Le misure di sicurezza per la protezione dei dati personali

di Gianluca Satta (*)

L'articolo illustra brevemente alcuni aspetti critici legati alla sicurezza dei dati personali e analizza, sotto il profilo giuridico, l'evoluzione delle norme in materia di misure di sicurezza, partendo dalla precedente impostazione del Codice della Privacy fino al nuovo approccio alla sicurezza introdotto con il Reg. UE 2016/679.

La sicurezza dei dati personali

Nell'ambito della tutela del diritto alla *privacy*, il tema della sicurezza dei dati personali costituisce da sempre un elemento di assoluta centralità.
Senza entrare nel merito delle evoluzioni storiche del concetto di *privacy* e delle sue interpretazioni dottrinali, la moderna concezione del "diritto alla *privacy*" si può riassumere in una duplice prospettiva: da una parte, il diritto dell'individuo a non vedersi violata la propria sfera privata e, dall'altra, il diritto dell'interessato (colui al quale il dato personale si riferisce) di controllare le proprie informazioni e le modalità di trattamento delle stesse.
Dal punto di vista giuridico, tale concezione è ben consolidata all'interno dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) (1) e dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea (2), in base ai quali il diritto alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è considerato innanzitutto un diritto fondamentale dell'individuo.
Fatta chiarezza sull'origine e sul fondamento giuridico del diritto alla *privacy*, inteso nella sua duplice accezione, è ora più agevole comprendere la forte connessione di tale diritto e con la sicurezza dei dati personali. In questo senso, infatti, la mancata adozione di misure in grado di garantire la sicurezza sui dati personali non può che aumentare il rischio che si producano eventi negativi per gli stessi; conseguentemente, l'assenza di sicurezza costituisce di per se una forma di lesione della sfera privata dell'individuo, il quale si vedrebbe minacciato dall'incombere di eventi pregiudizievoli della propria persona. Allo stesso modo, non può esservi un'efficace forma di controllo delle proprie informazioni e delle modalità di trattamento delle stesse senza l'adozione di misure in grado di abbassare il rischio di eventi lesivi non solo a danno dei dati personali, ma della sfera privata dell'interessato. In altri termini, non può esservi tutela della *privacy* senza l'adozione di misure in grado di garantire la sicurezza dei dati personali.
Tale assunto è ancora più valido se si considera il costante ricorso al trattamento dei dati personali per qualunque operazione o scambio di beni e servizi nella società moderna, sempre più condizionata dall'impiego di nuove tecnologie. Infatti, se è vero che il trattamento informatizzato, da una parte, agevola notevolmente

Note:
(*) Avvocato in Cagliari, cultore in materia di Diritto dell'Informatica delle Nuove Tecnologie presso l'Università degli Studi di Cagliari
(1) L'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) dispone in questo senso: "ogni persona ha diritto al rispetto della propria via privata e familiare, del proprio domicilio e della propria corrispondenza".
(2) L'art. 8 della Carta dei Diritti Fondamentali dell'UE, riporta quanto segue: "1.Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

i processi di gestione dei dati personali, dall'altra, comporta un significativo aumento del rischio di eventi pregiudizievoli a danno degli stessi.
In ragione di questo inscindibile rapporto tra la sicurezza e la tutela del diritto alla *privacy*, il legislatore europeo, già a partire dall'emanazione del primo testo normativo in materia di *privacy* con la Direttiva 95/46/CE (3), seguito poi dal legislatore italiano con la Legge 31 dicembre 1996, n. 675 (4), successivamente abrogata e sostituita dal D.Lgs. 30 giugno 2003, n. 196 (5) (Codice della *Privacy*), hanno introdotto precise regole in materia di misure di sicurezza che, ad oggi, con l'emanazione del Reg. UE 2016/679 (Regolamento Generale in materia di Protezione dei Dati, di seguito anche "RGPD"), sono state sensibilmente modificate nei termini che meglio si illustreranno nel prosieguo.
A conclusione di questa parte introduttiva e prima di affrontare nello specifico la disciplina normativa in materia di misure di sicurezza, occorre fare una doverosa precisazione in merito alla portata semantica dei concetti, già richiamati in questo primo paragrafo, di "protezione dei dati personali" e di "sicurezza dei dati personali", spesso erroneamente utilizzati come sinonimi e, per questo, foriere di equivoci e fraintendimenti. In particolare, in considerazione di quanto già illustrato, l'espressione "protezione dei dati personali" individua ogni forma di tutela del dato come parte della sfera personale dell'individuo (nell'ambito del diritto fondamentale alla *privacy*), mentre con "sicurezza dei dati personali" si indica solo una parte degli obiettivi da raggiungere per garantire la più ampia tutela dei dati personali. In altri termini, la "sicurezza dei dati personali" costituisce una forma di espressione della "protezione dei dati personali" che, a sua volta, designa l'insieme delle regole poste a tutela delle persone fisiche, con riguardo al trattamento delle informazioni personali.

Le misure di sicurezza nel Codice della Privacy

Nella sistematica del D.Lgs. 30 giugno 2003, n. 196 (d'ora in poi "Codice della *Privacy*"), la sicurezza dei dati personali è garantita dall'insieme delle regole dettate nel titolo V, rubricato "Sicurezza dei dati e dei sistemi", nel quale si prevedono due differenti tipologie di misure: le misure minime di sicurezza e le misure idonee di sicurezza. La loro distinzione, oltre che sotto un profilo contenutistico, è fondamentale soprattutto in sede di valutazione delle responsabilità ad esse collegate; infatti, mentre la violazione delle misure minime comporta una responsabilità di natura penale o, in alcuni casi, solo amministrativa, la mancata adozione di misure idonee di sicurezza comporta, invece, una responsabilità esclusivamente di natura civile.
Per meglio comprendere la differenza tra le misure minime e le misure idonee di sicurezza occorre entrare nel merito delle disposizioni normative specificamente previste per ognuna di esse. In particolare, le misure minime di sicurezza, oltre ad essere richiamate dall'art. 33 del Codice della *Privacy* (6), sono disciplinate all'interno dell'Allegato B, il c.d. Disciplinare tecnico in materia di misure minime di sicurezza.
Le misure minime, come si evince dalla stessa espressione lessicale, rappresentano il nucleo minimo indispensabile di misure di sicurezza che ciascun Titolare del trattamento è tenuto ad adottare. Si tratta, in particolare, di una serie di accorgimenti di natura tecnica, informatica, organizzativa e procedurale in grado di garantire un livello di protezione minimo dei dati personali rispetto ai 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." (7).
Seguendo l'ordine presentato all'interno dell'Allegato B, nell'ambito dei trattamenti

Note:
(3) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. (G.U.C.E. n. L 281 del 23 novembre 1995, pag. 0031 - 0050).
(4) Legge 31 dicembre 1996, n. 675 recante "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" (G.U. n. 5 del 8 gennaio 1997 - Suppl. Ord. n. 3).
(5) D.Lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" (G.U. n. 174 del 29 luglio 2003 - Suppl. Ord. n. 123).
(6) L'art. 33 del D.Lgs. 30 giugno 2003, n. 196 prevede che "Nel quadro dei più generali obblighi di sicurezza di cui all'art. 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.".
(7) Art. 31, D.Lgs. 30 giugno 2003, n. 196.

con strumenti elettronici, la prima misura di sicurezza è costituita dall'adozione di un sistema di autenticazione informatica: tale sistema, in particolare, deve essere strutturato in maniera tale da garantire il trattamento dei dati personali con strumenti elettronici esclusivamente da parte di soggetti incaricati dotati di credenziali di autenticazione (8). Complementare alla misura di sicurezza appena esaminata, vi è poi l'obbligo di implementare un sistema di autorizzazione, attraverso l'attivazione di profili di autorizzazione per ciascun incaricato, affinché l'accesso di questi ultimi sia limitato ai soli dati necessari per effettuare le operazioni di trattamento. Infine, tra le altre misure di sicurezza "minime", il legislatore italiano ha previsto l'obbligo di attivare idonei strumenti per la protezione dei sistemi dal rischio di intrusione e dall'azione di programmi atti a danneggiare i sistemi informatici (*antivirus*, *firewall*, e così via), nonché l'aggiornamento dei *software*, il *backup* dei dati e l'adozione di procedure di *data recovery* (9).

Per garantire la sicurezza in materia di trattamento dei dati personali, tuttavia, non è sufficiente adottare le misure di sicurezza esclusivamente in ambito informatico, ma è necessario anche adottarle nell'ambito dei trattamenti svolti senza l'ausilio di strumenti elettronici. Per queste ragioni, nella seconda parte dello stesso Allegato B sono dettate alcune misure minime di sicurezza, di natura prevalentemente logistica e organizzativa, anche per quanto concerne i trattamenti non informatizzati, molto spesso sottovalutati nella loro incidenza sui rischi inerenti la sicurezza dei dati personali (10).

Se il rispetto delle misure minime di sicurezza, tassativamente individuate dal legislatore, da una parte, evita al Titolare del trattamento le sanzioni di natura penale e amministrativa, dall'altra, non basta per evitare il prodursi di eventuali danni nei confronti degli interessati. Per queste ragioni, il legislatore ha stabilito che il Titolare del trattamento è tenuto ad individuare le misure più idonee affinché con il trattamento non siano cagionati danni all'interessato e ai terzi.

Il Regolamento Generale in materia di Protezione dei Dati, rispetto alla precedente disciplina prevista dal Codice della Privacy, ha segnato un netto cambiamento nell'approccio alla sicurezza dei dati personali.

Le misure idonee, quindi, sono il risultato di una scelta bilanciata da parte del Titolare del trattamento tenuto conto delle variabili, previste dall'art. 31 del Codice della *Privacy*, quali: le conoscenze acquisite in base al progresso tecnico, la natura dei dati e le specifiche caratteristiche del trattamento (11). La

Note:

(8) Secondo il punto n. 2, dell'Allegato B, le credenziali di autenticazione "consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.". A ciascun incaricato deve essere assegnata una o più credenziali. Inoltre, l'Allegato B introduce delle regole sulla lunghezza minima delle parole chiave ("almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito") e sulle caratteristiche che devono rispettare ("non contiene riferimenti agevolmente riconducibili all'incaricato"). Infine, sono previste anche alcune regole minime di gestione delle credenziali nel momento del rilascio, durante il loro normale utilizzo e in caso di assenza dell'incaricato. Per una lettura più completa delle misure minime di sicurezza previste per i sistemi di autenticazione informatica, si vedano i punti da 1 a 11 dell'Allegato B al Codice della *Privacy*. Per un approfondimento in merito agli aspetti giuridici e tecnici delle misure minime di sicurezza, si veda M. Farina - F. Voltan, *La nuova privacy*, 2011, pag. 46 ss.

(9) Sulle misure di sicurezza citate, in questa sede, è inevitabile sottolineare come l'Allegato B preveda dei tempi di aggiornamento di almeno sei mesi per i programmi quali gli *antivirus*, o addirittura, una volta all'anno per i programmi per elaboratore in generale. Allo stesso modo, il *backup* dei dati è previsto con "frequenza almeno settimanale", mentre di sette giorni è il termine massimo stabilito per garantire il ripristino dei dati. Come è evidente, quantomeno per le tempistiche esaminate, si tratta di misure di sicurezza, al giorno d'oggi, del tutto fuori da ogni logica di sicurezza informatica ma che, al momento della loro introduzione, rappresentavano un giusto *standard* di sicurezza minimo da garantire.

(10) Tra le misure minime di sicurezza in ambito non informatico, oltre al controllo degli accessi fisici agli archivi, l'Allegato B prevede anche l'introduzione di specifiche istruzioni ai soggetti che eseguono le operazioni di trattamento, finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali.

(11) L'art. 31 del D.Lgs. 30 giugno 2003, n. 196, stabilisce che "I dati personali oggetto di trattamento sono 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.".

mancata adozione delle misure idonee di sicurezza, quando è fonte di pregiudizio, ai sensi dell'art. 15 del Codice della *Privacy* e del richiamato art. 2050 del Codice civile, il Titolare del trattamento è tenuto a risarcire l'eventuale danno cagionato (12).

La nuova disciplina delle misure di sicurezza nel Regolamento

Il Regolamento Generale in materia di Protezione dei Dati, rispetto alla precedente disciplina prevista dal Codice della *Privacy*, ha segnato un netto cambiamento nell'approccio alla sicurezza dei dati personali.
Come già evidenziato in precedenza (13), infatti, il sistema del doppio binario, basato sulla preventiva individuazione delle misure minime di sicurezza, si è dimostrato inefficace dinanzi ai rapidi cambiamenti legati all'uso delle nuove tecnologie e all'incombere di nuove minacce per la sicurezza dei dati personali (14). Per queste ragioni, al fine di garantire la massima tutela dei dati personali, il legislatore europeo non ha previsto obblighi generalizzati di adozione di misure "minime" di sicurezza, bensì ai titolari e ai responsabili del trattamento ha attribuito l'onere di valutare, caso per caso, le misure di sicurezza più adeguate in rapporto ai rischi specificamente individuati. Tale nuovo approccio, pienamente in linea con il principio di responsabilizzazione che pervade l'intero impianto normativo del Regolamento, in linea di principio, consente di assicurare la massima tutela possibile per i dati personali, senza il ricorso all'individuazione *a priori* delle misure di sicurezza (15).
Secondo la nuova impostazione del Regolamento, inoltre, la sicurezza dei dati personali è inquadrata all'interno del più ampio principio generale di "integrità e riservatezza", a cui tutti i trattamenti devono conformarsi; in particolare, in forza del suddetto principio, i dati personali devono essere sempre "trattati in maniera da garantire un'adeguata sicurezza [...], compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (16).
Passando all'esame delle disposizioni in materia di misure di sicurezza, come in parte già anticipato sopra, l'art. 32 del Regolamento ha introdotto l'obbligo in capo al titolare e al responsabile del trattamento di adottare "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". Lo stesso articolo, al paragrafo 2, ha previsto che "Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.".
Per individuare correttamente le misure più adeguate, quindi, è necessario procedere ad una attenta valutazione di tutti i fattori di rischio inerenti i trattamenti effettuati, in particolare, con riferimento a: trattamenti automatizzati e non, apparati utilizzati per effettuare il trattamento, locali ove sono ospitati i dati personali e i sistemi di memorizzazione dei dati stessi. Inoltre, dal tenore letterale della disposizione in esame ("in special modo") emerge chiaramente come il legislatore non abbia inteso limitare la valutazione dei fattori di rischio ai soli eventi ivi elencati e che, pertanto, i titolari del trattamento sono chiamati ad effettuare una valutazione del rischio che

Note:
(12) Per un maggiore approfondimento sulla responsabilità civile derivante dalla mancata adozione delle misure idonee di sicurezza, si veda M. Farina, *Fondamenti di diritto dell'informatica*, 2012, pag. 183 ss.
(13) Vedi nota n. 9 del presente articolo.
(14) Gli effetti dell'evoluzione tecnologica sui dati personali sono ben evidenziati anche nel considerando n. 6 del Regolamento, in cui si rileva che "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso Paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.".
(15) In questo modo, secondo il principio della neutralità tecnologica, si evita anche l'effetto della rapida obsolescenza delle disposizioni normative che impongono il ricorso ad una determinata tecnologia, come è accaduto per le misure minime di sicurezza previste dall'Allegato B del Codice della *Privacy*.
(16) Art. 5, par. 1, lett. f), RGPD.

comprenda ogni tipo di evento la cui probabilità di realizzazione sia anche minima.
Esaurita questa prima fase valutativa, lo *step* successivo sarà quello di identificare ed implementare le misure di sicurezza "tecniche e organizzative adeguate" in grado di ridurre al minimo l'incidenza dei rischi individuati, tenendo conto di una serie di elementi indicati dall'art. 32 del Regolamento, quali: lo stato dell'arte (17) e i costi di attuazione (18), la natura, l'oggetto, il contesto e le finalità del trattamento, nonché il rischio per i diritti e le libertà delle persone fisiche (19).

Per individuare correttamente le misure più adeguate alla tutela della privacy secondo le nuove imposizioni, è necessario procedere ad una attenta valutazione di tutti i fattori di rischio inerenti i trattamenti effettuati.

Lo stesso articolo, inoltre, con una elencazione meramente esemplificativa, suggerisce l'adozione di alcune tipologie di misure di sicurezza tecniche e organizzative. La prima misura di sicurezza indicata è la "pseudonimizzazione", definita dal Regolamento come il "trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (20). In particolare, si tratta di una misura molto importante tanto che rientra fra quelle ritenute idonee a soddisfare il principio della "*data protection by design and by default*" (art. 25 del Regolamento). Inoltre, come rilevato dal legislatore al considerando n. 28 del Regolamento, pur non escludendo la rilevanza e l'adozione di altre forme di protezione dei dati, l'applicazione della pseudonimizzazione può contribuire a ridurre i rischi per gli interessati e aiutare i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati.
La "cifratura", invece, consiste in una forma di protezione dei dati personali in grado di rendere inintelligibili ai terzi, non in possesso della chiave di cifratura, le informazioni relative alle persone fisiche cui si riferiscono. In particolare, tale misura di sicurezza riveste una funzione molto importante in caso di accesso non autorizzato, sottrazione dei dati personali e ogni altro evento che comporta la divulgazione dei dati a soggetti non autorizzati; inoltre, la violazione dei dati personali sottoposti a cifratura, in astratto, potrebbe essere valutata priva di rischi per i diritti e le libertà degli interessati e, pertanto, non darebbe luogo alla necessaria notifica all'autorità di controllo e alla comunicazione della violazione agli interessati (c.d. *data breach*) (21).
Proseguendo nell'ordine, l'art. 32 del Regolamento suggerisce anche l'adozione di misure di sicurezza in grado di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (22). All'interno di questa categoria rientrano, ad esempio, tutte le misure tecniche e organizzative in grado di prevenire accessi abusivi ai sistemi di trattamento, l'intercettazione, la sottrazione, l'alterazione, la perdita, la copia abusiva dei dati, nonché l'accesso non autorizzato nei locali e negli archivi (23). Per quanto concerne, invece, l'integrità e la disponibilità dei dati occorre riflettere anche sui rischi inerenti i locali ove sono ospitati i dati

Note:
(17) La scelta deve tenere conto delle tecnologie e delle soluzioni che il mercato offre al momento della valutazione.
(18) La considerazione dei costi di attuazione comporta una scelta parametrata alla ragionevole capacità di spesa del titolare; in questo senso, ad esempio, a parità di condizioni di trattamento, ad una piccola azienda dal fatturato modesto non potranno essere richieste le medesime misure di sicurezza di un grosso istituto bancario.
(19) La valutazione di adeguatezza delle misure deve anche considerare, quindi, il numero di dati e di interessati coinvolti, la natura del dato (ad esempio, se il dato fa parte delle categorie previste dall'art. 9 e 10 RGPD), le categorie di interessati particolarmente deboli (ad esempio, soggetti minori o disabili) e così via.
(20) Art. 4, par. 1, n. 5, RGPD.
(21) L'art. 33 del Regolamento prevede che "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".
(22) Art. 32, par. 1, lett. b), RGPD.
(23) A mero titolo esemplificativo, per ridurre al minimo tali rischi, è possibile adottare le più comuni misure di sicurezza di tipo tecnico, quali: sistemi di autenticazione e autorizzazione, dotazione di *software antivirus* aggiornati, *firewall*, memorizzazione di *logfiles*, impianti di videosorveglianza e controllo degli accessi. Inoltre, tra le misure di sicurezza di tipo organizzativo, è possibile individuare e impartire istruzioni precise al personale addetto al trattamento dei dati, assicurare la continua formazione del personale, utilizzare armadi e archivi con chiusure a chiave.

personali, quali il rischio di incendi, di cedimenti strutturali, e quelli di tipo sismico.
Secondo le indicazioni del Regolamento, inoltre, è opportuno anche adottare misure di sicurezza che assicurino la possibilità di "ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico" (24); in questo senso, sarebbe opportuno considerare tutti i rischi derivanti dall'interruzione o dalla mancanza di energia elettrica, necessaria per alimentare i sistemi utilizzati per il trattamento, così come i rischi dovuti ai malfunzionamenti dei sistemi *hardware* e *software* (25).
Infine, l'ultima delle misure di sicurezza raccomandate all'art. 32 del Regolamento, prevede l'adozione di "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" (26). Quest'ultima indicazione, pur facendo parte di un elencazione non tassativa, rappresenta un adempimento essenziale per garantire nel tempo la costante adeguatezza delle misure di sicurezza tecniche ed organizzative implementate. Inoltre, la previsione di una procedura in grado di monitorare e valutare le misure di sicurezza rientra tra gli obblighi di responsabilizzazione previsti in capo al titolare del trattamento, in quanto consente a quest'ultimo di dimostrare l'adeguatezza delle proprie scelte e, quindi, il rispetto degli obblighi in materia di sicurezza (27).
Per quanto concerne, invece, le sanzioni previste per il mancato rispetto delle norme in materia di misure di sicurezza, attualmente l'unico riferimento normativo è dato dall'art. 83 del Regolamento che stabilisce l'applicazione delle sanzioni amministrative pecuniarie dello scaglione più basso (fino a dieci milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo) (28).

Conclusione

In conclusione, quindi, considerato il nuovo approccio richiesto per garantire l'adeguata sicurezza dei dati personali e vista l'assenza di una preventiva determinazione delle misure di sicurezza concretamente applicabili, per i titolari del trattamento sarà fondamentale effettuare una completa e scrupolosa valutazione dei rischi, seguita poi dall'adozione delle misure di sicurezza adeguate, scelte sulla base delle migliori conoscenze disponibili sul mercato (29).

Note:
(24) Art. 32, par. 1, lett. c), RGPD.
(25) Oltre ai comuni sistemi di *backup* e *data recovery*, alcune misure di sicurezza efficaci potrebbero essere rappresentate dall'utilizzo di apparati in grado di garantire la continuità dell'energia elettrica (gruppi di continuità - UPS), dalla certificazione degli impianti elettrici e, infine, dalla predisposizione di procedure in grado di garantire la tempestiva manutenzione dell'*hardware* e del *software*.
(26) Art. 32, par. 1, lett. d), RGPD.
(27) Sul punto si veda l'art. 5, par. 2, RGPD.
(28) Per una completa valutazione del quadro sanzionatorio si dovrà attendere l'esito delle modifiche del Codice della *Privacy* ad opera dei decreti delegati in forza dell'art. 13, Legge 25 ottobre 2017, n. 163.
(29) L'art. 32, par. 3, del Regolamento prevede anche la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, in attesa che tali meccanismi e certificazioni siano resi operativi, la stessa Autorità Garante per la Protezione dei Dati Personali non ha escluso la possibilità di realizzare un documento contenente le linee guida o buone prassi che tutti i titolari potranno utilizzare come punto di riferimento per la corretta individuazione delle misure di sicurezza più adeguate.