things": qualificazione giuridica e controllo di validità degli standard tecnici armonizzati*, in *Il diritto dell'economia*, n. 3/2020, pp. 757-771; B.BRUNO, *"Cybersecurity" tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Federalismi.it*, n. 14/2020, pp. 11-45.

[34] Ai sensi dell'art. 4, par. 1, n. 7 del GDPR "titolare del trattamento" è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

pubblici poteri o di compiti di interesse pubblico, può avvenire solo in caso di previsione normativa o, in mancanza, se il Garante per la Protezione dei Dati Personali (di seguito "Garante") non abbia espresso osservazioni nel termine di 45 giorni sulle misure da adottare a tutela degli interessati, cioè dei cittadini coinvolti.

Il G.D.P.R. non impone che vi sia un atto legislativo specifico per ogni singolo trattamento, altrimenti si correrebbe il rischio di una proliferazione eccessiva di norme *ad hoc*. Un unico atto legislativo, infatti, «può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri»[35], purché la norma considerata contenga tutti gli elementi prescritti dal G.D.P.R. per garantire un adeguato livello di tutela degli interessati.

L'emanazione di specifici atti normativi non è necessaria, inoltre, per giustificare il flusso di dati tra Titolare e Responsabile del trattamento[36]. In tal caso, infatti, non si configura una «comunicazione» ai sensi dell'art. 2-*ter* del Codice Privacy[37], ma un mero scambio *interna corporis*, dal momento che il Responsabile del trattamento agisce in nome e per conto del Titolare, nei limiti delle funzioni e dei compiti ad esso delegati.

Ulteriori garanzie definite dagli artt. 9[38] e 10[39] del G.D.P.R. sono previste per il trattamento di "dati particolari" (sesso, razza, religione, orientamento politico, etc.) e di quelli c.d. "giudiziari" (relativi a condanne penali e reati) dove la base del trattamento e per lo più sottoposta a "riserva di legge".

I dati particolari possono essere trattati solo in virtù di una norma europea, ovvero di una norma di legge o di regolamento (se previsto dalla legge), quando il trattamento sia necessario per motivi di interesse pubblico rilevante[40]. La norma in questione dovrà specificare le categorie di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per la tutela dell'interessato.

---

[35] Cfr. Considerando n. 45 del GDPR.

[36] Ai sensi dell'art. 4, par. 1, n. 8 del GDPR "responsabile del trattamento" è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

[37] Ai sensi dell'art. 2-ter, co. 4, lett. a) del Codice Privacy, per "comunicazione" si intende «il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione».

[38] Si definiscono dati particolari i «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

[39] Per dati giudiziari si intendono i «dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza».

[40] Cfr. art. 9, par. 2, lett. g) del GDPR e dell'art. 2-*sexies*, comma 2 del Codice Privacy.

Inoltre, qualora il trattamento abbia ad oggetto dati genetici, biometrici e relativi alla salute, esso dovrà avvenire nel rispetto di una delle condizioni di cui al paragrafo 2 dell'art. 9 del G.D.P.R. (es. il consenso dell'interessato, la necessità di assolvere gli obblighi ed esercitare i diritti specifici in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, ecc.) e in conformità alle misure di garanzia disposte dal Garante con cadenza biennale.

Il trattamento di dati giudiziari, invece, può essere effettuato:

(i) sotto il controllo dell'autorità giudiziaria, con le medesime garanzie prescritte per il trattamento di dati particolari, ovvero

(ii) se autorizzato da una norma di legge o, se previsto, di regolamento nell'ambito di una delle materie elencate al comma 3 dell'art. 2-*octies* del Codice privacy e che preveda garanzie appropriate per i diritti e le libertà degli interessati. Vi rientrano, ad esempio, le norme che disciplinano l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ecc.;

(iii) in mancanza di tale norma autorizzativa, il trattamento dovrà essere effettuato nel rispetto delle misure e garanzie prescritte con decreto del Ministero della Giustizia, sentito il Garante, nonché in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata, stipulati con il Ministero dell'interno o con le prefetture-UTG.

Indipendentemente dalla categoria di dati e/o di interessati, il trattamento deve rispettare le prescrizioni generali del G.D.P.R. e del Codice Privacy, sia sotto il profilo tecnico che organizzativo. Ciò presuppone l'adozione di un sistema di gestione della privacy che preveda:

(i) l'implementazione e manutenzione delle procedure, istruzioni operative e della modulistica necessaria per la gestione degli adempimenti normativi in materia (tenuta e aggiornamento del registro dei trattamenti, svolgimento della valutazione di impatto (*Data Protection Impact Assessment*) e dell'analisi dei rischi, gestione dei *data breach* e delle istanze degli interessati, ecc.);

(ii) l'individuazione e formalizzazione dei ruoli privacy dei soggetti coinvolti nel trattamento (Contitolari, Responsabili e sub-responsabili del trattamento), nonché

(iii) la definizione di un sistema formale di deleghe per l'individuazione del personale autorizzato alle attività di trattamento, con definizione delle correlate responsabilità, tenendo conto delle dimensioni organizzative dell'ente considerato.

I titolari e responsabili che operano in ambito pubblico, inoltre, sono tenuti a designare il *Data Protection Officer* ("DPO"), indipendentemente dalle caratteristiche dei trattamenti effettuati e delle categorie di dati trattati. Il DPO deve essere designato in funzione delle sue

qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di *privacy*. È chiamato a svolgere attività di consulenza e supporto al titolare per la gestione degli aspetti legati alla *privacy* e ad operare quale punto di contatto per gli interessati e nei rapporti con il Garante. Il GDPR precisa, inoltre, che più autorità pubbliche o organismi pubblici, tenuto conto della dimensione e struttura organizzativa, possono nominare un unico DPO.

Il ruolo di DPO può essere attribuito sia ad una figura interna alla realtà aziendale che ad un soggetto esterno sulla base di un contratto di servizi e gli possono essere attribuiti altri compiti e funzioni, purché gli sia consentito di agire in condizioni di autonomia e indipendenza, in collaborazione diretta con il vertice gerarchico dell'organizzazione[41]. In tale prospettiva, secondo le indicazioni fornite dal Garante e dalle competenti autorità europee, possono sussistere situazioni di conflitto riguardo a ruoli manageriali di vertice (es. amministratore delegato, membro del consiglio di amministrazione, direttore generale, ecc.), ovvero a soggetti che operano nell'ambito delle strutture aziendali aventi potere decisionale sulle finalità e modalità del trattamento (es. direzione risorse umane, direzione *marketing*, direzione finanziaria, responsabile IT ecc.). Analogamente sono state sollevate perplessità sulla compatibilità tra il ruolo di DPO e lo svolgimento di funzioni di *compliance* aziendale o, in generale, di funzioni che comportino la capacità di incidere sulle scelte aziendali e sui dipendenti (es. *internal audit, risk management*, ecc.)[42].

Tra gli obblighi di carattere generale, si rammentano, infine, le prescrizioni in materia di "violazione di dati personali" (c.d. *data breach*), consistente in una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati[43]. Il titolare del trattamento, senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, è tenuto a notificare la violazione occorsa al Garante, a meno che «sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche». Se poi la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla anche a tutti gli interessati utilizzando i canali più idonei, salvo non abbia già adottato misure tali da ridurne l'impatto.

---

[41] Sulla figura del DPO cfr. artt. 37-39 del GDPR.

[42] Sul conflitto di interessi del DPO cfr. Autorità belga per la protezione dei dati personali, Provvedimento del 28 aprile 2020; Gruppo di Lavoro Articolo 29 – «Linee-guida sui responsabili della protezione dei dati (RPD)»– (wp243rev.01) – adottate il 13 dicembre 2016 ed emendate in data 5 aprile 2017; European data Protection Supervisor – «Position paper on the role of Data Protection Officers of the EU institutions and bodies»del 30 settembre 2018; Garante per la Protezione dei Dati Personali – «*Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato*" e "*Faq sul Responsabile della Protezione dei Dati (RPD) in ambito pubblico*».

[43] Art. 4, par 1, n. 12 del GDPR.

Il soggetto che operi in qualità di Responsabile del trattamento è invece tenuto ad informare il titolare senza giustificato ritardo dopo essere venuto a conoscenza della violazione, sì da consentirgli di agire tempestivamente in conformità agli obblighi previsti dal G.D.P.R.

3.2. Normativa in materia di *cybersecurity*

La disciplina di riferimento è costituita principalmente dal d.lgs. 18 maggio 2018, n. 65, con il quale è stata recepita nel nostro ordinamento la Direttiva NIS (*Network and Information Security*)[44], e dalla normativa che istituisce e regola il Perimetro di Sicurezza Nazionale Cibernetica (§3.2.2).

3.2.1 Disciplina NIS.

Il decreto attuativo della Direttiva NIS si rivolge ai soggetti qualificabili come:

(i) *Operatori di servizi essenziali* (Ose), ossia operatori che agiscono come gestori dei sistemi di rete dedicati ai servizi della sanità dell'energia, dei trasporti, del sistema bancario e dei mercati finanziari, della fornitura e distribuzione di acqua potabile nonché dei servizi e delle infrastrutture dei sistemi di telecomunicazioni. Affinché un operatore possa essere qualificato come Ose deve fornire servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali e la fornitura del servizio deve dipendere dalla rete e dai sistemi informativi sì che un eventuale incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio;

(ii) *Fornitori di servizi digitali* (Fsd), che erogano servizi rientranti nei settori dell'*e-commerce*, del *cloud computing* e dei motori di ricerca *online*.

Gli Ose e i Fsd sono tenuti ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano, nonché a predisporre misure per prevenire e minimizzare l'impatto di potenziali incidenti di sicurezza, al fine di assicurare la continuità dei servizi erogati.

Tali soggetti sono inoltre tenuti a notificare gli incidenti di sicurezza aventi un impatto rilevante al *Computer Security Incident Response Team* italiano ("CSIRT)", istituito presso la Presidenza del Consiglio dei Ministri, cui sono stati trasferiti i compiti e le funzioni già del *Computer Emergency Response Team* ("CERT") nazionale e del "CERT-PA" operante presso l'AgID.

[44] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

In particolare, gli Ose sono individuati con provvedimenti delle Autorità competenti NIS[45] per ciascun settore di riferimento e iscritti in un apposito elenco nazionale istituito presso il Ministero dello sviluppo economico e aggiornato su base regolare almeno ogni due anni.

3.2.2 Perimetro di Sicurezza Nazionale Cibernetica.

Il d.-l. 21 settembre 2019, n. 105[46] ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (di seguito anche "Perimetro"), al fine di assicurare la continuità delle funzioni e dei servizi essenziali svolti da enti pubblici e privati tramite la tutela della sicurezza dei loro sistemi. Il quadro normativo sarà completato con l'adozione di successivi provvedimenti attuativi.

Il 5 novembre 2020 è entrato in vigore il primo di tali provvedimenti, il DPCM 30 luglio 2020, n. 131, che definisce i criteri e le modalità di individuazione degli operatori pubblici e privati inclusi nel Perimetro, nonché per la predisposizione e l'aggiornamento, da parte di tali soggetti, degli elenchi delle proprie reti, sistemi informativi e servizi informatici[47].

I Ministeri e la Presidenza del Consiglio dei Ministri[48], nell'ambito dei settori di rispettiva competenza, identificano gli operatori pubblici o privati che svolgono funzioni e servizi essenziali, la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale.

L'elencazione dei soggetti così individuati è contenuta in un atto amministrativo adottato dal Presidente del Consiglio dei Ministri per il quale è escluso il diritto di accesso, fermo restando

---

[45] Ministero dello Sviluppo Economico, Ministero della Salute, Ministero delle Infrastrutture e dei Trasporti, Ministero dell'Economia e delle Finanze, il Ministero dell'Ambiente e della tutela del Territorio e del Mare e le Regioni e Province Autonome di Trento e Bolzano.

[46] Convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[47] I criteri di individuazione sono forniti dall'art. 2 del DPCM, il quale dispone che (i) un soggetto esercita una funzione essenziale dello Stato laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti; (ii) un soggetto pubblico o privato presta un servizio essenziale per gli interessi dello Stato, laddove ponga in essere attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

[48] In particolare, il Ministero dell'interno per il settore interno; il Ministero della difesa per il settore della difesa; la Presidenza del Consiglio dei ministri per il settore spazio e aerospazio; il Ministero dello sviluppo economico per il settore energia e delle telecomunicazioni e, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per il settore servizi digitali; il Ministero dell'economia e delle finanze per il settore economia e finanza, il Ministero delle infrastrutture e dei trasporti per il settore trasporti; il Ministero del lavoro e delle politiche sociali per il settore enti previdenziali/lavoro; la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca per il settore tecnologie critiche.

che a ciascun soggetto incluso nell'elenco è comunque data separata comunicazione dell'avvenuta iscrizione[49].

L'appartenenza al Perimetro comporta una serie di obblighi sotto il profilo organizzativo, quale l'obbligo di redigere e aggiornare, con cadenza almeno annuale, l'elenco dei beni ICT necessari per lo svolgimento della funzione o servizio essenziale, con la specifica indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono.

Con il DPCM 14 aprile 2021, n. 81, è stato introdotto il Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del predetto decreto e di misure volte a garantire elevati livelli di sicurezza[50].

Il regolamento in esame prevede che al verificarsi di uno degli incidenti aventi impatto su beni ICT, i soggetti inclusi nel Perimetro procedono alla notifica al CSIRT tramite appositi canali di comunicazione, entro un termine particolarmente stringente, che può essere al massimo di un'ora o di sei ore, a seconda della tipologia e, quindi, della gravità dell'incidente occorso.

Inoltre, i soggetti qualificati come Ose o Fsd ai fini della normativa NIS che siano inclusi nel Perimetro, nella comunicazione al CSIRT italiano dovranno indicare che la notifica costituisce anche adempimento degli obblighi prescritti ai fini della disciplina NIS e indicare l'Autorità NIS competente alla quale la notifica dovrà essere inoltrata.

Analogamente, le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi del Codice delle comunicazioni elettroniche[51], sono tenuti a comunicare al CSIRT che la notifica costituisce anche adempimento degli obblighi previsti dall'art. 16-*ter* del predetto Codice e delle correlate disposizioni attuative.

Gli obblighi di notifica previsti dal Regolamento troveranno applicazione a partire dal 1° gennaio 2022. Tuttavia, i soggetti inclusi nel Perimetro provvedono ugualmente alle notifiche in via sperimentale fino al 31 dicembre 2021, con decorrenza dalla data di avvenuta trasmissione dell'elenco dei propri beni ICT alla Presidenza del Consiglio dei Ministri o, se si tratta di soggetti privati, al Ministero dello Sviluppo economico. Ove la trasmissione degli elenchi sia già avvenuta prima dell'entrata in vigore del Regolamento, l'applicazione in via sperimentale decorre dal 26 giugno 2021.

---

[49] Dopo la definizione del primo elenco, in data 15 giugno 2021 il Presidente del Consiglio dei Ministri ha firmato l'estensione dell'ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che, complessivamente, esercitano, attraverso reti, sistemi informativi e servizi informatici, 223 funzioni essenziali dello Stato, ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche. Cfr. https://www.governo.it/it/articolo/cyber-aggiornato-l-elenco-dei-soggetti-del-perimetro-di-sicurezza-cibernetica-nazionale .

[50] Pubblicato in Gazzetta Ufficiale Serie Generale n.138 del 11 giugno 2021 e che entrerà in vigore il 26 giugno 2021.

[51] D.lgs. 1° agosto 2003, n. 259.

Va segnalato che l'obbligo di notifica degli incidenti *cyber* ai sensi della suesposta disciplina non esclude l'obbligo di notifica al Garante per la protezione dei dati personali ove l'evento occorso abbia avuto impatto su dati personali e ricorrano i presupposti richiesti dalla normativa in materia (cfr. §3.1 Normativa privacy).

Il Regolamento prevede, inoltre, le misure di sicurezza che i soggetti inclusi nel Perimetro sono tenuti ad adottare rispetto ai beni e servizi ICT di rispettiva pertinenza.

Le misure sono elencate nell'Allegato B al DPCM e suddivise in due appendici: le misure indicate nell'appendice n.1 dovranno essere implementate entro il termine di 6 mesi dalla trasmissione degli elenchi di beni ICT alle autorità competenti; quelle indicate nell'appendice n. 2 entro il termine di 36 mesi da tale data. Qualora la trasmissione degli elenchi sia avvenuta prima dell'entrata in vigore del Regolamento, i predetti termini decorrono dal 26 giugno 2021.

L'avvenuta adozione e le relative modalità dovranno essere tempestivamente comunicate al Dipartimento delle Informazioni per la Sicurezza.

I soggetti appartenenti al Perimetro sono tenuti a rispettare specifici obblighi in materia di acquisto di beni e servizi ICT che rientrino nelle categorie da individuarsi con decreto del Presidente del Consiglio dei Ministri. Tali obblighi riguardano le procedure, le modalità e i termini per l'affidamento di forniture di beni, sistemi e servizi ICT da impiegare sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici essenziali.

L'intenzione di procedere all'acquisto dovrà essere comunicata al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, unitamente ad una valutazione del rischio associato all'oggetto della fornitura che tenga conto anche dell'ambito di impiego. Decorso il termine di 45 giorni senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione potranno proseguire nella procedura di affidamento; in caso di imposizione di condizioni e test *hardware* e/o *software*, invece, i relativi bandi di gara e contratti dovranno essere integrati con condizioni sospensive o risolutive correlate all'esito favorevole dei test e/o delle ulteriori condizioni disposte dal CVCN. Decorso il termine per la conclusione dei test, sarà possibile proseguire nella procedura di affidamento.

La suddetta normativa è in fase di attuazione. In particolare, con il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, entrato in vigore l'8 maggio 2021, sono stati definiti i termini, le modalità e procedure per le valutazioni da parte del CVCN, nonché i criteri tecnici per l'individuazione delle categorie di beni, sistemi e servizi ICT che saranno oggetto della valutazione nel caso in cui siano destinati agli asset "strategici", che saranno specificamente individuate con d.p.c.m.

Il D.L. 14 giugno 2021, n. 82 ha previsto che l'obbligo di comunicazione al CVCN sarà efficace dal trentesimo giorno dalla data di pubblicazione in Gazzetta Ufficiale del DPCM che,

sentita l'Agenzia nazionale per la cybersicurezza, attesti l'operatività del CVCN e comunque dal 30 giugno 2022.

Dalla suddetta data l'obbligo di comunicazione al CVCN, ai fini della relativa valutazione, troverà applicazione anche rispetto ai soggetti che intendono procedere all'acquisto, a qualsiasi titolo, di beni, servizi e componenti relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, rientranti tra le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale ai sensi decreto-legge 15 marzo 2012, n. 21, soggetti all'esercizio del c.d. Golden Power da parte della Presidenza del Consiglio dei Ministri.

Rimane inteso che fino all'entrata in vigore della suddetta disciplina, le attività di approvvigionamento si svolgono secondo la disciplina ordinaria (cfr. §1 *Procurement* di beni e servizi ICT).

4. *Cybersecurity Act.*

La Legge di Delegazione Europea 2019-2020[52] all'art. 18, prevede l'adozione da parte del Governo di uno o più decreti legislativi per adeguare la normativa nazionale al Regolamento europeo sulla cybersicurezza (cd. Cybersecurity Act)[53], che richiede a tutti gli Stati Membri di designare una o più Autorità Nazionali di Certificazione della Cybersicurezza (*National Cybersecurity Certification Authorities*, in sigla NCCA) che vigileranno sull'applicazione dello stesso a livello nazionale e coopereranno con le autorità designate dagli altri Stati Membri, la Commissione Europea e l'agenzia europea ENISA nella realizzazione e revisione del quadro europeo di certificazione.

Alle NCCA sono assegnati cogenti poteri allo scopo di far rispettare il quadro europeo di certificazione nel proprio ambito nazionale e avranno anche il compito di rilasciare i certificati di cybersicurezza nel caso in cui questi abbiano un livello di affidabilità elevato e in altri casi, debitamente giustificati, ove previsto esplicitamente in singoli sistemi europei di certificazione. Questi poteri si associano alla possibilità di adottare e infliggere pesanti sanzioni ai soggetti che dovessero contravvenire alle disposizioni impartite dalle predette Autorità. In tal senso l'art. 18 della Legge di Delegazione Europea prevede, *inter alia*, la delega al Governo per la definizione del sistema di sanzioni applicabili nonché l'attribuzione al Ministero dello Sviluppo economico del ruolo di NCCA.

---

[52] Legge n. 53 del 22 aprile 2021, «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020».

[53] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013. Per maggiori informazioni sull'intervento normativo previsto dalla Legge di Delegazione Europea cfr. https://atc.mise.gov.it/images/documenti/Scheda_Informativa.pdf.

Il quadro in tema di sicurezza e *cyber security* sin qui ricostruito è stato recentemente riorganizzato dalle modifiche apportate dal D.L. 14 giugno 2021, n. 82. È stata infatti istituita l'Agenzia nazionale per la cyber-sicurezza cui sono state trasferite una parte rilevante delle funzioni attribuite alle autorità ed istituzioni sin qui menzionate. *Inter alia*, il decreto prevede che l'Agenzia agisca quale Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del relativo Regolamento e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dell'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni. Il tempo ci dirà se questa riforma semplificherà o renderà ancor più complesso il quadro di riferimento in materia.

5. Conclusioni operative.

Quanto sin qui esposto avrebbe la presunzione di rappresentare una ricostruzione sintetica delle disposizioni normative e regolamentari, comprese quelle c.d. di *soft law*, che disciplinano, organizzano e regolamentano l'acquisizione degli strumenti ICT necessari ad implementare i processi di *e-government*. In estrema sintesi la regolamentazione del settore dell'"informatica pubblica".

Il quadro che ne esce è complesso e affollato da attori diversi spesso con competenze che solo agli occhi di un esperto di informatica potrebbero non risultare "concorrenti". La complessità riguarda sia l'individuazione delle linee strategiche di sviluppo dei "sistemi pubblici" e la conseguente scelta degli strumenti ICT più idonei a soddisfare i fabbisogni della PA ma anche quello del *procurement* di tali strumenti. Per non parlare, da ultimo, dei requisiti tecnici che tali strumenti debbono avere per garantire l'interoperabilità e la sicurezza dei sistemi che custodiscono spesso i dati personali dei cittadini.

Nell'ambito delle riforme legate agli obbiettivi del Piano Nazionale di Ripresa e Resilienza quelle legate alle riforme della P.A. della giustizia e della semplificazione amministrativa sono centrali[54]. La missione 1 del PNRR è in gran parte dedicata alla digitalizzazione, innovazione e sicurezza della PA, cioè di quanto sin qui affrontato in termini di informatica pubblica.

Il rischio di una sovrapposizione di competenze tra i diversi organismi pubblici[55] coinvolti nei processi di informatica pubblica rischia decisamente di complicare ulteriormente il quadro rendendo assai improbabile il raggiungimento degli obbiettivi che il PNRR si prefigge. La prospettiva pare dunque essere lo stallo su tematiche tecniche e strategiche inerenti la

[54] Si veda il PNRR 2.A Le riforme pp. da 43 a 78, e Missione 1 pp. 83-96.

[55] Solo per ricordarne alcuni: AGID, Dipartimento per la Sicurezza delle Informazioni, Direzioni Generali delle Amministrazioni Centrali coinvolte, Agenzia per la Sicurezza, Autorità Garanti, PDCM su Golden Power, etc. etc.

digitalizzazione della P.A., cui devono accostarsi le difficoltà di approvvigionamento, le c.d. attività di *procurement*, che nel pubblico si traducono in gare ed appalti. Si tratta di procedimenti i cui atti sono sottoposti al controllo di legittimità della giustizia amministrativa che, di fronte a norme "tecniche" complesse e farraginose, si trova spesso costretta a sospendere i procedimenti in attesa di ricevere chiarimenti dagli organismi pubblici coinvolti con ciò dilatando oltre modo i tempi e la conclusione dei contratti, al contempo lasciando l'amministrazione senza gli strumenti ICT necessari al processo di digitalizzazione e semplificazione.

In questa prospettiva, a parere di chi scrive, sarebbe importante individuare uno o più "Responsabili dei sistemi informativi pubblici" che possano rivestire un ruolo operativo centrale quale braccio tecnico delle amministrazioni. A tali soggetti andrebbe anche assegnato il compito di coordinarsi con i diversi organismi pubblici deputati al coordinamento delle tematiche strategiche dell'informatica pubblica. Il tutto per arrivare alla costruzione di un portfolio di servizi e strumenti ICT "a scaffale" già validati nel momento del *design* architetturale sotto i diversi profili della compatibilità tecnica, dell'interoperabilità e delle garanzie in materia di tutela della *privacy* e della *cybersecurity*. Un ruolo centrale potrebbero così essere rivestito dalle società pubbliche e più in generale dai Poli Strategici Nazionali utilizzando, anche in prospettiva *Opex*, le diverse soluzioni disponibili sul mercato e, con queste, costruendo l'offerta scalabile dei diversi mattoncini (in termini di risorse elaborative, servizi ed applicazioni) di volta in volta necessari al titolare dell'azione amministrativa per costruire gli strumenti ICT atti a soddisfare la digitalizzazione e la semplificazione dei processi e dei procedimenti amministrativi.