Le nuove linee guida AgID sul documento informatico

La novellata versione del *Codice dell'Amministrazione Digitale (CAD)**[1]* ha previsto che l'Agenzia per l'Italia Digitale (AgID), "*previa consultazione pubblica da svolgersi entro il termine di trenta giorni* […] *adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del […] Codice*"[2] (1). Tali linee guida "*divengono efficaci dopo la loro pubblicazione**[3]** nell'apposita area del sito Internet istituzionale dell'AgID*"[4], (1).

Il 16 novembre 2019 si è conclusa la fase di consultazione pubblica della bozza delle Linee Guida AgID sul documento informatico, precedentemente avviata il 17 ottobre dello stesso anno. Al momento siamo in attesa di pubblicazione[5] sul sito istituzionale di AgID della versione definitiva delle linee guida. A partire dal giorno successivo alla loro pubblicazione le linee guida entreranno in vigore, e quindi si applicheranno successivamente "*a partire dal centottantesimo giorno successivo alla loro entrata in vigore*"[6],(2).

Il contesto di riferimento

Lo scopo delle linee guida è sicuramente quello di aggiornare le attuali regole tecniche concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici, in base alle disposizioni di cui all'articolo 71 del *Codice dell'amministrazione digitale*. Esiste comunque anche un'altra e ben più importante finalità che è quella di "*incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo a un «unicum» normativo che disciplini gli ambiti materiali sopracitati, nel rispetto della disciplina in materia di Beni culturali*"[7], (2).

L'**ambito di applicazione** delle linee guida è duplice, essendo

sia soggettivo che oggettivo. Per quanto concerne l'ambito soggettivo, le linee guida si applicano[8] alle pubbliche amministrazioni, ai gestori di servizi pubblici, alle società a controllo pubblico, nonché, per specifiche disposizioni, anche ai privati, ove non diversamente previsto. Invece, per quanto riguarda l'ambito oggettivo di applicazione, le l*inee guida contengono le regole tecniche sugli ambiti materiali disciplinati da alcune disposizioni del CAD****[9]****.*

In pratica le nuove Linee Guida "*costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nei DPCM del 2013 e 2014*"[10] (2). Con esse, il legislatore ha voluto fornire una gestione complessiva e semplificata del documento informatico, che ora si esprime "*attraverso una visione d'insieme che aggrega in un «corpo unico» materie prima disciplinate separatamente*"[11] (2).

Si tratta di un approccio metodologico di tipo olistico, finalizzato "*a mettere in evidenza e a rappresentare le interdipendenze funzionali tra le varie fasi della gestione documentale dal momento della formazione fino alla selezione per lo scarto o la conservazione permanente*"[12](2).

La natura vincolante delle linee guida

Il parere del Consiglio di Stato – numero 02122/2017, del 10/10/2017 – fornisce interessanti **interpretazioni** in merito alla vincolatività delle nuove linee guida adottate da AgID, che sostituiranno le regole tecniche in precedenza previste dall'art. 71 del CAD. Nello specifico, la Commissione ha rilevato *"come la scelta di introdurre nella normativa di settore uno strumento di regolazione più flessibile rispetto alle regole tecniche appaia sostanzialmente in linea con il criterio direttivo****[13]****[…] della legge di delega* (3)". Tale conformità si concretizza nell'esigenza "*che le disposizioni del Codice siano connotate da «neutralità tecnologica», al*

fine di evitare il rischio che le previsioni del CAD comportino la necessità di ricorrere a soluzioni e servizi tecnologici non in linea con lo sviluppo, di certo rapido, del settore" (4).

In particolar modo, "*la Commissione ritiene che le citate linee guida, per poter consentire al Codice di trovare una applicazione uniforme su tutto il territorio nazionale e nei confronti dell'intera collettività, non possono che assumere una valenza erga omnes e un carattere di vincolatività*" (4). Dunque, per quanto concerne il profilo della gerarchia delle fonti, queste dovrebbero essere inquadrate "*come un atto di regolazione seppur di natura tecnica, con la conseguenza che le medesime dovrebbero ritenersi pienamente giustiziabili dinanzi al giudice amministrativo*" (4).

Il Consiglio di Stato evidenzia anche che il "*procedimento di approvazione e di pubblicazione […] previsto dal novellato art. 71 del CAD*" [4], è in linea con le osservazioni contenute nel parere n. 855 del 2016 (5), laddove si evidenziava che nel caso di linee guida di natura vincolante, fosse necessaria la presenza di garanzie procedimentali al fine di "*compensare la maggiore flessibilità del «principio di legalità sostanziale» con un più forte rispetto di criteri di «legalità procedimentale»*" (5).

Le novità delle linee guida

Le nuove linee guida introducono delle significative novità rispetto alle vigenti regole tecniche, sia relativamente al sistema di conservazione, sia per quanto concerne la formazione e la gestione dei documenti informatici. Nel prosieguo dell'articolo ci concentreremo su alcune riflessioni in merito al ruolo delle norme ISO, così come presentate dalle linee guida, per rimandare a due successivi articoli di approfondimento gli altri aspetti citati.

Le linee guida e le norme ISO/IEC

In conclusione vorrei evidenziare alcune affermazioni, contenute nelle linee guida, che potrebbero essere fuorvianti rispetto l'utilizzo corretto e consapevole delle norme ISO/IEC, nonché dei processi di certificazione connessi con alcune di loro.

Infatti, nelle linee guida si afferma che "*le certificazioni di sistema ISO 9001 e 27001 rappresentano […] – lato organizzazione – una ragionevole garanzia di qualità a fronte delle variabili tecnologiche individuate*"[14] (2). Personalmente credo che si tratti di **un'affermazione pericolosa**, nonché collegata a una visione semplicistica di sistemi complessi. Pur senza voler negare i vantaggi che tali certificazioni di processo potrebbero portare in organizzazioni che decidessero di implementarle modificando la cultura aziendale nell'ottica di recepire lo spirito delle norme stesse, è evidente che la letteratura scientifica ha più volte sottolineato che tali certificazioni di processo non sono effettivamente in grado di assicurare nulla sull'effettiva qualità dei prodotti realizzati, nonché sul grado di sicurezza effettivamente conseguito, dovendosi necessariamente limitarsi a rilevare che, dall'analisi dei processi in essere sia presumibile che questi risultati possano essere raggiunti.

Se a titolo esemplificativo si prende come termine di paragone la norma ISO/IEC 27001:2013, questa "*non si occupa direttamente di cosa ci sia all'interno della policy in questione; dunque, non si occupa della qualità intrinseca della policy, né tantomeno della qualità dello strumento […] che da tale policy è governato*" (6); infatti il suo "*focus è tutto sulla presenza dello strumento di gestione e sul fatto che in esso siano presi in considerazione gli obiettivi del controllo ivi indicati*" (6).

Nella sua formulazione lo standard ISO/IEC 27001:2013 si

occupa essenzialmente della qualità dei processi in essere in un sistema di gestione della sicurezza delle informazioni, ma si disinteressa della **qualità delle soluzioni** che sono implementate nel sistema stesso.

Non a caso la declinazione pratica della norma, quella che poi è oggetto di certificazione, si appoggia nei fatti su altre norme (come la ISO/IEC 27002:2013) che nascono come "*riferimento per la scelta dei controlli nel processo di attuazione di un Sistema di gestione della sicurezza delle informazioni basato sulla ISO/IEC 27001:2013*" (6). Non a caso nel certificato, che viene rilasciato all'organizzazione da parte di un organismo di certificazione, si indica che si è proceduto a verificare "*la corretta applicazione dei controlli contenuti nella norma a uno specifico ambito di certificazione*" (6).

Per dare concretezza ai ragionamenti testé effettuati è possibile fare riferimento al recente Provvedimento d'urgenza[15], (7) del **Garante per la protezione dei dati personali,** con cui l'autorità di controllo è intervenuta nei confronti di un noto gestore di servizi fiduciari, nonché del servizio di posta elettronica certificata[16]. Tale azione è avvenuta a seguito della rilevazione di numerose vulnerabilità emerse durante un accertamento ispettivo in merito alla gestione del servizio PEC.

A titolo esemplificativo il Garante ha evidenziato che "*circa 560.000 utenti utilizzavano ancora, per l'accesso alla propria casella pec, la password iniziale, scelta per loro da uno degli 8.900 partner della società […] senza che fosse imposto, come avrebbe dovuto, l'obbligo di modifica al primo accesso*" (8). Ma anche che "*le password tecniche di gestione di alcuni servizi informatici erano riportate in chiaro nei log di tracciamento delle operazioni*" (8). Inoltre, era possibile "*consultare ed esportare, da rete internet, i log dei messaggi scambiati da oltre 6 milioni di caselle pec*" (8), anche attraverso l'utilizzo di *"un'utenza, con elevati privilegi di*

amministrazione (superadmin), utilizzata da più persone, in violazione dei più elementari principi di sicurezza del trattamento".

Ai fini della nostra trattazione è d'interesse il fatto che il gestore in questione fosse in possesso di numerose certificazioni in materia di sicurezza ivi incluse la ISO/IEC 27001:2013. Malgrado ciò, le vulnerabilità rilevate erano proprio insite nelle procedure informatiche adottate e la valutazione di alcuni rischi connessi era risultata carente (8).

Da qui, la **critica** alle affermazioni riportate all'interno delle Linee guida, nella quali sembra che il possesso della certificazione ISO/IEC 27001 sia sufficiente a garantire con ragionevolezza la qualità del processo, mentre questa, limitandosi a verificare la coerenza tra i controlli implementati e gli obiettivi di sicurezza dichiarati e auto-prefissatesi dall'organizzazione, "*andrebbe vista come una sorta di norma base, la cui implementazione conforme non possa prescindere dalla consultazione e dal rispetto di altre norme*" (6).

In tal senso, interessante è anche il parere[17] emesso dal *Garante* sullo schema delle linee guida, nel quale si evidenzia come sia "*opportuno ribadire che i titolari del trattamento devono mettere in atto, ed essere in grado di comprovare, al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, l'adozione di misure tecniche ed organizzative adeguate avendo riguardo anche ai principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita (artt. 5, 24 e 25 del Regolamento)*" (9).

Note

[1] Il D.lgs. 82/2005 ha subito moltissime modifiche e integrazioni, tra le quali (in ordine cronologico) le ultime

sono state quelle apportate: dal D.lgs. 26 agosto 2016, n. 179, dal D.lgs. 13 dicembre 2017, n. 217, dal D.L. 28 settembre 2018, n. 109, convertito con modificazioni dalla L. 16 novembre 2018, n. 130, dal D.L. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, dalla Legge 30 dicembre 2018, n. 145 e dal D.L. 26 ottobre 2019, n. 124.

[2] D.lgs. 82/2005, articolo 71, comma 1.

[3] Di tale circostanza ne è poi data notizia nella Gazzetta Ufficiale della Repubblica italiana.

[4] Idem 2.

[5] Fonti ufficiose sembrerebbero confermare l'uscita della versione definitiva delle linee guide entro il mese di marzo dell'anno 2000.

[6] Linee guida sulla formazione, gestione e conservazione dei documenti informatici (Release bozza) – Paragrafo 1.4 "Abrogazioni e norme transitorie".

[7] Linee guida sulla formazione, gestione e conservazione dei documenti informatici (Release bozza) – Paragrafo 1.1 "Scopo del documento".

[8] Ovvero si applicano ai soggetti indicati nell'articolo 2, commi 2 e 3 del CAD.

[9] Nello specifico il riferimento è alle disposizioni di cui agli articoli 20, 21, 22, 23, 23-bis, 23-ter, 23-quater, 34, 40, 40-bis, 41, 42, 43, 44, 45, 46, 47, 49, 50, 51, 64-bis e 65.

[10] Linee guida sulla formazione, gestione e conservazione dei documenti informatici (Release bozza) – Paragrafo 1.9 "Premessa metodologica".

[11] *Ibidem*.

[12] *Ibidem*.

[13] Il riferimento è al criterio direttivo recato dall'articolo 1, comma 1, lettera m) della legge di delega (ovvero la legge 7 agosto 2015, n. 124). In tale provvedimento si fa riferimento, tra l'altro, alla necessità di rispettare il criterio direttivo di "semplificare le modalità di adozione delle regole tecniche e assicurare la neutralità tecnologica delle disposizioni del CAD, semplificando allo stesso tempo il CAD medesimo in modo che contenga esclusivamente principi di carattere generale" [3].

[14] Allegato 3 "Certificazione di processo" al documento "Linee guida sulla formazione, gestione e conservazione dei documenti informatici (Release bozza) – Paragrafo 2.3 "Ciclo di dematerializzazione: requisiti, fasi e controlli".

[15] Il riferimento è al Provvedimento n. 228 del 18 dicembre 2019.

[16] Si evidenzia la criticità delle fattispecie, dato che il gestore in questione ha in carico oltre sei milioni di caselle utilizzate da vari soggetti, sia pubblici che privati.

[17] Il riferimento è al Provvedimento del Garante n. 32 del 13 febbraio 2020.

Bibliografia

1. Decreto legislativo 7 marzo 2005, n. 82 (come modificato dal Decreto legislativo 13 dicembre 2017, n. 217 (in G.U. 12/01/2018, n.9), GU n.112 del 16-5-2005-Suppl. Ordinario n. 93, 2005.
2. Agenzia per l'Italia Digitale, *"Linee guida sulla formazione, gestione e conservazione dei documenti informatici Release bozza AGID".* Roma, pp. 1–39,
3. Legge 7 agosto 2015, n. 124 – *"Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche".* Gazzetta della Repubblica Italiana, 2015,

pp. 5–53.
4. Consiglio di Stato, “Parere del Consiglio di Stato, n. 02122/2017, del 10/10/2017, sullo schema di decreto legislativo recante disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179”, 2017.
5. Consiglio di Stato, “Parere del Consiglio di Stato, n. 855/2016, del 1/4/2016, sullo schema di decreto legislativo recante “Codice degi appalti pubblici e dei contratti di concessione.”
6. Ciclosi, *La protezione dei dati e la gestione del rischio nella pubblica amministrazione. Un approccio unificato nel contesto del GDPR e del framework europeo di sicurezza cibernetica*. Santarcangelo di Romagna (RN): Maggioli Editore, 2019.
7. Garante per la Protezione dei dati personali, “Provvedimento correttivo d’urgenza nei confronti di Aruba Posta Elettronica Certificata S.p.a. (n. 228 del 18 dicembre 2019) [doc. we.9283040]”, Roma, 2019.
8. Garante per la protezione dei dati personali, “Newsletter 06/03/2020 – Prescritte ad un gestore misure urgenti per la sicurezza del servizio pec – Sanità: più tutele privacy nei bandi di gara – Scuola, graduatorie docenti: no alla pubblicazione di dati sulla salute o non necessari – Privacy: luci e om,” 2019. [Online]. Available: https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283047#1. [Accessed: 08-Mar-2020].
9. Garante per la protezione dei dati personali, “Parere sullo schema di ‘Linee Guida sulla formazione, gestione e conservazione dei documenti informatici’ (n. 32 del 13 febbraio 2020) [doc. web. 9283921]”, Roma, 2020.

Articolo a cura di **Francesco Ciclosi**

https://www.ictsecuritymagazine.com/articoli/le-nuove-linee-guida-agid-sul-documento-informatico/