STUDIO LEGALE CIACCI
Diritto delle nuove tecnologie

Relazione

sulle misure di sicurezza nelle attività di trattamento di dati personali secondo quanto previsto dal

D.Lgs. 30 giugno 2003 n. 196

e dalla disciplina di settore

Via Nomentana, n. 373, 00162 ROMA
Tel. 06/86327973 - Fax 06/83390932 e-mail: *studiociacci@jei.it* - web-site: *http://www.jei.it*

1. Una breve premessa: il contesto giuridico di riferimento.

Le misure di sicurezza sono quegli accorgimenti tecnici da porre in essere al fine di proteggere i dati personali oggetto del trattamento da una serie di rischi: in particolare quelli, come stabilito dall'art. 31 del D.Lgs. 30 giugno 2003 n. 196 (detto Codice della privacy), "di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Spesso confuse con la globalità degli adempimenti previsti dalla complessa disciplina in materia, mentre ne rappresentano solo una parte (a cui si deve unire quella relativa all'osservanza degli obblighi di natura maggiormente giuridica, come ad esempio per la redazione dell'informativa, o per le nomine di incaricati o responsabili), sono disciplinate dal Titolo V della Parte I del Codice, e dettagliate nei loro aspetti maggiormente tecnologici dal suo Allegato B, denominato appunto "Disciplinare tecnico in materia di misure di sicurezza"; ulteriori norme che si riferiscono a questo argomento si riscontrano poi in specifici interventi normativi degli ultimi anni, anche non specificamente dettati per il settore in esame, come nel caso del D.L. 9 febbraio 2012, n. 5, intitolato "*Disposizioni urgenti in materia di semplificazione e di sviluppo*", convertito con modificazioni dalla L. 4 aprile 2012, n. 35.

Delle misure di sicurezza si possono effettuare diverse classificazioni.

2. Classificazione delle misure di sicurezza.

Tali accorgimenti tecnici richiesti obbligatoriamente dalla normativa in materia possono infatti inizialmente dividersi in due diverse tipologie, da cui derivano importanti conseguenze soprattutto a livello di responsabilità conseguenti alla loro inosservanza: da una parte, abbiamo le misure di sicurezza c.d. "idonee", disciplinate in particolare dall'art. 31 del D.Lgs. 196/2003, le quali, se adottate correttamente, esonerano da qualsiasi tipo di responsabilità (civile o penale) il titolare del trattamento; dall'altra, quelle c.d. "minime", la cui regolazione è riscontrabile negli artt. 33 e ss. e nell'Allegato B del D.Lgs. 196/2003, le quali, se adottate correttamente, eliminano per il titolare esclusivamente la responsabilità penale e quella amministrativa, ma non quella civile.

A seconda poi delle modalità con cui viene effettuato il trattamento delle informazioni relative all'individuo, ed identificative dello stesso, se con strumenti

elettronici o senza di essi (e quindi essenzialmente attraverso i tradizionali metodi collegati all'uso della carta), si distinguono alcuni tipi di accorgimenti tecnici da altri, e di conseguenza l'applicazione di alcune norme o di altre: in particolare, l'art. 34 del D.Lgs. 196 e gli artt. 1-26 del suo Allegato B per i trattamenti con strumenti elettronici; l'art. 35 e gli artt. 27-29 dell'Allegato B per i trattamenti senza tali strumenti.

2.1. *Le misure di sicurezza "idonee" e "minime".*

L'art 31 del D.Lgs. 196/2003 descrive quali sono le misure di sicurezza idonee, utilizzando una formulazione aperta, non analitica [1]: questo perché le misure idonee non possono essere determinabili a priori in maniera puntuale, ma devono rapportarsi a determinati elementi che rendono variabili nelle diverse fattispecie concrete le misure da adottare. Tale impostazione permette poi nel concreto di procedere nell'adeguamento tenendo ben presente la propria struttura, le sue caratteristiche, le modalità dei trattamenti che vengono effettuati e il contesto generale in cui si svolgono: è cioè intuitivo che le misure di protezione che dovrà adottare un istituto di credito (ad esempio, quegli accorgimenti tecnici che devono proteggere dal rischio di accessi esterni non autorizzati), o un laboratorio di analisi, devono essere ben più serie di quelle di una palestra o di un esercizio commerciale.

Gli elementi per determinare in concreto le misure idonee sono:

- *le conoscenze acquisite in base al progresso tecnico*, e quindi il fatto che si debba rapportare la valutazione circa la correttezza della soluzione adottata non rispetto ad un valore assoluto di sicurezza (tra l'altro forse irraggiungibile), ma a quello relativo del c.d. "tecnico medio" (che quindi permette di ricondurre ad un livello di ragionevolezza l'adempimento di questo obbligo);
- *la natura dei dati*, e dunque il fatto che siano più o meno lesivi del diritto alla protezione dei dati personali dell'individuo o di quello alla riservatezza, come nel caso dei dati sensibili o di quelli giudiziari;
- *le specifiche caratteristiche del trattamento*, cioè gli ambiti e le finalità per cui vengono posti in essere.

Se il sistema del D.Lgs. 196/2003 prevede una formulazione "aperta" delle misure idonee, da individuare poi nel concreto tenendo presente i parametri indicati, per una più sicura protezione dei dati personali viene introdotto dall'art. 33 il concetto di

[1] Art. 31: "I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

"misura *minima*" di sicurezza ("i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo - … - volte ad assicurare un livello minimo di protezione dei dati personali"): e quindi elencati con precisione i vari accorgimenti tecnici (si vedano gli artt. 34 e 35 e l'Allegato B al Codice) che devono farsi rientrare in tale concetto.

Distinzione tra tipologie di misure che poi ha una diretta conseguenza sulle responsabilità derivanti dalla loro mancata adozione: qualora il titolare del trattamento non adotti nessuna misura, incorrerà in una triplice responsabilità (penale, civile e amministrativa); nell'ipotesi in cui invece adotti le sole misure minime ne deriverà una responsabilità esclusivamente civile. Al fine di evitare qualsivoglia tipologia di responsabilità dovrà predisporre ambedue gli strumenti di tutela, sia minimi che idonei.

2.2. *Le misure di sicurezza per trattamenti di dati personali con e senza "strumenti elettronici".*

La distinzione analizzata nel presente paragrafo trae la sua fonte dagli articoli 34 e 35 della legge, e si spiega sulla base della considerazione della diversa modalità con cui si effettuano trattamenti di dati personali sulla base della tipologia dello strumento utilizzato: diversa modalità che chiaramente influisce sul tipo di accorgimento tecnico da adottare.

Così, l'articolo 34 del Codice stabilisce che i trattamenti che si svolgono mediante l'ausilio di mezzi elettronici debbano contemplare l'adozione delle seguenti misure per realizzare un sistema minimo di protezione dei dati personali sottoposti a trattamento:

- autenticazione informatica;
- procedure di gestione delle credenziali di autenticazione;
- utilizzazione di sistemi di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito di trattamento per singolo incaricato;
- protezione di strumenti informatici e dati rispetto alla pirateria informatica;
- adozione di procedure di back up e di ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura per i trattamenti di dati sensibili nel caso vengano effettuati da organismi sanitari.

Le misure di sicurezza così enunciate tramite questa semplice elencazione dall'art. 34 vengono poi specificate nel disciplinare tecnico allegato al Codice, quindi nei punti 1-26 dell'Allegato B [2].

Interessante rilevare anche che, a livello di sistema da rendere sicuro, la definizione di "strumenti elettronici" risulta essere amplia: secondo il D.Lgs. 196 (art. 4, comma 3, lett. *b*) sono infatti tali "gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento". In questo modo l'applicazione delle previsioni non deve essere limitata al solo uso del computer, ma anche a tutti gli altri dispositivi che oggi integrano le nuove tecnologie (ad esempio i cellulari, gli *smartphone*, i *tablet*, le videocamere digitali, ...) nel momento in cui vengono utilizzati per trattare dati personali: e si tenga presente, a tale proposito, che "dato personale", nella definizione ampia fornita dal Codice, potrebbe essere considerata anche l'immagine di una persona.

Per quanto riguarda i trattamenti senza gli strumenti elettronici, previsti dall'art. 35 del Codice e dai punti 26-29 dell'Allegato B, è chiaro che la tipologia più rilevante è quella attraverso modalità cartacee, ma potrebbe riguardare anche ulteriori sistemi.

Vediamo quali sono tali misure, tenendo anche in questo caso presente non solo il formalismo richiesto dalla disciplina normativa, ma altresì le varie finalità che stanno alla base di questa tipologia di adempimento (nel dettaglio, come si è detto, evitare la distruzione o perdita, anche accidentale, dei dati personali trattati, l'accesso non autorizzato ad essi, i trattamenti delle informazioni relative all'individuo non consentito o non conforme alle finalità per cui sono stati raccolti e per cui è stato dato il consenso dall'interessato). In particolare quindi:

- agli incaricati sono impartite istruzioni scritte finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- nel procedere all'aggiornamento periodico, da effettuarsi con cadenza almeno annuale, dell'individuazione delle operazioni di trattamento consentite ai singoli incaricati, la lista di questi può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione (la misura che abbiamo visto in ambito informatico vale dunque anche per i documenti cartacei: occorre quindi sempre un profilo di autorizzazione per accedere ai dati);

[2] Si ricorda che il D.L. 9 febbraio 2012, n. 5, convertito con modificazioni dalla L. 4 aprile 2012, n. 35, che ha eliminato l'obbligo del D.P.S. adottando come tecnica normativa l'abrogazione di parti del testo originario del D.Lgs. 196: nella specie, il suo art. 34, lett. *g*, nella parte che si riferiva al documento programmatico sulla sicurezza, e la collegata regola 19 dell'Allegato B.

- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi da questi fino alla restituzione al termine delle operazioni affidate, in modo che ad essi non accedano persone prive di autorizzazione;
- l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato, ossia si deve attivare un sistema di verifica su chi può accedere o non può accedere ai dati, come ad esempio un armadio/archivio chiuso a chiave, e la cui chiave sia in possesso solo delle persone autorizzate;
- le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Avv. Gianluigi Ciacci

ALLEGATO

Check List Per Verifica

Adempimento Misure Di Sicurezza

CHECK LIST PER ADEMPIMENTO MISURE DI SICUREZZA

Adempimento	Si	No	Note
Individuazione degli strumenti a disposizione per il trattamento dei dati			
Attribuzione delle credenziali di autenticazione (*user id* e *password*) ai propri incaricati e responsabili			
Sistema di controllo della congruità delle password (complesse e minimo di 8 caratteri)			
Adozione di un sistema di gestione in caso di password dimenticate o necessità di "accesso forzato" ai sistemi			
Individuazione dei profili di autorizzazione dei propri incaricati e responsabili			
Aggiornamento delle credenziali di autenticazione (scadenza delle password almeno ogni 180 giorni, in caso di trattamenti di dati sensibili ogni 90 giorni)			
Aggiornamento dei profili di autorizzazione dei propri incaricati e responsabili			
Disattivazione credenziali non utilizzate			
Attivazione salvaschermo con parola chiave			
Adozione misure di prevenzione dei rischi di accesso non consentito e/o distruzione dei dati			
Installazione antivirus			
Installazione firewall			
Predisposizione aggiornamento antivirus			
Predisposizione di un sistema di back up di dati e sistemi			

Adempimento	Si	No	Note
Politica di sicurezza dei dati che possono uscire dall'azienda su supporti removibili (chiavette USB) o su PC portatili			
Predisposizione di attività di formazione degli incaricati			
Esistenza e diffusione di un regolamento sull'uso dei sistemi informatici aziendali			
Fissazione delle modalità di accesso agli archivi da parte degli incaricati			
Adozione di misure per la conservazione dei fascicoli			
Protezioni fisiche (chiavi, allarmi o vigilanza) agli archivi contenenti dati (stanza server, archivi cartacei)			
Elaborazione di un prospetto di valutazione dei rischi			
Protezione degli apparati hardware da malfunzionamento (gruppi di continuità, stabilizzatori di corrente)			
Adozione misure di ripristino dei dati e dei programmi in caso di malfunzionamento			
Individuazione e nomina della figura dell'amministratore di sistema			
Implementazione di un sistema di log degli accessi dei soggetti con privilegi da amministratore di sistema			