12. Sicurezza, continuità operativa e *disaster recovery*

Il Codice dell'Amministrazione Digitale contiene l'obbligo per gli uffici pubblici di utilizzare le nuove tecnologie per la gestione dei procedimenti amministrativi e l'erogazione di servizi a cittadini e imprese.
Conseguentemente - e con l'obiettivo di creare una PA efficiente, rapida e sicura - il legislatore si è occupato di fornire fornisce precise indicazioni anche in merito alla sicurezza dei nuovi sistemi, per ridurre al minimo i rischi di perdita di dati o di default del sistema.

La sicurezza nell'Amministrazione Digitale

Le Pubbliche Amministrazioni nell'esercizio della propria attività istituzionale raccolgono, producono ed archiviano un'enorme quantità di dati e documenti. In base alle norme fin qui esaminate, tutte queste informazioni devono essere rese disponibili "in modalità digitale". Questo significa che i dati devono essere formati, acquisiti e conservati nei sistemi informatici delle Amministrazioni titolari.
Si tratta di un vero e proprio patrimonio che deve essere tutelato per:
a) mantenere l'integrità, e quindi l'affidabilità, delle informazioni pubbliche;
b) prevenire e limitare i danni da intrusioni e accessi abusivi;
c) evitare possibilità di diffusioni non autorizzate di informazioni;
d) consentire un corretto funzionamento dell'apparato burocratico ed evitare interruzioni nell'erogazione dei servizi *on line*.

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente.
Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurare l'integrità, la riservatezza e la disponibilità delle informazioni archiviate nei sistemi informatici.

La centralità del tema della sicurezza dei sistemi informativi delle Pubbliche Amministrazioni, e quindi dei dati in esse contenuti, trova conferma nell'art. 51 D. Lgs. n. 82/2005.

È importante sottolineare come in tale norma siano indicati i principi cui devono essere improntati i sistemi informativi delle Amministrazioni:
a) integrità ed esattezza dei dati. I dati custoditi nei sistemi devono essere modificati o eliminati solo dai soggetti all'uopo abilitati; è quindi necessario che il sistema sia congegnato in modo tale da prevedere diversi livelli di autenticazione e consentire comunque che rimanga traccia delle diverse operazioni svolte;
b) disponibilità e accessibilità. I dati devono poter essere fruibili alle Amministrazioni e ai cittadini che ne abbiano diritto;
c) riservatezza e confidenzialità. Il sistema deve essere strutturato in modo da evitare il rischio di accessi non autorizzati.

L'art. 51 CAD, che rinvia ad apposite regole tecniche in merito alle modalità per garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture nonché per assicurare che i documenti informatici siano custoditi e controllati in modo tale da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alla finalità della raccolta, affida all'Agenzia per l'Italia Digitale, il compito di:
a)raccordare le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b)promuovere intese con le analoghe strutture internazionali;
c) segnalare al Ministro per la Pubblica Amministrazione e l'Innovazione il mancato rispetto delle citate regole tecniche parte delle pubbliche amministrazioni.

Quelle contenute nel CAD non sono le uniche norme in materia di sicurezza informatica dei sistemi informativi delle Amministrazioni: sul tema della sicurezza informatica nel settore pubblico insistono già molteplici provvedimenti (leggi, direttive, circolari).

Tra questi, va tenuta presente la disciplina in materia di riservatezza dei dati personali (Codice Privacy, D. Lgs. n. 196/2003) che prevede una serie di obblighi di sicurezza per tutti i soggetti, pubblici come privati, che compiano operazioni di trattamento dei dati personali. Il Codice Privacy impone l'adozione di un duplice ordine di cautele in materia di sicurezza - misure minime (art. 33 e All. B) e misure idonee (art. 31) - di cui ogni Ente deve farsi carico congiuntamente: le prime per evitare sanzioni penali e amministrative, le seconde per evitare responsabilità civili.

La continuità operativa e il *disaster recovery*

La crescente complessità dell'attività istituzionale implica un utilizzo sempre più compiuto delle tecnologie dell'informazione e della comunicazione nelle attività delle Pubbliche Amministrazioni. L'azione amministrativa risulta, quindi, esposta a rischi sempre crescenti di interruzione delle attività istituzionali per eventi imprevedibili o catastrofici che possono interessare i sistemi informativi.

In questo scenario il principio costituzionale secondo cui i pubblici uffici sono organizzati in modo da assicurare il buon andamento e l'imparzialità dell'amministrazione (art. 97) si traduce anche nell'obbligo per la PA di salvaguardare l'integrità e la disponibilità del patrimonio informativo (dati e risorse software) in proprio possesso, in quanto quest'ultimo costituisce il presupposto necessario per assicurare la continuità dei servizi resi all'utenza.

Si rende, quindi, necessaria – oltre alla prevenzione delle possibili interruzioni del servizio – la predisposizione di strumenti ed attività in grado di minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che abbia colpito un'amministrazione pubblica o parte di essa .

La casistica dei possibili eventi in grado di compromettere la funzionalità di un sistema informatico e l'integrità dei dati è piuttosto varia, tra i più comuni vi sono i malfunzionamenti dei processi organizzativi implementati dal servizio ICT, malfunzionamento di sistemi, applicazioni e infrastrutture, attacchi esterni al sistema, eventi naturali di tipo accidentale, disastri (intesi come l'effetto di un evento improvviso che determina danni e/o perdite per l'organizzazione gravi e prolungati).

In proposito, con l'espressione "continuità operativa" viene indicata la capacità dellorganizzazione di proseguire l'esercizio delle proprie attività istituzionali anche di fronte ad eventi disastrosi che possono colpirla. Si tratta di un requisito che un'organizzazione può avere solo a grazie ad un'attenta analisi dei rischi, seguita da una attenta programmazione degli interventi.

Attraverso queste misure è possibile garantire la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività in caso di eventi disastrosi. Intesa in questo senso, la continuità operativa travalica l'ambito informatico (cui tecnicamente è riferita) e va ad interessare l'intera funzionalità dell'organizzazione amministrativa, compresi gli aspetti fisici e organizzativi dell'Amministrazione e le persone necessarie per il suo funzionamento. L'obiettivo della continuità operativa è quello di riportare l'intera struttura amministrativa, che si avvale del sistema informativo, alle condizioni antecedenti ad un evento disastroso.

La centrale importanza che i sistemi informatici rivestono nell'Amministrazione digitale impone agli uffici di occuparsi – nell'ambito della continuità operativa - di "*disaster recovery*"; con tale termine si intendono gli accorgimenti organizzativi e le soluzioni tecnico-procedurali adottate per garantire il ripristino dello stato di un sistema Informatico (o di parte di esso), compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

La continuità operativa, nell'implementazione dei sistemi di *e-governement*, costituisce un momento dotato di forte valenza strategica: essa, infatti, assicura la reale disponibilità dei servizi *on-line* superiore a quella degli accessi tradizionali tramite sportello.

Gli obblighi in materia di continuità operativa per le PA

L'articolo 50-bis del CAD (che attiene alla "Continuità operativa") delinea gli obblighi, gli adempimenti e i compiti che spettano alle pubbliche amministrazioni in materia di continuità operativa.

In particolare, è previsto che tutti gli Enti tenuti all'applicazione del CAD debbano e definire piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività; a tal fine definiscono un vero e proprio piano di continuità operativa e di *disaster recovery*.

Tutte le Pubbliche Amministrazioni, a partire dal 25 aprile 2012, sono chiamate a predisporre:

– il piano di continuità operativa, che fissa obiettivi e principi da perseguire oltre a contenere la descrizione delle procedure per la gestione della continuità operativa (anche affidate a soggetti esterni). Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

– il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa ed individua le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

La norma, per razionalizzare i processi di implementazione della continuità operativa, ha individuato una serie di obblighi ed adempimenti ripartiti tra Agenzia per l'Italia Digitale, Pubbliche Amministrazioni, e Ministero per la pubblica amministrazione e l'innovazione.

Innanzitutto, è previsto che i piani siano adottati sulla base di appositi e dettagliati studi di fattibilità tecnica sui quali deve essere acquisito il parere obbligatorio dell'Agenzia per l'Italia Digitale.

La normativa, inoltre, attribuisce all'Agenzia per l'Italia Digitale un ruolo fondamentale nei processi di realizzazione e di attuazione dei piani di *disaster recovery*. In particolare, nell'ambito dei piani di *disaster recovery*, l'Agenzia:

– definisce, sentito il Garante per al protezione dei dati personali, le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche;

– verifica annualmente il costante aggiornamento dei piani di *disaster recovery* delle Amministrazioni interessate;

– informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

Infine, al Ministro per la Pubblica Amministrazione e l'innovazione è affidato il compito di assicurare l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni, anche sulla base delle informative annuali che l'Agenzia per l'Italia Digitale è tenuta a comunicargli relativamente all'aggiornamento dei piani di *disaster recovery* delle Amministrazioni.

Riferimenti Normativi	*D. Lgs. n. 82/2005: artt. 50-bis, 51, 71 – D.Lgs. n. 196/2003: artt. 31, 33, All. B*
Regole tecniche e provvedimenti attuativi	- *Linee Guida per il disaster recovery delle PA* - *Provvedimento Garante Privacy n. 394/2011* - *Circolare DigitPA n. 58/2011*
Tag	*Organizzazione, Sicurezza, Diritti digitali*
Voci di glossario	*Cloud computing - Continuità operativa/disaster recovery – Infrastruttura critica - Piano della sicurezza del sistema di conservazione - Piano della sicurezza del sistema di gestione informatica dei documenti - Piano di continuità operativa (PCO) - Piano di Disaster Recovery (PDR) - Politiche di sicurezza - Responsabile del trattamento dei dati - Responsabile della sicurezza*