Camera dei Deputati

Commissioni I e IX riunite

Conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale AC 3161

Memoria della Prof.ssa Ginevra Cerrina Feroni*

1. L'Agenzia per la cybersicurezza nazionale: funzioni e peculiarità

Ringrazio le Commissioni per quest'invito alla riflessione su di una disciplina, quale quella introdotta dal decreto-legge, particolarmente innovativa e stimolante sotto il profilo dell'analisi giuridica.

Sono molti i profili d'interesse per il costituzionalista, in particolare se esperto di nuove tecnologie: da quelli più strettamente ordinamentali a quelli di merito; dagli aspetti legislativi (oggetto peraltro di un articolato parere del Comitato per la legislazione) a quelli inerenti l'architettura istituzionale proposta.

Nell'impossibilità di analizzare, in questa sede, ciascuno dei profili d'interesse, il presente contributo si limiterà ad alcune considerazioni relative alla natura dell'Agenzia e, quindi, ai riflessi che la sua collocazione ordinamentale spiega sul regime di trattamento dei dati personali, sulla base di una particolare declinazione del rapporto tra protezione dati e *cybersecurity*.

Va anzitutto premesso come il decreto-legge, oltre ad istituire l'Agenzia per la cybersicurezza nazionale (infra: ACN), disponga una complessiva e organica revisione del quadro ordinamentale in materia di cybersicurezza, a partire dalla definizione di tale nozione sino alla relativa architettura istituzionale, ridisegnando le attribuzioni dei vari organi in materia, adeguandole alle nuove esigenze di tutela emerse con l'accelerazione del processo di digitalizzazione. In tal senso, il decreto-legge rappresenta un ulteriore tassello nella cornice normativa delineatasi a partire dalla l. 133 del 2012 (che ha attribuito

all'intelligence compiti in materia di attività di ricerca informativa finalizzata alla sicurezza cibernetica), con gli sviluppi più recenti determinati dal d.lgs. 65 del 2018, attuativo della direttiva NIS e, da ultimo, con il Perimetro di sicurezza nazionale cibernetica di cui al d.l. 105 del 2019.

Il decreto-legge rafforza, in questo senso, il sistema istituzionale complessivo a tutela della *cybersecurity*, attribuendo tuttavia (e più correttamente) a un organo, quale l'Agenzia, estraneo agli Organismi informativi, compiti di gestione attiva della strategia di sicurezza, non propri in senso stretto del Comparto intelligence.

Secondo la riformulazione operata dal decreto-legge in esame, dunque, il sistema nazionale di sicurezza cibernetica ha al suo vertice il Presidente del Consiglio dei Ministri cui è attribuita l'alta direzione e la responsabilità generale (di natura eminentemente politica) delle "politiche di cybersicurezza", oltre che l'adozione della relativa strategia nazionale. Al Presidente del Consiglio dei Ministri spettano anche la nomina e la revoca, previa informativa al Presidente del COPASIR, del Direttore generale (scelto tra le categorie soggettive tra le quali può essere nominato il segretario generale della Presidenza del Consiglio, pur con documentata esperienza di elevato livello nella gestione dei processi d'innovazione) e del Vice direttore generale dell'ACN. L'Autorità delegata, ove istituita, può svolgere le funzioni appunto delegatele dal Presidente del Consiglio dei ministri, ad eccezione di quelle previste come esclusivamente presidenziali. Replicando in parte il modello del CISR (Comitato interministeriale per la sicurezza della Repubblica), viene istituito, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC). Anche tale Comitato svolge funzioni prevalentemente consultive, propositive e di controllo, tuttavia nello specifico ambito della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

La più significativa innovazione del decreto concerne, tuttavia, l'istituzione dell'ACN: un attore istituzionale al centro del sistema nazionale di sicurezza cibernetica, ma esterno al comparto intelligence in senso stretto, di cui non

duplica le funzioni (vista anche la clausola di esclusività delle attribuzioni degli Organismi di cui all'art. 8 della l. 124/2007) ma con il quale è strettamente interrelato. L'Agenzia presenta dunque, in tal senso, una natura ancipite che le deriva dal disporre di una competenza estesa tanto agli interessi nazionali nel campo della cybersicurezza, quanto a quelli di s*icurezza nazional*e in ambito cibernetico. Tali ultimi aspetti l'assimilano, almeno in parte, agli Organismi, pur con l'attribuzione di un ruolo di gestione attiva meno riferibile agli organi d'intelligence t*out cour*t. L'ACN è designata, in particolare, quale Autorità nazionale per la cybersicurezza, titolare del potere di coordinamento tra i soggetti pubblici coinvolti in materia e Autorità nazionale competente, nonché punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al d.lgs. 65 del 2018, a tutela dell'unità giuridica dell'ordinamento, competente altresì all'accertamento delle violazioni e all'irrogazione delle relative sanzioni amministrative previste dallo stesso decreto legislativo. Presso l'Agenzia è inoltre costituito il Nucleo per la cybersicurezza previsto, in via permanente, quale organo di supporto del Presidente del Consiglio dei Ministri in materia, attualmente previsto dal dPCM 17 febbraio 2017, rispetto al quale dunque il decreto-legge eleva la fonte di disciplina.

Ma l'organico inserimento dell'Agenzia nel sistema istituzionale a tutela della sicurezza nazionale in ambito cibernetico, che non potrebbe dunque prescindere da uno stretto collegamento con gli Organismi, è esemplificato in maniera palese dal ruolo che l'Agenzia assumerà, al posto del DIS, nel Perimetro di sicurezza nazionale cibernetica, come pure dall'attribuzione al Copasir del potere consultivo e di controllo sull'operato dell'Agenzia (e corrispondentemente sul rispetto del principio di esclusività di cui al citato art. 8).

La stretta interrelazione tra l'Agenzia e il Comparto intelligence, con il quale essa condivide, sia pure per profili diversi, alcune attribuzioni in materia di sicurezza nazionale, è assicurata non solo dal conferimento, comune in capo al Presidente del Consiglio dei Ministri, dell'alta direzione e della responsabilità

politica anche in materia di *cybersecurity* ("*anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico*"), ma anche dal ruolo svolto sul punto dall'Autorità delegata. Si istituisce così un punto di raccordo politico per le attività di sicurezza nazionale nello spazio cibernetico e, in particolare, tra quelle nel campo della cybersicurezza e quelle nel campo delle attività di ricerca informativa proprie dell'intelligence.

Anche sotto il profilo organizzativo l'Agenzia presenta delle peculiarità significative.

Nonostante la denominazione essa non segue integralmente, infatti, il modello tradizionale delle Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (se non per l'esigenza di specifiche professionalità cui affidare la gestione di un settore) e neppure quello delle agenzie fiscali, caratterizzantesi come noto per una più marcata autonomia dal paradigma generale. Rispetto ad esso, l'ACN presenta un'autonomia ancor più rilevante. E questo non solo per il riconoscimento della personalità giuridica di diritto pubblico (propria anche delle agenzie fiscali) e dell'autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, ma anche per la diretta dipendenza dal Presidente del Consiglio e, ove istituita, dall'Autorità delegata (entrambi i quali dell'ACN possono avvalersi ex art. 5, c. 2).

Tuttavia, nonostante le molte affinità con gli Organismi, l'ACN presenta uno statuto giuridico peculiare sotto molto profili: organo non ricompreso nel Comparto intelligence ma, comunque, titolare di compiti rilevanti in materia di sicurezza nazionale.

2. La disciplina del trattamento dei dati personali svolto dall'Agenzia

La natura giuridica peculiare dell'Agenzia si riflette, del resto, anche sul regime previsto (dall'art.13 del decreto-legge) per il trattamento dei dati personali, che ne costituisce anzi un indice particolarmente significativo.

Va sul punto premesso che sin dalla l. 675/1996, il legislatore italiano ha compiuto la scelta essenziale di non sottrarre (come invece in molti altri Paesi) i trattamenti per fini di sicurezza nazionale (materia come noto sottratta alle attribuzioni comunitarie) alla disciplina-*privacy*, riconoscendo invece all'interessato una sfera essenziale di prerogative, anche mediante i poteri di intervento e controllo attribuiti al Garante. Con il d.lgs. 196 del 2003, la disciplina del trattamento dei dati personali a fini di sicurezza nazionale si è articolata ulteriormente, con la distinzione essenziale tra i trattamenti svolti da organi del Comparto intelligence e quelli effettuati, invece, da soggetti pubblici diversi benché sempre per fini di sicurezza nazionale, diversamente modulando l'intensità delle deroghe (più netta per i primi, meno per i secondi) rispetto al diritto comune.

In particolare: ai trattamenti - svolti dai Servizi o su dati coperti da segreto di Stato - si applicavano i principi generali aventi carattere d'indirizzo e le norme generali del d.lgs. 196 del 2003; le disposizioni su modalità di trattamento e requisiti dei dati (principi di liceità, correttezza, pertinenza, non eccedenza, esattezza, aggiornamento, minimizzazione del trattamento di dati identificativi); divieto di profilazione; obblighi di sicurezza e adozione delle misure minime; regime del risarcimento del danno cagionato per effetto d'illecito trattamento, poteri d'intervento del Garante (art. 58, c.1). Al trattamento effettuato da soggetti pubblici diversi da quelli del Comparto Intelligence - ma comunque per fini di difesa o sicurezza dello Stato- in base a previsione legislativa espressa, si applicavano inoltre gli obblighi di notificazione del trattamento di dati genetici, biometrici, sanitari o inerenti la vita sessuale o trattati con tecniche di profilazione, con le relative sanzioni amministrative in caso d'inadempimento (art. 58, c. 2).

La novella del d.lgs. 196 del 2003 - operata dal d.lgs. 101 del 2018, nell'esercizio della discrezionalità riconosciuta al legislatore nazionale rispetto a una materia, quale la sicurezza nazionale, sottratta alla competenza UE - ha mantenuto tale dicotomia, modulando diversamente il raggio di applicazione del d.lgs. 51 del

2018, assunto a riferimento principale in materia in quanto relativo ai trattamenti di dati personali in ambito giudiziario penale e di polizia, dunque in certa misura contiguo a quello della sicurezza nazionale.

Pertanto, ai trattamenti svolti dal Comparto intelligence, o comunque su dati coperti da segreto di Stato, si applicano i principi e le norme relative ai trattamenti automatizzati, agli obblighi del titolare, alla figura del responsabile del trattamento, alla *privacy by design* e *by default*, agli obblighi di sicurezza, alle funzioni del Garante, alla responsabilità risarcitoria, alle sanzioni amministrative e penali[1].

Inoltre, qualora il trattamento sia effettuato da soggetti pubblici diversi dagli Organismi - ma comunque per fini di difesa o sicurezza dello Stato - in base a previsione legislativa espressa, oltre alle norme suddette, si applicano anche quelle su valutazione d'impatto e consultazione preventiva del Garante. Si rimette poi a uno o più regolamenti - emanati sentito anche il Garante, ex art. 24, c. 2 d.lgs. 51 del 2018 in combinato disposto con l'art. 58, p. 2 - la previsione delle modalità di applicazione di tale disciplina. Sul punto si potrebbe pensare di estendere a tali regolamenti la procedura prevista per quelli emanati nell'ambito dell'art. 58, c.1, dunque con il coinvolgimento del COPASIR, anche al fine di garantirne il ruolo di supervisione complessivo così determinante ai fini della coerenza complessiva del sistema.

L'articolo 13 del decreto-legge rende applicabili ai trattamenti svolti dall'ACN quest'ultimo regime (di cui all'articolo 58, comma 2, del d.lgs. 196/2003). Si tratta di soluzione corretta, in quanto riferisce all'Agenzia - che non svolge attività d'intelligence ma opera a tutela della sicurezza nazionale - la disciplina del trattamento dei dati personali a fini di sicurezza nazionale, svolti da soggetti

---

*Ordinario di Diritto Costituzionale Comparato, Università di Firenze, Vicepresidente dell'Autorità Garante per la protezione dei dati personali. La memoria è resa a titolo esclusivamente personale, non impegna l'Autorità e non deve intendersi rilasciata ai fini di cui all'art. 36, par. 4, Gdpr.

1 Cfr. A. SORO, *Segreto di Stato ed accesso agli archivi,* Lezione tenuta alla Scuola superiore della magistratura, 18 settembre 2015. in www.garanteprivacy.it

diversi dagli Organismi. Resta inteso che, ai trattamenti meramente amministrativi o comunque svolti non nell'esercizio delle competenze dell'Agenzia funzionali alla tutela della sicurezza nazionale, si applicherà il regime di diritto comune, come del resto sottolinea la stessa Relazione illustrativa del decreto-legge.

Va infine sottolineato come il decreto-legge preveda espressamente la facoltà dell'Agenzia di realizzare una specifica cooperazione con il Garante (oltre che la sua consultazione), anche mediante protocolli d'intesa, relativi tra l'altro alle notifiche dei *data breach*. La necessità di consultazione e cooperazione con il Garante è tanto più rilevante in ragione dell'assunzione, da parte dell'ACN, del ruolo di Autorità nazionale ai fini della direttiva NIS, positivamente superando l'attuale frammentazione di compiti in materia con un unico centro di responsabilità.

In linea generale, la previsione assai opportunamente estende all'Agenzia la preziosa prassi collaborativa, ormai consolidata, tra il Garante e gli Organismi (il DIS, in particolare), sviluppatasi in maniera proficua, nel rispetto delle diverse posizioni ordinamentali dei due soggetti istituzionali. Tale collaborazione, almeno dal 2013 (data di sottoscrizione del primo protocollo d'intenti, successivamente all'adozione della direttiva "Monti" sulla cybersecurity) ha rappresentato una delle più innovative e paradigmatiche espressioni di quella sinergia tra protezione dati e sicurezza cibernetica che, sempre più, costituirà l'architrave del governo del digitale nel prossimo futuro.