Parere su uno schema di linee-guida in materia di Disaster Recovery delle pubbliche amministrazioni - 20 ottobre 2011 [1851672]

[doc. web n. 1851672]

Parere su uno schema di linee-guida in materia di Disaster Recovery delle pubbliche amministrazioni - 20 ottobre 2011

Registro dei provvedimenti
n. 394 del 20 ottobre 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

Vista la richiesta di parere di DigitPa;

Visto l´art. 154, comma 4 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell´Ufficio formulate dal segretario generale ai sensi dell´art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

PREMESSO

DigitPA ha richiesto il parere del Garante in ordine a uno schema di linee-guida in materia di "Disaster Recovery delle pubbliche amministrazioni", emanato ai sensi dell´articolo 50-bis, comma 3, lettera b), del Codice dell´amministrazione digitale (infra: CAD), di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.

Il provvedimento in esame mira a definire le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, sulla base di un modello al quale le pubbliche amministrazioni che vi sono tenute (quelle di cui all´articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 e successive modificazioni) dovranno conformarsi nella redazione dei propri piani di disaster recovery.

RILEVATO

1. Contenuti e struttura del documento.

Le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche delle pubbliche amministrazioni non rappresentano l´unico oggetto del provvedimento in esame, che ha una portata più ampia rispetto a quella prevista dal citato articolo 50-bis. Lo schema di linee-guida affronta infatti ad ampio spettro il tema della continuità operativa, a cominciare dai suoi obiettivi nell´ambito delle pubbliche amministrazioni (cap. 1), dalle novità introdotte dalle recenti modifiche apportate al Codice dell´amministrazione digitale e in particolare dal decreto legislativo 30 dicembre 2010, n. 235 (cap. 2), da un´ampia rassegna degli standard e delle best practices internazionali di riferimento per l´attuazione della continuità operativa, a partire dallo standard britannico BS 25999 e dal BS 25777, fino agli standard ISO 22399, ISO 22301, ISO 24762, ISO 27031 e ISO 27002 e alle linee-guida ITIL ed NFPA (cap. 3).

Particolare rilievo ai fini della disciplina in materia di protezione dei dati personali assumono le parti del provvedimento più strettamente inerenti al disaster recovery e quindi, in particolare, il capitolo 4 relativo alla gestione della continuità operativa, il capitolo 5 concernente la realizzazione della continuità operativa e del disaster recovery (con riferimenti alle tecnologie di cloud computing), nonché il capitolo 6 in tema di "strumenti giuridici e operativi per l´acquisizione di un servizio di disaster recovery" (che tratta, oltre agli aspetti contrattuali dell´acquisizione di servizi, anche i rapporti tra organizzazioni diverse per mutua cooperazione in tema di disaster recovery, fornendo peraltro dei sintetici riferimenti alla disciplina del trasferimento all´estero di dati personali).

I successivi capitoli trattano aspetti che, pur assumendo notevole rilievo rispetto agli obiettivi complessivi di DigitPA, non hanno invece una significativa incidenza sul diritto alla protezione dei dati personali: il capitolo 7 espone infatti le modalità di redazione degli studi di fattibilità tecnica, dei piani di continuità operativa e dei piani di disaster recovery, mentre il capitolo 8 tratta la continuità operativa e il disaster recovery nel contesto delle c.d. infrastrutture critiche senza introdurre specificità di rilievo riguardo agli aspetti di protezione dei dati personali affrontati nei capitoli precedenti. Il capitolo 9 è infine dedicato alle conclusioni.

Costituiscono parte del provvedimento anche cinque appendici, volte a proporre schemi di documenti di analisi e pianificazione, nonché elementi utili ai fini contrattuali.

2. Terminologia.

Con il termine "disastro" si intende, ai fini del provvedimento in esame, "l´effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l´organizzazione", mentre l´espressione "Disaster Recovery" si riferisce all´insieme degli accorgimenti organizzativi, delle soluzioni tecniche e procedurali adottate per garantire il ripristino dello stato di normale funzionamento di un sistema informatico. Nell´ottica dell´articolo 50–bis del CAD, il provvedimento in esame definisce più propriamente la nozione di disaster recovery come "l´insieme delle misure tecniche e organizzative adottate per assicurare all´organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell´organizzazione stessa, anche in siti alternativi a quelli primari/di produzione, a fronte di eventi bloccanti, di qualunque natura, che provochino indisponibilità prolungate".

Il disaster recovery comprende quindi le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e di servizi di comunicazione.

3. Norme vigenti in tema di salvaguardia di dati personali.

Relativamente al "salvataggio periodico", ovvero alle operazioni di backup e recovery dei dati personali che costituiscono la base di qualunque piano di disaster recovery, il Codice in materia di protezione dei dati personali (infra: Codice) prevede già importanti

adempimenti in capo ai titolari del trattamento. In particolare, le pubbliche amministrazioni che nell´ambito delle rispettive attività istituzionali si avvalgono di sistemi informatici e gestiscono con strumenti elettronici banche dati contenenti (anche) dati personali sono già tenute – come ogni altro titolare del trattamento - a proteggerle adeguatamente, mediante l´adozione di idonee misure di sicurezza, al fine di ridurre al minimo il rischio, non solo di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta, ma anche di distruzione o perdita, anche accidentale, dei dati (art. 31 del Codice).

All´articolo 34, comma 1, lettera f), il Codice prevede inoltre, quale misura minima di sicurezza applicabile al trattamento di dati personali effettuato con strumenti elettronici, l´adozione di procedure per la custodia di copie di sicurezza, nonché per il ripristino della disponibilità dei dati e dei sistemi.

Il Disciplinare tecnico allegato "B" al Codice richiede, in proposito (regola 18), che siano impartite "istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale" mentre il Documento programmatico sulla sicurezza obbliga i soggetti tenuti a redigerlo a includervi (regola 19.5) "la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23" nonché a prevedere, nel caso di trattamenti di dati personali sensibili o giudiziari (regola 23), che siano adottate "idonee misure per garantire il ripristino dell´accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni".

Oltre alle citate disposizioni – che sanciscono obblighi di protezione dei dati e dei sistemi in capo al titolare del trattamento in quanto tale – l´articolo 50-bis, comma 3, lettera b), del CAD, impone alle amministrazioni la redazione e il costante aggiornamento dei propri piani di disaster recovery, sulla base di appositi studi di fattibilità tecnica, sui quali deve essere acquisito il parere di Digit-PA.

RITENUTO

Tra le parti del provvedimento che assumono maggiore rilievo ai fini delle competenze di questa Autorità, ve ne sono alcune suscettibili di perfezionamento - al fine di rafforzare le garanzie del diritto alla protezione dei dati personali trattati dalle amministrazioni pubbliche – secondo le modalità di seguito esposte.

4. Modalità di implementazione delle procedure di backup e restore dei dati.
Nell´ambito delle "indicazioni per l´attuazione di una corretta politica di backup" (§ 4.5), si prevede che al fine di ottemperare a regole specificamente indicate e di semplificare i processi di gestione, "è possibile ricorrere a specifici prodotti disponibili sul mercato che automatizzano le operazioni di backup e di ripristino; le specifiche scelte organizzative e di processo devono essere rappresentate all´interno dei documenti programmatici per la sicurezza dovuti a termine di legge".

Dal momento che non tutti i titolari del trattamento sono tenuti alla redazione del Documento programmatico sulla sicurezza (cfr. art. 34, comma 1-bis del Codice), si ritiene che la sede più idonea per documentare le scelte anche implementative in materia di procedure per il salvataggio periodico dei dati sia - oltre al Documento programmatico sulla sicurezza alla cui predisposizione l´amministrazione sia eventualmente tenuta - proprio il Piano sulla continuità operativa e, in quell´ambito, il Piano per il disaster recovery, che dovranno invece essere obbligatoriamente redatti da tutte le pubbliche amministrazioni.

5. Periodo di conservazione dei dati.
5.1. Per quanto riguarda il periodo di conservazione dei dati di backup di cui al paragrafo 4.5.3 del provvedimento ("Periodo di ritenzione") si osserva come la previsione di periodi di

conservazione anche illimitati non sia in generale conforme al principio di finalità nel trattamento di dati personali (cfr. art. 11, comma 1, lett. b) ed e), del Codice).

Occorrerebbe quindi commisurare il periodo di conservazione dei dati di backup alle finalità cui la stessa conservazione è preordinata e, in definitiva, ai tempi di conservazione dell´informazione che si intende salvaguardare mediante le operazioni di disaster recovery.

5.2. In relazione al paragrafo 4.5.7 ("Archiviazioni") che prevede l´archiviazione periodica di tutti o parte dei dati su dispositivi che ne preservino l´integrità per lunghi periodi, si osserva come anche per tale conservazione andrebbero individuati termini definiti, distinguendo le misure necessarie al mantenimento dell´efficiente funzionalità del sistema informativo e alla protezione dei dati in esso trattati dagli accorgimenti preordinati, invece, a realizzare forme di archiviazione storico-documentale.

6. Aspetti di sicurezza dei backup.
Il provvedimento in esame prevede, al paragrafo 4.5.9, che le operazioni di backup e restore dei dati debbano essere effettuate attraverso una rete separata a livello logico (creando opportune segregazioni mediante sotto-reti virtuali) o a livello fisico (con apparati e segmenti di rete dedicati), che le porte di comunicazione dei sistemi di backup debbano essere protette attraverso adeguati "filtri di comunicazione IP" e che le informazioni memorizzate su supporti utilizzati per il backup debbano essere cifrate.

In relazione a tale ultima previsione –volta a soddisfare esigenze di protezione dei dati personali anche in relazione allo smaltimento o al riuso dei supporti usati per la memorizzazione – appare preferibile precisare che le modalità tecniche e organizzative della realizzazione di tali operazioni di cifratura devono essere tali da non pregiudicare la disponibilità dei dati in caso di necessità, assicurando a tale scopo la compatibilità tecnologica dei supporti, dei formati di registrazione, degli strumenti crittografici e degli apparati di lettura dei dati per tutta la durata della conservazione del dato.

7. Clausole contrattuali.
7.1.Relativamente alle indicazioni fornite al capitolo 5 sugli aspetti contrattuali dei servizi di disaster recovery e di backup/restore dei dati, con riferimento alle tecnologie di cloud computing di cui al paragrafo 5.3.2.3 ("Le soluzioni cloud"), appare opportuno precisare che il fornitore del servizio è tenuto a indicare, con apposita dichiarazione resa in sede contrattuale, l´esatta localizzazione geografica dei dati gestiti. Solo attraverso tale previsione, infatti, il titolare del trattamento è in condizione di valutare se questa particolare modalità di realizzazione del servizio rispetti effettivamente la normativa in materia di protezione dei dati personali e segnatamente l´articolo 45 del Codice, che vieta il trasferimento "anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all´Unione europea", qualora "l´ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato", a tal fine valutandosi anche "le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza".

7.2. Sempre nel medesimo paragrafo, appare auspicabile tenere conto, a titolo informativo, anche del recente documento "Cloud computing: indicazioni per l´uso consapevole dei servizi" allegato alla relazione annuale 2010 del Garante, presentata alle Camere il 23 giugno 2011 (reperibile anche online sul sito web istituzionale del Garante all´indirizzo http://www.gpdp.it/garante/document?ID=1819933).

7.3. I paragrafi 6.3.1 e 6.8, nell´ambito di una ricognizione degli "strumenti giuridici e operativi per l´acquisizione di un servizio" di disaster recovery richiamano – quali parametri di cui le

amministrazioni devono garantire il rispetto, anche obbligandovi con opportune clausole contrattuali il prestatore del servizio - le norme del Codice e i provvedimenti del Garante, inerenti in particolare le misure di sicurezza e l´individuazione delle figure dei responsabili, degli incaricati del trattamento e degli amministratori di sistema. In tale contesto sarebbe opportuno richiamare, a titolo informativo, anche il provvedimento emanato dal Garante in data 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il cui testo è consultabile anche online all´indirizzo http://www.gpdp.it/garante/doc.jsp?ID=1577499.

8. Fattori di rischio e tipologie di dati.
L´appendice C del documento, relativa ai valori per la determinazione della classe di rischio del sistema, annovera la tipologia dei dati trattati tra i vari parametri che devono orientare la determinazione della classe di rischio del sistema. A sua volta, la categoria della tipologia dei dati trattati individua al suo interno varie classi di dati (amministrativi, tecnici, anagrafici semplici, personali sensibili, sanitari, giudiziari) a ciascuna delle quali è attribuito un 'peso specifico´ diverso (cfr. la prima tabella di p. 109).

Per quanto concerne la terminologia, è opportuno utilizzare le definizioni previste dalla normativa di rango primario e, con particolare riferimento ai dati personali, dal Codice. In tal senso, andrebbe sostituito il riferimento alla categoria dei dati "anagrafici semplici" con il riferimento a quella (più ampia e definita dall´articolo 4, comma 1, lettera b), del Codice) dei "dati personali", idonea a ricomprendere tutti i dati personali diversi da quelli sensibili o giudiziari.

Al fine di conformare le previsioni in esame al diverso regime sancito dal Codice per ciascuna tipologia di dati, appare inoltre auspicabile attribuire lo stesso 'peso specifico´ (comunque maggiore di quello conferito ai dati personali "comuni") ai dati personali sensibili e a quelli giudiziari, in quanto soggetti, secondo la normativa primaria, a una disciplina analoga.

Infine, è preferibile accomunare in un´unica tipologia – quali dati "supersensibili" – i dati idonei a rivelare lo stato di salute e quelli idonei a rivelare la vita sessuale, attribuendo loro lo stesso 'peso specifico´ (comunque maggiore di quello attribuito alla categoria dei dati personali sensibili e giudiziari), così da garantire a tale tipologia di dati quella tutela rafforzata riconosciuta dal Codice (cfr., in particolare, art. 60).

IL GARANTE

esprime parere favorevole sullo schema di linee-guida in materia di "Disaster Recovery delle pubbliche amministrazioni", con le seguenti condizioni:

a) il provvedimento preveda l´annotazione delle modalità concrete di effettuazione dei backup, oltre che nel Documento programmatico sulla sicurezza (laddove ne sia prevista la redazione), anche nel Piano di continuità operativa e, al suo interno, nel Piano di disaster recovery (punto 4);

b) ai paragrafi 4.5.3 e 4.5.7 si individuino periodi di conservazione dei dati definiti, commisurandoli alle finalità cui la stessa conservazione è preordinata e, in definitiva, ai tempi di conservazione dell´informazione che si intende salvaguardare mediante le operazioni di disaster recovery (rispettivamente, punti 5.1 e 5.2);

c) al paragrafo 5.3.2.3, si precisi che il fornitore del servizio è tenuto a indicare, con apposita dichiarazione resa in sede contrattuale, l´esatta localizzazione geografica dei dati gestiti (punto 7.1);

e con le seguenti raccomandazioni:

d) consideri l´Amministrazione l´opportunità di prevedere modalità tecniche e organizzative di realizzazione delle operazioni di cifratura di cui al paragrafo 4.5.9 tali da non pregiudicare la disponibilità dei dati in caso di necessità, assicurando a tale scopo la compatibilità tecnologica dei supporti, dei formati di registrazione, degli strumenti crittografici e degli apparati di lettura dei dati per tutta la durata della conservazione del dato (punto 6);

e) al paragrafo 5.3.2.3 si valuti l´opportunità di inserire un riferimento al documento "Cloud computing: indicazioni per l´utilizzo consapevole dei servizi" (punto 7.2);

f) ai paragrafi 6.3.1. e 6.8, valuti l´Amministrazione l´opportunità di richiamare, a titolo informativo, anche il provvedimento emanato dal Garante in data 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (punto 7.3);

g) all´appendice C, nell´ambito della prima tabella di p. 109, si valuti l´opportunità di sostituire il riferimento alla categoria dei dati "anagrafici semplici" con il riferimento a quella dei "dati personali"; di attribuire lo stesso ‘peso specifico´ ai dati personali sensibili e a quelli giudiziari; di accomunare in un´unica tipologia i dati idonei a rivelare lo stato di salute e quelli idonei a rivelare la vita sessuale, attribuendo loro lo stesso ‘peso specifico´ (punto 8).

Roma, 20 ottobre 2011

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
De Paoli