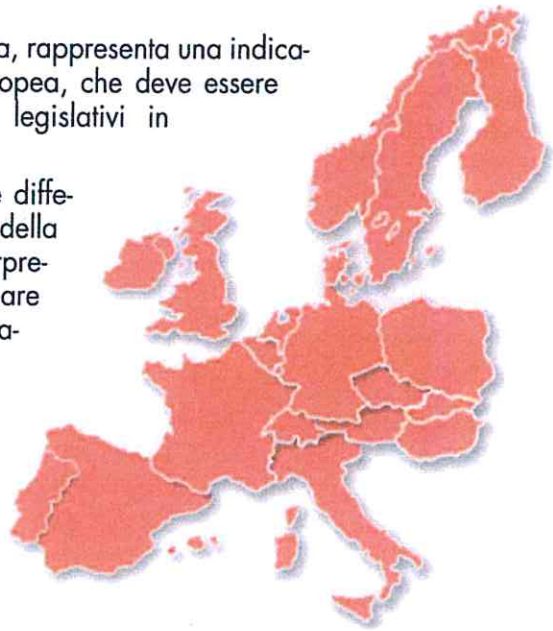
INDICE

IL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

Ricordiamo ai lettori che in Italia dopo la legge 675/1996, è oggi vigente il decreto legislativo 196/2003, che dà attuazione ad una direttiva europea, in tema di protezione dei dati personali.

Una direttiva, per sua natura, rappresenta una indicazione della Commissione europea, che deve essere recepita con provvedimenti legislativi in ogni nazione.



Ciò porta ad una possibile differente attuazione dei principi della direttiva, in funzione di interpretazioni nazionali. Con il passare del tempo, queste interpretazioni possono diversificarsi sempre più, fino a far venir meno il principio di libera circolazione dei dati personali in tutta Europa, che è il fondamento giuridico della direttiva.

La Commissione europea, rendendosi conto che ormai la differenza di approccio alla protezione dei dati personali, nelle varie nazioni europee, aveva raggiunto un livello insostenibile, creando grosse difficoltà a coloro che dovevano trasferire dati da un paese all'altro, ha deciso di avviare la procedura, che ha portato alla pubblicazione di un regolamento.

Il regolamento, sempre per accordo europeo, deve essere recepito integralmente, senza modifiche, in tutti i Paesi europei e quindi garantisce quella omogeneità di trattamento dei dati, che nel corso degli anni si era smarrita.

D'altro canto, l'emissione di un regolamento è faccenda assai complessa, proprio perché è vincolante in ogni Paese. Ecco perché all'inizio del 2012 la Commissione europea presentò una proposta di regolamento, che venne successivamente esaminata dalla commissione LIBE del parlamento europeo (Commissione per le libertà civili, la giustizia e gli affari interni) e successivamente dal consiglio dell'Unione europea. Il procedimento di approvazione del regolamento, che prevede colloqui trilaterali tra la commissione, il Parlamento e il Consiglio della Unione europea, è andato avanti per anni, con successive edizioni di proposte di regolamento, modifiche ed integrazioni.

La versione finale fu approvata all'inizio del 2016 e votata a larghissima maggioranza dal Parlamento europeo. A questo punto l'iter legislativo si è concluso e il regolamento europeo sulla protezione dei dati personali è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea, diventando a tutti gli effetti vincolante per tutti i Paesi membri.

Stante le significative differenze che il regolamento ha introdotto, rispetto alla precedente direttiva, è stato concesso un lasso di tempo di due anni, ai Paesi europei, per dare piena attuazione alle disposizioni del regolamento, che comunque entra in vigore il 29 maggio 2016.

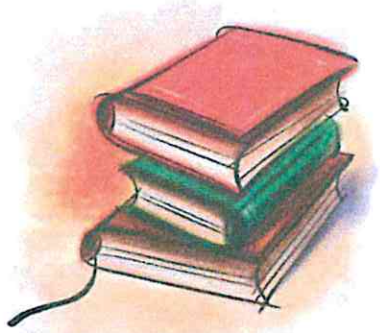
Giova rammentare che, seguendo un iter legislativo simile, in pari data è stata approvata dal Parlamento europeo la direttiva

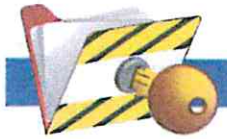
relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

È opportuno che i lettori abbiano conoscenza della approvazione di questa direttiva, in quanto molte disposizioni legislative, illustrate nel regolamento, si ripetono anche essa.

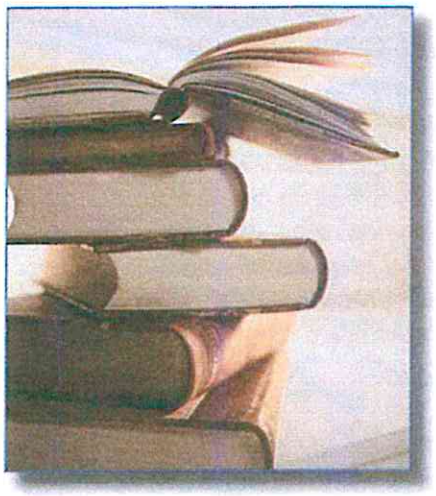
Il nuovo regolamento ha introdotto tutta una serie di nuove figure, o per meglio dire in parte nuove ed in parte con compiti diversi, rispetto a quelle illustrate nel precedente decreto legislativo.

Pur lasciando un certo margine di libertà ai singoli Paesi nel dare attuazione ad alcune misure del regolamento, il legislatore europeo si è preoccupato di introdurre dei meccanismi di coerenza, che hanno proprio l'obiettivo di evitare quella diversificazione di regole, nei vari Paesi europei, che ha portato alla decisione di introdurre un regolamento, anziché una direttiva.





Sono stati inoltre potenziati i diritti degli interessati, cioè dei soggetti cui i dati personali si riferiscono.



Severe disposizioni si applicano in caso di violazione dei dati, con interventi radicali e allargati, rispetto alle precedenti assai più morbide disposizioni legislative.

L'evoluzione dello scenario di trattamento dei dati, che prevede il trasferimento di questi dati nel *cloud* e che permette sempre più spesso il trattamento degli stessi dati tramite *smartphone*, con possibile memorizzazione su chiavetta USB, pone nuovi rischi, che occorre mettere tempestivamente sotto controllo, attuando misure innovative e sensibilizzando in modo appropriato gli incaricati del trattamento.

Meritano anche particolare attenzione le sanzioni, che sono cresciute in misura straordinaria proprio perché è fermo intendimento dei legislatori europei convincere, con le buone o con le cattive, i titolari del trattamento a rispettare puntualmente i dettati legislativi.

I PERSONAGGI E LE ISTITUZIONI COINVOLTI NELLA TUTELA DEI DATI

Prima di procedere all'illustrazione dettagliata delle disposizioni del nuovo regolamento, è bene presentare ai lettori i personaggi e le istituzioni, che sono coinvolti nell'attuare queste disposizioni.

Come i lettori vedranno, alcune figure sono già note, mentre altre sono affatto nuove.

IL TITOLARE DEL TRATTAMENTO

Questa figura è certamente ben nota a tutti coloro che si occupano di protezione dei dati personali, perché è la persona fisica o giuridica, cui competono tutte le responsabilità in merito ad un corretto trattamento di dati personali.

Salvo alcune modifiche, il profilo del titolare del trattamento è simile al titolare, illustrato nel decreto legislativo 196/2003, anche se, in fase di elaborazione della procedura legislativa europea, si sono verificate alcune sorprese. Nell'iniziale traduzione in italiano della bozza di regolamento, infatti, il titolare del trattamento era stato chiamato responsabile del trattamento, che in Italia è tutt'altro personaggio. Una forte pressione nei confronti dei traduttori, cui ha contribuito anche chi scrive, ha permesso di correggere proprio all'ultimo minuto il testo in italiano del regolamento, riportando in auge la figura del titolare del trattamento, che in Italia era già ben nota.

In particolare, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al regolamento europeo. Non solo è posto un obbligo al titolare di dimostrare, in caso di ispezioni, il rispetto delle indicazioni del regolamento, ma si impone anche che queste misure vengano riesaminate e aggiornate quando necessario. Se poi il titolare tratta dati che hanno caratteristiche particolari, come ad esempio dati biometrici, dati sanitari, dati afferenti a convincimenti religiosi o ad affiliazioni sindacali, gli è fatto obbligo di adottare ulteriori e più incisive misure di protezione.

IL RESPONSABILE DEL TRATTAMENTO

Anche questo personaggio era in Italia già ben noto, in quanto gli era stata attribuita la funzione di sostegno operativo, per così dire, del titolare del trattamento.

Al proposito, è bene ricordare che il titolare del trattamento è tale, perché si trova al vertice dell'organizzazione che tratta i dati; ciò, però, non significa che egli abbia una specifica competenza su questi delicati argomenti tecnici. Ecco la ragione per la quale il regolamento gli permette di avvalersi dell'opera di un soggetto competente, che lo potrà aiutare negli adempimenti di legge.

La situazione è alquanto simile a quella che i lettori già conoscono, in relazione al decreto legislativo afferente la sicurezza nell'ambiente di lavoro. In questo caso tutte le responsabilità sono in

capo al datore di lavoro, ma egli può richiedere l'affiancamento di uno specialista, il famoso responsabile del servizio prevenzione e protezione, che lo aiuti nel dare piena attuazione al decreto legislativo in questione.

Il regolamento introduce una differenza rispetto alla legislazione preesistente, in quanto, mentre in precedenza la designazione di un responsabile del trattamento era facoltativa, nella fattispecie la designazione del responsabile è praticamente obbligatoria, non solo per la ben maggiore complessità degli adempimenti previsti dal regolamento europeo, ma anche perché è ben difficile che il titolare abbia la possibilità di gestire in prima persona, con risorse e competenze sufficienti, il rispetto degli adempimenti stessi.

Questa differente impostazione fa sì che il ruolo del responsabile del trattamento sia ben più impegnativo, rispetto al precedente profilo, creando tutt'una serie di opportunità professionali, per coloro che decideranno di acquisire le competenze necessarie e mettersi a disposizione dei titolari, che indubbiamente avranno bisogno di supporti specializzati.

Non per nulla, il rapporto fra il titolare ed il responsabile del trattamento deve essere puntualmente contrattualizzato, se il responsabile è soggetto esterno, o comunque è compito del titolare dare precise istruzioni di comportamento al responsabile prescelto, sia che esso sia dipendente, sia che esso sia consulente terzo.

Appare evidente, per la possibile mancanza di sufficiente esperienza e conoscenza da parte del titolare, che il contratto in questione sia redatto congiuntamente.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Ci troviamo davanti ad un soggetto affatto nuovo, mai prima contemplato in Italia. Questa è la ragione per la quale vale la pena di illustrare in ampio dettaglio il profilo e le competenze di questa persona, che dà un contributo determinante nel rispetto delle regole corrette di trattamento dei dati.

Tanto per cominciare, non tutti i titolari debbono designare un responsabile della protezione dei dati. Durante la fase di elaborazione del documento legislativo, l'articolo nel quale si elencano le attività di trattamento per le quali è obbligatoria la designazione di un responsabile a protezione dei dati, è stato più volte modificato. Nella versione finale, l'obbligo di designazione del responsabile della protezione dei dati si ha ogni qual volta:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate procure e tribunali;
- le attività del titolare fanno riferimento a trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati, su larga scala;
- le attività del titolare fanno riferimento a trattamenti, anch'essi su larga scala, di categorie particolari di dati personali e dati relativi a condanne penali o a reati.

È facile rilevare che i titolari che debbono designare un responsabile della protezione dati personali sono numerosissimi, perché tutti gli enti pubblici, come comuni, province, regioni, agenzie di varia natura e simili, rientrano certamente in questo obbligo.

Un po' più sfumato è il caso illustrato al secondo punto, dove si parla di trattamenti che richiedono un monitoraggio su larga scala. Vi possono essere pochi dubbi sul fatto che le catene di supermercati e le autorità che gestiscono grandi impianti di videosorveglianza, ad esempio nell'ambito di centri commerciali, parcheggi, reti metropolitane, aeroporti, indubbiamente debbano designare un responsabile della protezione dei dati personali.

La terza categoria di trattamenti, che ricadono in questo obbligo, fanno riferimento ad aziende sanitarie, per dare solo un esempio di enti che trattano dati particolari.

Anche in questo caso, il responsabile della protezione dei dati può essere soggetto dipendente dal titolare, oppure soggetto terzo esterno sotto contratto.

Quest'ultima soluzione appare evidentemente più garantistica, perché può diminuire le capacità di influenza del titolare o del responsabile su questo soggetto che, in un certo senso, deve *"fare le bucce"* alle modalità di trattamento messe in atto dal titolare.

Questa è la ragione per la quale il regolamento, all'articolo 38, si preoccupa che *"il responsabile della protezione dei dati*

non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Inoltre esso non può essere rimosso o penalizzato dal titolare, in fase di adempimento dei propri compiti". Come ben si vede, il legislatore europeo si è preoccupato di proteggere in ogni modo questo soggetto da possibili influenze, più o meno coercitive.

Al proposito, giova rammentare che in precedenti edizioni del regolamento si imponeva addirittura che il responsabile, una volta assunto o messo sotto contratto, non potesse essere licenziato prima di un certo periodo di tempo, proprio per proteggerlo da possibili pressioni.

I compiti del responsabile della protezione dei dati fanno riferimento alla fornitura di consulenza al titolare, nonché a tutti gli incaricati, in merito agli obblighi derivanti dal regolamento. Ciò significa ad esempio, che il responsabile della protezione dei dati può intervenire nell'allestire corsi di formazione per tutti i soggetti coinvolti. Anzi, questa particolare attività è proprio prevista all'articolo 39, comma 1, lettera b).

Un altro importante ruolo attribuito a questo responsabile è di fungere da mediatore fra l'autorità di controllo, l'ormai famoso Garante per la protezione dati personali, e il titolare, in modo da facilitare le attività ispettive da parte dell'autorità Garante, oppure rispondere a specifici quesiti.

Infine, egli può essere certamente coinvolto nello sviluppo di attività di audit, che possono o convalidare il corretto trattamento dei dati da parte del titolare, o mettere in evidenza lacune, cui si può porre tempestivamente rimedio.

Tracciando un parallelo con

altri profili professionali coinvolti nel controllo delle attività di un'azienda, può venire in mente un revisore dei conti, che per sua natura, pur essendo sotto contratto con l'azienda mandante, ha tuttavia responsabilità autonome e può e deve essere in grado di riferire al vertice aziendale, ad esempio all'assemblea degli azionisti, eventuali situazioni che egli ritenga bisognose di essere messe sotto controllo.

È un ruolo delicato, in cui grandi competenze tecniche devono abbinarsi ad un profilo psicologico appropriato, che per molti aspetti ricordano il profilo del professionista della security, contemplato nella norma UNI 10491:2015.

Si fa presente anche che questa figura, pur sconosciuta in Italia, era invece già presente da anni a livello di istituzioni europee, ognuna delle quali doveva obbligatoriamente dotarsi di un responsabile della protezione dei dati, proprio per garantire a tutte le nazioni europee che il trattamento dei dati, acquisiti e gestiti a Bruxelles o a Strasburgo, avvenisse nel pieno rispetto delle disposizioni di legge.

L'ADDETTO AL TRATTAMENTO, OSSIA L'INCARICATO

Dal momento che non può esistere un esercito fatto solo di generali ed alti ufficiali, è evidente che nella operatività quotidiana il titolare ed il responsabile hanno bisogno di avvalersi del supporto di personale operativo, che in precedenza era

stato chiamato nel decreto legislativo già menzionato, "incaricato del trattamento".

Nel regolamento europeo questo soggetto non appare più con una specifica indicazione, ma tutti coloro che operano sotto l'autorità del titolare del trattamento del responsabile del trattamento possono essere chiamati più genericamente "addetti al trattamento".

Alcuni specialisti del settore, facendo riferimento all'articolo 29 del regolamento che tratta appunto questo argomento, preferirebbero usare l'espressione "addetto al trattamento ex articolo 29", ma mi sembra che questa denominazione sia un poco troppo impegnativa.

D'altro canto nulla ci impedisce di continuare ad utilizzare l'espressione "incaricato del trattamento", dal momento che ormai tutti sanno esattamente quale sia il ruolo attribuito a queste persone.

Le condizioni perché un addetto al trattamento sia tale, rispecchiano da vicino le condizioni già vigenti in Italia. In particolare:

- l'incaricato del trattamento deve aver ricevuto specifiche e puntuali istruzioni su ciò che può e non può fare in fase di trattamento dei dati personali su cui opera;
- è bene che tali specifiche e puntuali istruzioni siano illustrate per iscritto, per evitare qualsiasi possibile malinteso;
- l'incaricato del trattamento deve sottoscrivere uno specifico impegno alla riservatezza sui dati che tratta.

Infine, anche se il regolamento non lo prescrive formalmente, appare evidente che la partecipazione a un processo specifico di formazione, con illustrazione dettagliata dei compiti affidati

e delle modalità con le quali possono essere rispettati gli adempimenti del trattamento, è altamente raccomandata.

A tale proposito, a sostegno di questa impostazione, l'incaricato del trattamento deve ricevere puntuali istruzioni su tutta una nuova serie di rischi del trattamento, afferenti a contesti operativi, che ai tempi del decreto legislativo italiano non esistevano o erano presenti in misura ridotta.

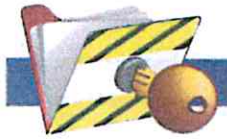
Ecco perché l'incaricato del trattamento deve ricevere precise istruzioni sulle modalità di gestione di *smartphone* e tablet, grazie ai quali egli può collegarsi al sistema informativo aziendale e trattare dati personali.

Parimenti, occorre dare istruzioni differenziate, in funzione del fatto che questi terminali informatici portatili siano di proprietà dell'incaricato, oppure siano affidati in comodato d'uso dal titolare. Infine, la diffusione quasi incontrollata dei supporti di memoria, le ormai famigerate **chiavette USB**, rende ormai necessario inserire nel percorso formativo anche dettagliate istruzioni su come garantire che i dati presenti su questi supporti di memoria siano adeguatamente protetti.

IL CONTITOLARE DEL TRATTAMENTO

Quando in Italia venne approvato il decreto legislativo 196/2003, il contitolare del trattamento non esisteva. Ci si rese successivamente conto che, in determinate attività di trattamento, non poteva essere designato un solo titolare, ma era indispensabile condividere la responsabilità del trattamento anche con altri titolari: così nacque anche in Italia il contitolare del trattamento, che però non ebbe mai una accurata definizione.

Il regolamento invece dedica l'intero articolo 26 a questi



soggetti, chiarendo che sono contitolari del trattamento i soggetti che determinano congiuntamente le finalità e i mezzi del trattamento. Essi devono stabilire fra loro un accordo interno, distribuendo le rispettive responsabilità.

Un aspetto essenziale è che tale accordo deve permettere agli interessati, che vogliono ad esempio esercitare il proprio diritto di accesso ai dati, di individuare un singolo punto di contatto per gli interessati stessi.

Resta inteso che la responsabilità di questi due soggetti è solidale e quindi, in caso di contenzioso, l'interessato può indirizzare le sue lagnanze o rivendicazioni ad uno qualsiasi dei due o più contitolari.

IL RAPPRESENTANTE DI TITOLARI O RESPONSABILI DEL TRATTAMENTO, NON STABILITI NELL'UNIONE EUROPEA

La facilità con cui i dati personali circolano in tutto il mondo, specialmente quando essi vengono inseriti nei *social network*, ha destato grande preoccupazione nei soggetti che sono stati coinvolti nell'elaborazione del regolamento europeo.

Sappiamo tutti che una straordinaria quantità di dati di cittadini europei è conservata negli Stati Uniti, perché là ha sede l'organizzazione che gestisce uno dei maggiori *social network* del mondo. Il trasferimento di questi dati all'esterno dell'Unione europea è stato più volte motivo di preoccupazione. Ecco la ragione per la quale il regolamento si è preoccupato di obbli-

gare titolari e responsabili del trattamento, non stabiliti nell'Unione europea, a designare loro rappresentanti, che potranno essere chiamati in causa a fronte di una qualsiasi violazione o richiesta di chiarimenti, afferenti al trattamento di dati personali.

Il rappresentante deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati coinvolti, e viene designato ove i dati personali vengano trattati nell'ambito dell'offerta di beni o servizi, o di monitoraggio del comportamento degli interessati.

Questo rappresentante è interlocutore unico per tutte le questioni riguardanti il trattamento con tutte le responsabilità connesse, anche in relazione all'avvio di azioni legali. In questo caso gli interessati potranno avviare l'azione legale verso il rappresentante, invece che il titolare e responsabile, residenti in un lontano Paese e quindi più difficilmente perseguibili.

Si ritornerà su questo tema nel capitolo dedicato al trasferimento in paesi terzi di dati personali.

L'AUTORITÀ DI CONTROLLO INDIPENDENTE

Con questa denominazione il regolamento europeo fa riferimento ad un soggetto ormai ben noto a tutti coloro che si occupano di dati personali in Italia: l'autorità Garante per la protezione dei dati personali, istituita un paio di mesi dopo l'entrata in vigore della legge 675/96.

Le caratteristiche dei componenti di questa autorità di controllo indipendente sono rimaste praticamente inalterate,

perché ancora una volta il regolamento fa riferimento all'indipendenza che deve essere garantita ai componenti dell'autorità, nonché alle condizioni generali, in base alle quali sono designati i componenti dell'autorità di controllo. In particolare, si richiede che ogni componente, per poter essere designato, debba avere una specifica competenza ed esperienza nel settore della protezione dei dati, per garantire un costruttivo contributo all'attività dell'autorità, nell'esercizio di funzioni e poteri.

Anche in questo caso, sono previste norme garantistiche che impediscono che un componente venga rimosso, salvo casi di colpa grave o in sopravvenuta assenza delle condizioni richieste per l'esercizio delle sue funzioni.

La differenza fondamentale, presente nel regolamento europeo, è legata al fatto che una nazione può designare diverse autorità di controllo indipendenti attribuendo loro incarichi specifici: ad esempio, un'autorità di controllo può operare nei confronti di una specifica attività di trattamento, mentre un'altra autorità può operare su altri fronti. In Italia, al momento, questa opportunità non è ancora stata sfruttata, ma, ove lo fosse, il regolamento si preoccupa di far presente che una sola autorità potrà rappresentare la nazione nel comitato per la

protezione dei dati personali, che viene di seguito illustrato.

Si vedrà, in seguito, che non tutte le autorità di controllo sono uguali, ma in alcune circostanze viene designata una autorità di controllo capofila.

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Questo Comitato è un organismo dell'unione europea ed è dotato di personalità giuridica. Per i lettori che già hanno avuto notizia dell'esistenza di un supervisore europeo per la protezione dei dati, al cui vertice si trova oggi l'italiano Giovanni Buttarelli, si fa presente che questo supervisore europeo opera solo nei confronti delle istituzioni europee, mentre il Comitato europeo opera nei confronti di tutte le nazioni europee.

Il Comitato europeo è composto da figure di vertice delle autorità di controllo per ciascuno Stato membro, nonché dal Garante europeo della protezione dei dati, il già menzionato Giovanni Buttarelli, ed infine da un rappresentante della Commissione europea, che però non ha diritto al voto.

Anche in questo caso, per essere componenti di questo Comitato, occorre dare appropriate garanzie di indipendenza, sottolineando il fatto che nell'esecuzione

dei suoi compiti o nell'esercizio dei suoi poteri il Comitato non sollecita né accetta istruzioni da alcuno.

L'istituzione di questo Comitato è fondamentale, perché esso deve tenere sotto controllo possibili derive istituzionali che si creino in singole nazioni europee, portando gradualmente a diversificazioni di trattamento che potrebbero portare alla situazione nella quale ci si è trovati nel 2012, quando ogni nazione europea era una repubblica quasi autonoma, almeno in tema di trattamento di dati personali.

Questo è il motivo per cui il regolamento prevede che tutte le autorità Garanti nazionali, ove assumano decisioni che possono influenzare il trattamento dei dati in altri Paesi europei, comunichino tali decisioni al Comitato europeo, nell'ambito della procedura chiamata di *"cooperazione e coerenza"*.

L'obiettivo di questa procedura è proprio quello di impedire derive, accertandosi che ogni provvedimento sia armonizzato con provvedimenti emessi in altre nazioni.

Il responsabile del monitoraggio di queste attività di coordinamento è proprio il Comitato europeo per la protezione dei dati.

I compiti attribuiti a questo Comitato sono assai numerosi e sono elencati puntualmente nell'articolo 70 del regolamento.

Infine, si apprezza il fatto che, per risparmiare preziose risorse, la segreteria del Comitato europeo è affidata proprio al supervisore europeo, che già da anni opera con incisività e *"moral suasion"* nei confronti delle istituzioni europee.

Così come accade per l'autorità Garante italiana, il Comitato elegge un presidente e due vicepresidenti, scelti tra i suoi membri. Questi tre soggetti hanno un mandato di cinque anni, rinnovabile una volta sola.

I DIRITTI DEGLI INTERESSATI

Il regolamento europeo dà un ampio spazio ai diritti dell'interessato. L'esperienza passata ha dimostrato che, anche se le declaratorie della direttiva europea, recepita in Italia ed in altri Paesi, davano spazio ai diritti dell'interessato, nell'esperienza pratica questi diritti spesso venivano ignorati. È questo il motivo per cui un intero capo del regolamento europeo è dedicato ai diritti dell'interessato. Tra l'altro, questi diritti sono stati ampliati in maniera sensibile dopo che una recente sentenza della Corte di Giustizia europea ha riconosciuto il cosiddetto "diritto all'oblio", che fa riferimento non solo al diritto di veder cancellati i propri dati personali presso il titolare che li tratta, ma anche al diritto di veder cancellati i rinvii a questi dati, che potrebbero apparire sui motori di ricerca più diffusi. Altri diritti, sanciti dal nuovo regolamento, fanno riferimento alla messa sotto controllo di procedure automatizzate di valutazione dei profili di comportamento della personalità di interessati, che vengono sviluppati da motori di ricerca e *social network*.

Ancora una volta il pregio della adozione di un regolamento, eguale in tutti i paesi europei, facilita l'esercizio dei diritti dell'interessato, armonizzandoli nell'intera Europa.

L'INFORMATIVA

Uno degli aspetti più importanti del nuovo regolamento riguarda il fatto che l'informativa deve essere trasparente, comprensibile e completa. Bisogna attivarsi in ogni modo per

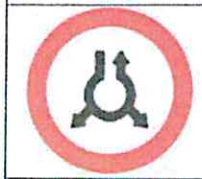
evitare le informative ambigue, lunghe cinque o sei pagine, che sembrano scritte apposta dagli uffici legali per renderle incomprensibili.

Un altro problema che si è manifestato in Europa è legato alle differenti lingue usate nei vari paesi, che rendono difficile ad un cittadino europeo, che ha piena libertà di movimento all'interno dell'Unione europea, di leggere e comprendere le informative che vengono offerte in lingue a lui non familiari.

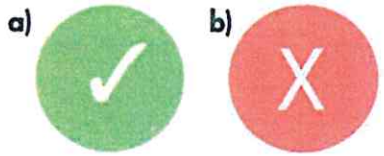
Il Presidente della commissione LIBE del parlamento europeo, Jan Philip Albrecht, ha dato un contributo determinante, in questa direzione, proponendo l'adozione di informative iconiche, vale a dire informative che usano immagini per convogliare un messaggio. Chissà quanti lettori di questo volumetto hanno avuto occasione di recarsi in un aeroporto, in un qualunque paese europeo, e comprendere immediatamente la differenza tra il percorso che porta alla zona partenze, perché essa è contraddistinta dal profilo di un aereo puntato verso l'alto, e il percorso che porta la zone arrivi, perché essa è contraddistinta dal profilo di un aereo che punta verso il basso, e quindi sta atterrando.

Lo stesso può valere per l'indicazione della zona recupero bagagli, la zona di attesa delle auto pubbliche, le aree destinate al prelievo oppure al cambio di valuta e via dicendo.

L'informativa iconica ha proprio il pregio che, una volta compreso il significato di un'immagine, esso non cambia quale che sia il Paese nel quale l'informativa viene presentata. La proposta della commissione LIBE del parlamento europeo è la seguente:

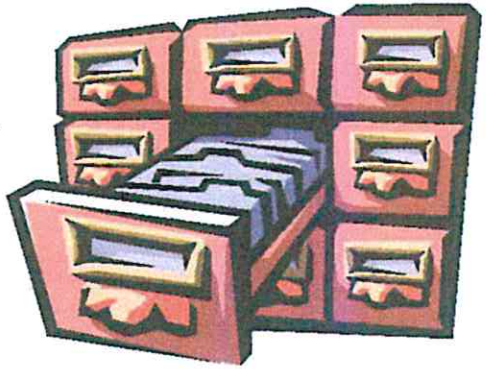
	la **raccolta** dei dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	La **memorizzazione** di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	Il **trattamento** di dati personali è limitato alle finalità per le quali sono stati raccolti	
	Non sono **forniti** dati personali a terze parti commerciali	
	Non sono effettuati **la vendita o l'affitto** di dati personali	
	I dati personali sono memorizzati in forma **cifrata**	

In corrispondenza di ognuna delle caselle precedenti deve essere inserito un contrassegno, a scelta tra i due che seguono, il cui significato è evidente:



Purtroppo la proposta del Presidente della Commissione LIBE non è stata approvata, ma è stato comunque approvato il principio che è facoltà della Commissione europea stabilire delle forme unificate e facilmente intelligibili di offerta di informativa. Si raggiunge così l'obiettivo di consentire anche a persone prive di specifica esperienza, e che potrebbero aver difficoltà nell'interpretare complesse informative, di intuire rapidamente le finalità per cui i loro dati vengono raccolti.

Restiamo in attesa di vedere quali modelli verranno proposti dalla Commissione europea, ma non v'è dubbio che questo approccio eviterà la comparsa di informative in varie lingue, come già oggi appare su alcuni cartelli informativi circa l'esistenza di impianti di videosorveglianza, posti da amministrazioni comunali.



Un altro aspetto, per il quale il nuovo regolamento si differenzia in modo significativo dalla precedente legislazione, riguarda l'obbligo di inserire nell'informativa il periodo di conservazione del dato. È questo un fattore spesso ignorato nelle attuali informative, che invece costituisce la premessa per l'esercizio dell'innovativo "diritto all'oblio".

Infine, resta valida la prescrizione che un trattamento viene considerato lecito, se necessario nell'ambito di un contratto o ai fini della conclusione di un contratto: in questo caso la firma del contratto costituisce già un consenso implicito da parte dell'interessato.

Tuttavia spesso i dati non vengono raccolti direttamente presso l'interessato, ma vengono raccolti presso un altro titolare. In questo caso il regolamento si preoccupa che l'interessato sia debitamente informato di questo fatto, in modo che egli abbia la possibilità di tenere sotto controllo una eventuale incontrollata proliferazione e distribuzione dei suoi dati.

Resta sempre valido il principio che, ove il titolare intenda trattare i dati già acquisiti per finalità diverse, rispetto quelle illustrate nell'informativa, ha comunque l'obbligo di acquisire un nuovo consenso. Tale consenso non è necessario se questi nuovi trattamenti vengono eseguiti in obbedienza ad un obbligo di legge. Parimenti, nulla impedisce al titolare di comunicare i dati personali acquisiti presso l'interessato ad un altro titolare, se, anche in questo caso, ci si trova davanti ad un obbligo di legge.

Ancora una volta, occorre trovare un ragionevole equilibrio tra completezza della informazione e lunghezza eccessiva della stessa, che in pratica porta ad una disinformazione per "stanchezza di lettura".

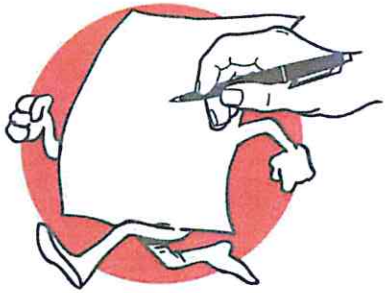
IL DIRITTO DI ACCESSO DELL'INTERESSATO

Questo diritto, che esisteva già nella precedente legislazione, viene ribadito e confermato nel nuovo regolamento. In particolare, l'interessato ha diritto di ricevere almeno una copia dei dati personali oggetto di trattamento, mentre potrebbe essere richiesto un modesto contributo spese, se sono richieste copie aggiuntive.

Deve essere cura del titolare predisporre una varietà di canali per l'esercizio del diritto di accesso, sia di tipo cartaceo, sia di tipo telefonico, sia di tipo elettronico.

Il titolare deve rispondere alla richiesta senza ingiustificato ritardo e al più tardi entro un mese dalla richiesta. Questa situazione è alquanto peggiorata, perché in Italia i tempi indicati dall'autorità Garante sono oggi molto più ristretti.

Nel caso il titolare ritenga di non dover esaudire una richiesta di accesso, deve comunque motivare la sua intenzione di non accoglierla.



IL DIRITTO DI RETTIFICA

Una naturale conseguenza del diritto di accesso è legata al diritto di rettifica, qualora l'interessato, esaminando i dati personali che sono stati acquisiti dal titolare, riscontri degli errori o delle anomalie.

In questo caso il titolare deve provvedere immediatamente alla rettifica o all'integrazione dei dati in suo possesso.

UN NUOVO IMPORTANTE DIRITTO: IL DIRITTO ALLA CANCELLAZIONE

Questo diritto, che correntemente viene chiamato "diritto all'oblio" pone rimedio ad un problema che negli anni si è dimostrato assai più grave di quanto non si percepisse inizialmente: l'interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei suoi dati personali per tutta una serie di ragioni, tra i quali certamente la più importante è la revoca del consenso o l'esaurimento delle finalità, per i quali

i dati vennero inizialmente raccolti.

L'evoluzione della società civile si rispecchia in questo articolo, laddove il regolamento specificamente prevede che l'interessato possa chiedere la cancellazione di dati raccolti relativamente all'offerta di servizi della società dell'informazione, vale a dire tramite servizi web di acquisto di beni e servizi, o servizi similari, ad esempio prenotazione di alberghi, che spesso acquisiscono informazioni personali senza dare un'informazione trasparente e li utilizzano poi in modo inappropriato.

È opportuno segnalare che il diritto all'oblio può essere attuato dal titolare sia cancellando direttamente i dati in suo possesso, sia, nel caso dei motori di ricerca, cancellando il link che collega l'interessato all'informazione, custodita presso altri titolari.

È questa la conseguenza di una ormai celebre sentenza della Corte di giustizia europea, che ha obbligato il motore di ricerca Google ad effettuare questa operazione, in riferimento ai link, presenti su motori di ricerca, che collegavano un interessato a procedimenti penali, assai lontani nel tempo e non più di attualità.

IL DIRITTO DI LIMITAZIONE AL TRATTAMENTO

È questo un altro nuovo diritto, certamente sacrosanto, dell'interessato, che può impedire al titolare di continuare a trattare dati personali, a lui riferibili, se l'interessato contesta l'esattezza dei dati, per tutto il periodo necessario per la correzione o aggiornamento dei dati stessi.

Lo stesso accade se l'interessato dichiara che il trattamento è

illecito, in quanto esula dal consenso a suo tempo prestato. La richiesta di limitazione al trattamento, o di notifica in caso di rettifica o richiesta di cancellazione, deve essere per legge comunicata, a cura e spese del titolare, a tutti gli altri destinatari cui egli ha trasmesso i dati personali. L'unica eccezione a questa disposizione riguarda il fatto che tale comunicazione si riveli assai difficile o implichi uno sforzo sproporzionato. Compete comunque al titolare impegnarsi per quanto possibile per soddisfare la richiesta avanzata dall'interessato.

PARLIAMO ORA DEL DIRITTO ALLA PORTABILITÀ DEI DATI

Il lettore si sta certamente rendendo conto del fatto che il nuovo regolamento ha accresciuto in maniera significativa i diritti dell'interessato, ponendo vari obblighi in carico al titolare. L'esperienza passata, infatti, ha messo in evidenza la necessità di aumentare la pressione sui titolari e aumentare i diritti degli interessati. Il diritto alla portabilità è una diretta conseguenza del diritto di accesso.

Se un interessato ha ricevuto, in conseguenza dell'esercizio del diritto di accesso, una copia dei suoi dati personali, magari in formato elettronico, è suo pieno diritto comunicare questi dati ad un nuovo titolare del trattamento, senza che il precedente titolare possa avanzare alcuna obiezione.

Anzi, il regolamento va ancora più in là, perché conferisce all'interessato il diritto di "ordinare" al titolare del trattamento di trasmettere direttamente i dati, se in formato elettronico, ad un nuovo titolare, che l'interessato avrà cura di indicare.

UN GRANDE PROBLEMA: LA PROFILAZIONE

Gli estensori del nuovo regolamento si sono resi conto che oggi la disponibilità di una grandissima quantità di dati, i famosi *big data*, riferiti ad un singolo interessato, permettono ad un titolare di costruire un profilo dell'interessato che certe volte raggiunge dei livelli di accuratezza, per non dire invasività, veramente sorprendenti.

Il fatto che molto spesso questi dati vengano comunicati inconsciamente dall'interessato al titolare, perché l'interessato non ha disabilitato alcune funzioni del suo *smartphone* o per altra ragione, non limita in alcun modo il diritto dell'interessato a vedere trattati in modo corretto i dati che lo riguardano, indipendentemente dalla quantità dei dati stessi e dal modo in cui sono stati acquisiti.

Per questa ragione il regolamento pone dei limiti ben precisi alle attività automatizzate, che permettono di costruire profili di un interessato, estraendoli da una grande massa di dati.

Una tipica applicazione è quella che permette di sviluppare attività di marketing mirato, semplicemente analizzando il profilo di navigazione di un interessato sul web, analizzando i siti contattati, analizzando i quesiti posti ai motori di ricerca e via dicendo.

Finché la profilazione permette a un titolare di proporre pernottamenti in alberghi, che si trovano in zone esaminate via web da un interessato, la cosa può essere fastidiosa, ma non grave.

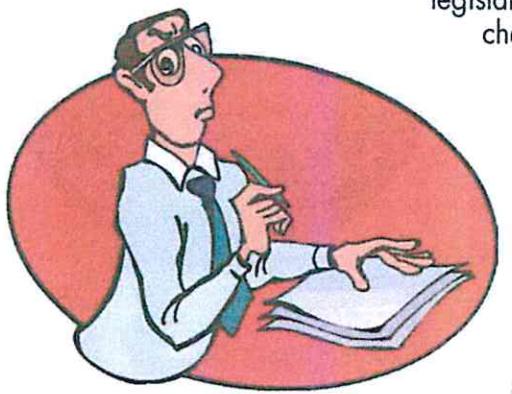
Diventa invece decisamente grave quando le decisioni assunte, nei confronti dell'interessato, sono basate esclusiva-

mente sull'analisi automatizzata del suo profilo. Ad esempio, in alcune istituzioni finanziarie che svolgono attività di prestito personale, per gestire con rapidità le richieste dei potenziali clienti, spesso si utilizzano degli applicativi, che ricercano sul web il massimo numero possibile di informazioni, afferenti al richiedente, e sulla base di queste informazioni propongono all'addetto al prestito varie ipotesi di concessione o perfino propongono di rifiutare il prestito.

Queste tipologie di trattamento di dati personali sono espressamente escluse dal nuovo regolamento, salvo esplicito consenso da parte dell'interessato.

LIMITAZIONE ALL'ESERCIZIO DEI DIRITTI SOPRA ILLUSTRATI

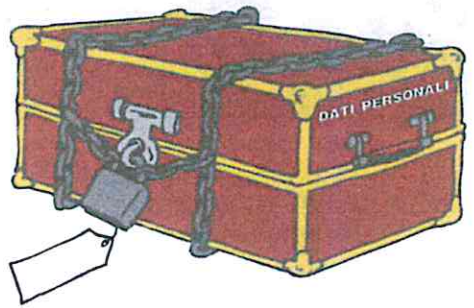
Come già previsto in precedenti disposizioni legislative, si ricorda ancora una volta che l'esercizio di tutti questi diritti non deve ledere i diritti e le libertà altrui.



Parimenti, esigenze di protezione della società civile, della sicurezza nazionale, della difesa e di indagini per l'accertamento dei reati, rappresentano condizioni esimenti nell'applicazione diritti sopra illustrati, che il regolamento esplicitamente prevede.

LA SICUREZZA DEL TRATTAMENTO E GLI STRUMENTI CHE PERMETTONO DI GARANTIRLA

Una significativa differenza fra il decreto legislativo 196/2003, in vigore in Italia, ed il nuovo regolamento europeo sta nel fatto che il decreto legislativo, grazie all'allegato B, dà alcune indicazioni sulle modalità con cui era possibile garantire la sicurezza dei dati personali trattati dal titolare.



Il nuovo regolamento ha ampliato in misura significativa questi aspetti, indicando addirittura tutta una serie di misure, alcune assai complesse, che permettono di garantire un'elevata sicurezza del trattamento di dati. Oltre a misure di carattere sistematico, il regolamento offre anche una serie di interventi di valutazione, che sono indubbiamente assai avanzati e possono, grazie a misure di prevenzione, migliorare in modo significativo il livello di sicurezza del trattamento.

In questa opera è indubbiamente prezioso il supporto del responsabile della protezione dei dati, che è il soggetto con specifiche competenze che deve mettere a disposizione del titolare e del responsabile del trattamento.

L'articolo 32 - Sicurezza del trattamento, elenca puntualmente le aree di intervento, che vengono di seguito esaminate.

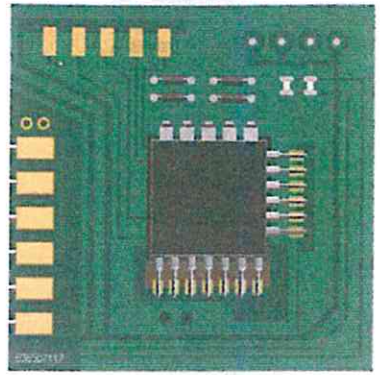
LA PSEUDONIMIZZAZIONE E LA CIFRATURA DEI DATI PERSONALI

Purtroppo i traduttori in lingua italiana del regolamento non sono riusciti a trovare una parola più felice dell'espressione originale inglese. Forse l'espressione pseudo-anonimato poteva essere più comprensibile. A questo punto, occorre accettare questa orrenda parola e cercare di capire cosa essa significhi.

Con questa parola si fa riferimento al trattamento di dati personali, in modo tale che essi non possano più essere attribuiti ad un interessato specifico, senza l'utilizzo di informazioni aggiuntive. Resta inteso che tali informazioni aggiuntive devono essere conservate separatamente e soggette a misure tecniche e organizzative, che ne garantiscano la protezione. Un esempio potrà meglio chiarire questa forma di protezione dei dati.

Supponiamo che un'agenzia di ricerche di mercato sia incaricata di intervistare un certo numero di visitatori di un centro commerciale, per raccogliere le loro valutazioni su un determinato prodotto. Per varie ragioni, la scheda che viene compilata dall'intervistatore comprende anche dati personali degli intervistati (ad esempio per inviare un omaggio). Se si decide di attribuire un codice alfanumerico ad ogni scheda, e successivamente, in fase di trattamento, si fa riferimento a tale codice, i dati personali del soggetto intervistato non sono più riconducibili all'interessato stesso, a meno che non si abbia a disposizione una tabella di corrispondenza tra il codice alfanumerico attribuito ad una scheda e la scheda stessa.

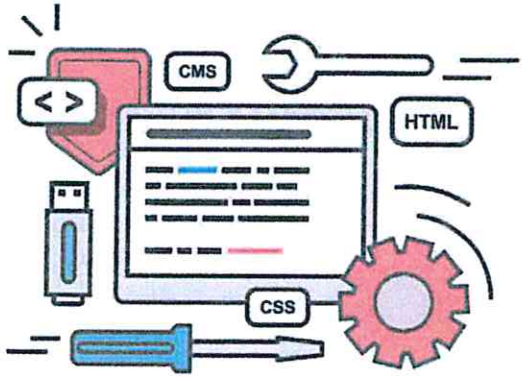
Oggi queste tecniche cominciano ad essere sempre più diffuse e costituiscono indubbiamente una forma relativamente semplice ed efficace di protezione dei dati personali di un interessato.



La seconda categoria di misure di protezione, vale a dire la cifratura dei dati, costituisce una forma più raffinata di mascheramento del dato, in quanto viene resa inaccessibile l'intera scheda, per tornare all'esempio precedente, e non soltanto il collegamento fra un codice e la scheda.

Oggi le tecniche di criptografia dei dati hanno fatto grandi passi avanti, soprattutto perché i fabbricanti di chip per computer mettono a disposizione dei circuiti specialmente progettati per gestire, con grande velocità e affidabilità, le operazioni di calcolo legate alla cifratura e decifratura dei dati.

I lettori avranno certamente avuto occasione di vedere già in commercio delle chiavette di memoria USB, che possono permettere di cifrare i dati archiviati sulla chiavetta stessa. A questo fatto si aggiunge anche la crescente disponibilità di algoritmi criptografici dotati di grande resistenza a tentativi di violazione, pur richiedendo una potenza di calcolo relativamente modesta.



Il parere concorde di tutti gli specialisti di protezione dei dati personali è che una applicazione su larga scala delle tecniche criptografiche rappresenti un'efficacissima misura di protezione del dato, a condizione ovviamente che le chiavi di codifica e decodifica siano custodite con la massima diligenza.

LE GARANZIE DI RISERVATEZZA, INTEGRITÀ, DISPONIBILITÀ E RESILIENZA DEI SISTEMI DI TRATTAMENTO

Nei paesi anglosassoni già da tempo era utilizzato l'acronimo CIA-*confidentiality, integrity, availability*, che corrisponde esattamente alle prime tre voci del titolo di questo paragrafo. Il regolamento ha ritenuto opportuno inserire anche un ulteriore parametro, la resilienza, che caratterizza la capacità di un sistema informativo di fronteggiare possibili anomalie, non solo limitando le conseguenze legate al loro verificarsi nei confronti dei dati custoditi nel sistema informativo stesso, ma anche ripristinando rapidamente le condizioni di funzionamento originali. Nell'acronimo anglosassone sopra riportato, infatti, non vengono prese in considerazione le capacità di adattamento e di flessibilità del sistema informativo, laddove le caratteristiche di resilienza contrassegnano proprio questa modalità reattiva del sistema.

LA CAPACITÀ DI RIPRISTINARE TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO AI DATI PERSONALI, IN CASO DI INCIDENTE FISICO O TECNICO

Appare evidente che questo requisito, posto dal regolamento, è direttamente connesso ai requisiti precedenti.

È opportuno ricordare che la nostra autorità Garante già aveva dato indicazioni in merito al fatto che non doveva essere ritardato oltremodo l'accesso ai dati, ad esempio a fronte di una richiesta di un interessato, ove il titolare si trovasse a fronteggiare un'avaria funzionale, oppure la temporanea indisponibilità del sistema di trattamento.

La precisazione, che fa riferimento a ipotesi di incidente fisico o tecnico, è legata evidentemente al fatto che il sistema informativo potrebbe non essere disponibile per un allagamento, un crollo, un sisma, un incendio, vale a dire per cause naturali, mentre la indisponibilità tecnica potrebbe essere dovuta a cause funzionali o di origine antropica, cioè criminosa o frutto di negligenza.

LA VERIFICA SISTEMATICA E PREVENTIVA DELL'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE ADOTTATE A FRONTE DEI RISCHI PRECEDENTI

Anche questa è un'attività che nel nostro decreto legislativo 196/2003 non è presa in esplicita considerazione.

Il fatto di svolgere sistematicamente delle attività di audit, che permettono di analizzare le caratteristiche di affidabilità e di puntuale attuazione delle misure tecniche e organizzative, legate alla continuità ed integrità del trattamento, rappresenta un aspetto assolutamente determinante.

Sotto questo aspetto, ancora una volta si mette in evidenza l'importanza del ruolo affidato al nuovo personaggio introdotto dal regolamento, vale a dire il responsabile della protezione dei dati, perché egli ha le competenze ed anche i poteri per svolgere questa attività, con un ruolo debitamente protetto da possibili interferenze dei soggetti controllati.

I REGISTRI DELL'ATTIVITÀ DI TRATTAMENTO

Dopo aver esaurito l'elenco delle misure suggerite nell'articolo 32, è il caso di passare ad esaminare l'articolo 30, che è strettamente connesso alla documentazione delle misure adottate in fase di trattamento.

In particolare, l'articolo impone che ogni titolare del trattamento mantenga un registro delle attività svolte sotto la sua responsabilità.

Il registro deve contenere tutt'una serie di informazioni, legate non solo al nome e ai dati di contatto del titolare ed altri soggetti coinvolti, ma anche alle finalità del trattamento, con una descrizione delle categorie di interessati coinvolti e delle categorie di dati personali trattati, nonché una descrizione generale delle misure di sicurezza tecnica e organizzative, illustrate appunto all'articolo 32.

Questi registri devono essere messi a disposizione dell'autorità Garante, a richiesta, per effettuare ispezioni o acquisire elementi di valutazione, in caso di violazione delle disposizioni del regolamento.

Il regolamento viene poi incontro alle esigenze delle piccole e medie imprese, esentandole dall'obbligo di tenere questo registro, ove esse abbiano meno di 250 dipendenti.

L'esenzione però non è concessa se la azienda, per quanto piccola, tratta particolari categorie di dati che esamineremo in seguito.

E SE QUALCOSA VA STORTO E I DATI VENGONO VIOLATI?

A fronte di questo evento, il regolamento impone prescrizioni assai più restrittive, rispetto alle prescrizioni in vigore in precedenza. L'autorità Garante italiana, recependo una direttiva europea, aveva già imposto ai titolari, coinvolti nella resa di servizi di telecomunicazione o trattamenti biometrici, di comunicare qualsiasi violazione di tali dati. Oggi questo obbligo si è allargato in misura significativa e, in pratica, qualsiasi violazione dei dati personali dell'interessato deve essere notificata all'autorità Garante. Il tempo massimo entro il quale la notifica deve essere inviata è di 72 ore, salvo casi che bisogna documentare con ampio dettaglio.

La notifica deve contenere tutt'una serie di dettagliate informazioni sulle modalità con cui la violazione si è verificata, sia di natura accidentale, sia di natura dolosa, nonché la tipologia dei dati e le categorie degli interessati coinvolti.

Ma non è finita!

Mentre l'obbligo di comunicazione all'autorità Garante vige sempre, ci si potrebbe domandare se e quando tale violazione debba essere anche comunicata agli interessati coinvolti. A questo tema critico è dedicato l'articolo 34.

Esso prescrive che la comunicazione all'interessato, circa l'avvenuta violazione dei suoi dati, descriva con un linguaggio semplice e chiaro la natura della violazione dei dati e offra anche delle raccomandazioni sui modelli di comportamento da adottare per limitare le conseguenze della violazione, nell'attesa che il titolare attivi adeguate misure di protezione.

Tuttavia, a differenza di quanto previsto nell'articolo 33 che prevede l'obbligo di comunicazione all'autorità Garante, non è richiesta la comunicazione all'interessato se sono soddisfatte alcune condizioni d'altronde intuitive.

Ad esempio, la violazione di dati protetti da algoritmo crittografico è certamente meno grave, rispetto alla violazione di dati in chiaro. Chi ha sottratto questi dati infatti non avrebbe comunque modo di accedere ai dati stessi.

L'articolo 34 prevede anche altre condizioni esimenti, ma lascia comunque sempre all'autorità Garante la decisione finale circa l'avvio della procedura di comunicazione, scavalcando eventuali decisioni contrarie del titolare.

LA PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

Poiché nessuno può dubitare del fatto che prevenire sia meglio che contrastare, il regolamento impone al titolare del trattamento di valutare attentamente, prima dell'avvio di un qualsiasi trattamento, quali potrebbero essere i rischi ad esso connessi.

Tali rischi evidentemente sono oltremodo variabili e, anche se sono stati elencati in precedenza, possono avere una dimensione, in termini di gravità e frequenza, variabile. Per questa ragione il titolare deve impostare e sviluppare misure tecniche ed organizzative, applicabili al trattamento che intende svolgere, tali da recepire, fin dall'avvio stesso della progettazione, principi ormai riconosciuti e accettati di protezione dei dati.

L'elenco delle misure illustrate in precedenza può essere un esempio di quanto deve essere recepito sin dalla progettazione del trattamento.

LA PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

È questa una brillante traduzione, adottata dai traduttori europei, dell'espressione inglese *"data protection by default"*. Questa espressione fa riferimento al fatto che il titolare del trattamento deve accertarsi di trattare solo i dati personali necessari per raggiungere una specifica finalità del trattamento.

Quest'obbligo vale non solo in riferimento alla quantità dei dati personali raccolti, ma anche in relazione al periodo di conservazione.

Appare evidente che, dopo aver sviluppato un'indagine di mercato presso i clienti di un centro commerciale, tesa a rilevare il livello di gradimento di un determinato prodotto, non ha alcuna importanza custodire a lungo le schede del rilevamento, in quanto è sufficiente estrarre dati statistici che certamente saranno più che sufficienti per soddisfare le esigenze dell'azienda che ha commissionato la ricerca.

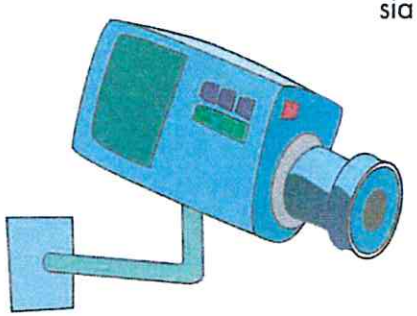
Questa misura e quella precedente sono del tutto nuove nel panorama di garanzie di sicurezza del trattamento, rispetto alle disposizioni precedenti.

LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Questa è la terza misura di sicurezza del trattamento che viene imposta dal regolamento.

Si tratta di una valutazione molto impegnativa, tant'è vero che il regolamento prevede debba essere sviluppata solo quando il trattamento impone l'uso di nuove tecnologie, applicabili a grandi quantità di dati, che potrebbero avere anche caratteristiche critiche.

Ancora una volta entra in gioco il già menzionato responsabile della protezione dei dati, se designato, la cui competenza e professionalità specifiche possono dare un contributo determinante a far sì che la valutazione di impatto sia tanto articolata, quanto accurata.



Tra i casi in cui la valutazione di impatto è obbligatoria si pone in particolare evidenza la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

I casi pratici che vengono subito in mente fanno riferimento, ad esempio, a impianti di videosorveglianza che controllano vaste aree.

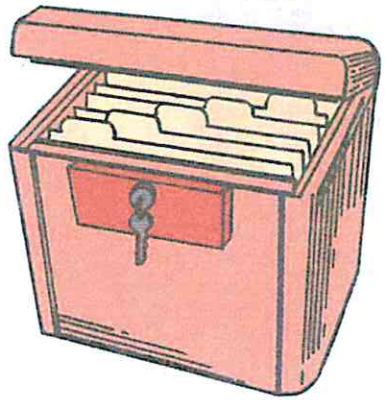
LA CONSULTAZIONE PREVENTIVA

A conclusione di questo capitolo, prendiamo in esame un'altra disposizione del regolamento, particolarmente apprezzabile.

Nel dubbio che il titolare del trattamento possa non valutare in modo appropriato l'opportunità di attivare, ad esempio, una valutazione di impatto, o comunque in ogni caso in cui il trattamento possa avere riflessi significativi sulla tutela dei dati personali, al titolare è fatto obbligo di rivolgersi all'autorità Garante per una consultazione preventiva.

A questo punto appare evidente che l'autorità Garante diventa una sorta di consulente del titolare e deve avere le competenze e le risorse necessarie per esaminare quanto già fatto dal titolare e mettere in evidenza possibili interventi migliorativi.

Stante il tempo necessario per portare a termine con sufficiente incisività tale analisi, il regolamento mette a disposizione otto settimane, dal ricevimento della richiesta di consultazione, per emettere un parere scritto. Ove la situazione sia particolarmente intricata, è possibile estendere ulteriormente il termine di sei settimane.

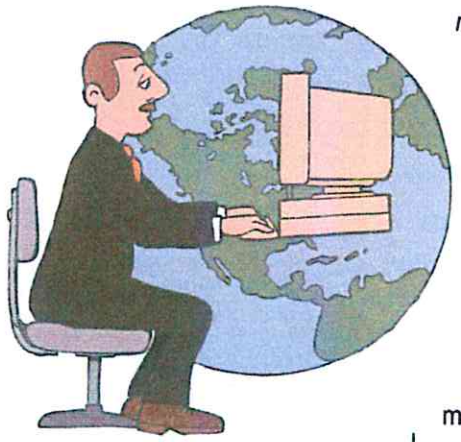


Resta ora da vedere se, nei vari paesi europei, le autorità nazionali avranno le competenze e le risorse necessarie, perché quest'opera di consultazione potrebbe rivelarsi assai più impegnativa di quanto non possa sembrare ad una prima lettura dell'articolo 36 del regolamento.

I TRATTAMENTI PARTICOLARI

A differenza di quanto prevede il decreto legislativo 196/2003, i dati personali, nel contesto del regolamento europeo, hanno un'unica definizione, invece delle due adottate in Italia. In Italia esistono dati personali, diciamo così "normali", e dati personali sensibili. Per contro, nell'articolo 4 del regolamento la definizione adottata per dato personale è la seguente:

"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;



Come si vede, la definizione include sia i dati personali normali, sia i dati sensibili.

La differenziazione tra le due categorie di dati viene fatta negli articoli che fanno riferimento alle modalità di trattamento di questi dati, che adesso andiamo ad esaminare.

QUANDO È POSSIBILE TRATTARE DATI PARTICOLARI

L'articolo 9 fa riferimento al trattamento di categorie particolari di dati personali. Al comma 1, esso afferma che:

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

A fronte di questo divieto generalizzato, vengono successivamente elencate numerose situazioni, nelle quali il trattamento di questi dati è consentito.

Una delle prime condizioni esimenti è evidentemente legato al fatto che l'interessato abbia prestato il proprio consenso esplicito, salvo alcuni casi, molto limitati, in cui all'interessato questo potere non è concesso. Per esempio possiamo mettere in evidenza i casi legati alla tutela della sicurezza e della salute pubblica, che fanno sì che, ad esempio, gli enti preposti alla tutela della salute pubblica possano intervenire quando l'interessato è affetto da una malattia contagiosa, che potrebbe trasmettersi a persone che si trovino nelle sue vicinanze, come può accadere ad uno scolaro che risulti infetto da una malattia fortemente contagiosa.

Un'esimente è legata evidentemente al fatto che il titolare del trattamento abbia l'obbligo di rispettare il diritto del lavoro, della sicurezza sociale e protezione sociale, nonché gli obblighi imposti da un contratto collettivo di lavoro, che coinvolga lo sfortunato interessato.

Vale anche qui il principio, già illustrato nel nostro decreto legislativo, che la tutela della salute dell'interessato abbia la precedenza sull'eventuale mancanza di un esplicito consenso

al trattamento di dati sanitari critici; è la tipica situazione che si verifica a fronte di un interessato colpito da un trauma per un incidente stradale, che venga ricoverato in ospedale e abbia bisogno di cure urgenti.

Particolarmente interessante è l'esenzione legata al fatto che il trattamento sia sviluppato da una fondazione, associazione o altro organismo senza scopo di lucro, che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con questi enti. Resta valido comunque il principio che i dati personali dell'interessato non devono essere comunicati all'esterno dell'associazione o fondazione, senza il consenso dell'interessato.

Parimenti, il divieto di trattamento non si applica a dati personali resi manifestamente pubblici dall'interessato.

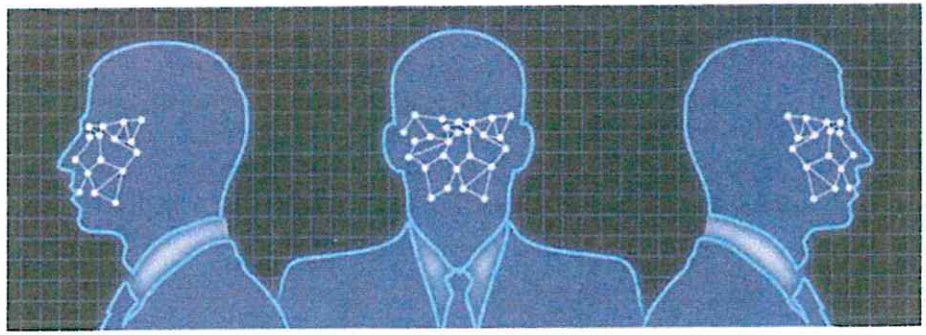
Se poi il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, oppure ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni specifiche, parimenti l'esenzione non si applica.

Di particolare interesse è il trattamento di dati particolari, conseguente all'attuazione dei principi di finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza a terapia sanitario-sociale, ovvero gestione dei servizi sanitari e sociali sulla base di leggi esistenti negli stati membri dell'Unione.

Non può non venire immediatamente a mente il decreto legislativo afferente alla sicurezza dell'ambiente di lavoro, laddove al medico competente vengono attribuiti particolari poteri di tutela del dipendente. In questi casi resta inteso che il medico competente è soggetto al segreto professionale.

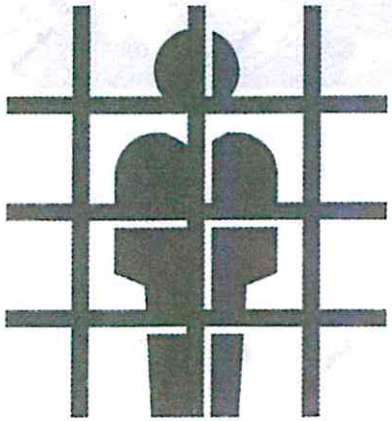
Poiché ormai si stanno diffondendo sempre più i dati biometrici, ad esempio per l'installazione di sistemi di riconoscimento dell'identità e controllo dell'accesso, il comma 4 dell'articolo 9 prevede che gli stati membri possano mantenere od introdurre ulteriori condizioni, ed anche limitazioni, riguardo il trattamento dei dati genetici, biometrici o relativi alla salute.

Ci troviamo nella condizione già operante in Italia, laddove l'autorità Garante per la protezione dei dati personali ha già pubblicato specifiche indicazioni, applicabili al trattamento di dati biometrici, soprattutto per applicazioni di controllo accessi, che oggi stanno incontrando un favore crescente per la loro affidabilità e semplicità di uso.



Questa disposizione dell'autorità Garante nazionale risulta quindi conforme ai dettati del regolamento.

CHE FARE PER IL TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI?



A questo argomento è dedicato l'articolo 10, che prende proprio in esame il trattamento di questi dati, nonché le eventuali misure di sicurezza applicate, ad esempio il divieto di allontanamento dal domicilio e altre imposizioni similari.

Il trattamento di questi dati è consentito, ma solamente ad autorità pubbliche, come ad esempio la magistratura inquirente e le forze di polizia. Ogni stato membro ha comunque il potere di emettere disposizioni specifiche, purché siano rispettate garanzie appropriate per i diritti e le libertà degli interessati.

Una speciale disposizione si applica alla compilazione e all'aggiornamento di un registro completo delle condanne penali, che può essere tenuto soltanto sotto il controllo dell'autorità pubblica, che pertanto deve operare come titolare del trattamento.

Come si vede, il divieto generale previsto dall'articolo 9, comma 1, prevede un certo numero di esenzioni, che per la verità non sono molto diverse da quelle già attualmente in vigore in molti paesi dell'unione europea ed in particolare in Italia.

I NUOVI RISCHI DEL TRATTAMENTO: CLOUD, CHIAVETTE USB, SMARTPHONE E BYOD, SOCIAL NETWORKS ED ALTRO

Il nuovo regolamento non prende in considerazione specificamente questi aspetti tecnologici, perché evidentemente affronta il problema in termini più generali.

Non vi è però alcun dubbio che un titolare e un responsabile del trattamento debbano dare appropriate istruzioni all'incaricato, perché egli possa sfruttare al meglio le nuove opportunità di archiviazione ed accesso ai dati, pur salvaguardando i fondamentali principi di sicurezza del trattamento, ben illustrati nel regolamento.

In questo capitolo viene quindi presentata una rassegna delle nuove opportunità tecnologiche disponibili per tutti i soggetti coinvolti, compresi gli incaricati, illustrandone gli aspetti positivi e negativi.

ARCHIVIARE I DATI NELLE NUVOLE

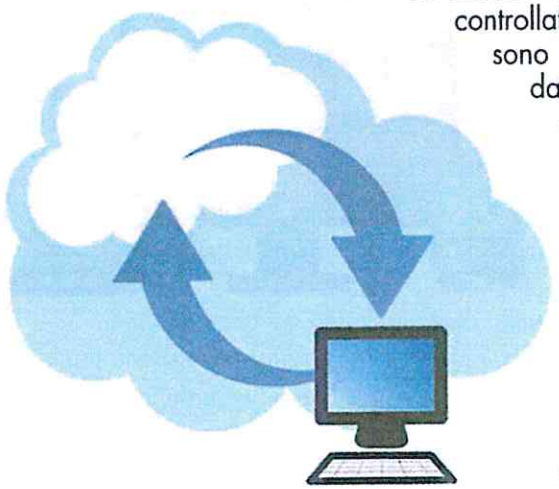
Oggi sono numerose le aziende che offrono servizi di archiviazione e trattamento dati in computer, che sono raggiungibili praticamente solo con una connessione Internet.

La comodità di avere a disposizione una grande capacità di memoria, nonché la possibilità di archiviare anche applicativi

in modo che sia possibile trattare dati anche se i computer installati in azienda presentano dei problemi, rappresentano indubbiamente dei fattori estremamente attraenti.

D'altro canto, basti pensare al fatto che l'archiviazione di dati nel *cloud*, per quanto sia comoda, perché accessibile da qualunque parte del mondo, potrebbe presentare problemi di cancellazione del dato, se il titolare del trattamento non ha ben chiaro il luogo fisico dove i dati sono custoditi.

Spesso nemmeno l'azienda che offre servizi di archiviazione *cloud* ha una chiara idea di dove si trovino fisicamente questi dati e potrebbe quindi diventare oltremodo difficile procedere alla cancellazione, o per esaurimento delle finalità per cui i dati vennero raccolti, o per soddisfare una precisa richiesta dell'interessato coinvolto.



La situazione è evidentemente molto più controllata e sicura, quando i dati sono custoditi sul *server* aziendale, perché l'operazione di cancellazione è rapida e dà risultati certi.

Questo è solo un esempio del fatto che l'utilizzo del *cloud*, come supporto ad attività primarie di trattamento sviluppate all'interno di un'azienda, sotto la diretta sorveglianza del titolare, del responsabile e perfino del responsabile della protezione dei dati, può presentare vantaggi, che è bene valorizzare al massimo, ma anche problemi, che è bene mettere sotto stretto controllo.

L'autorità Garante italiana ha pubblicato poco tempo fa un

prezioso volumetto di una trentina di pagine, nel quale vengono presi in considerazione gli aspetti positivi e negativi di questa modalità di trattamento e vengono offerte preziose indicazioni a tutti coloro che desiderano sfruttare al meglio il *cloud*.

Tanto per cominciare, i servizi che possono essere residenti nel *cloud* sono oltremodo variati e presentano livelli di rischio, anch'essi oltremodo variati.

Oggi si utilizzano correntemente degli acronimi, che fanno riferimento appunto al tipo di servizio richiesto.

Vi è il servizio di archiviazione dei dati, come funzione di backup (BaaS – Backup as a Service), vi è il servizio di archiviazione e trattamento di dati, che prevede quindi non solo il trasferimento di dati nel *cloud*, ma anche il trasferimento di software applicativi (PaaS – platform as a Service).

Un'altra interessante opportunità, che viene ormai utilizzata frequentemente da amministrazioni pubbliche, riguarda ad esempio l'archiviazione del *cloud* delle immagini videoregistrate, che provengono da impianti di videosorveglianza (VaaS – Videorecording as a service).

Quasi ogni giorno nascono nuovi servizi, che vanno attentamente valutati per mettere sempre a confronto vantaggi e rischi collegati.

È bene sottolineare che l'autorità Garante ha ritenuto opportuno pubblicare questo specifico manualetto, facilmente reperibile sul sito dell'autorità Garante, perché la direttiva europea, che è

stata recepita con il decreto legislativo 196 /2003, non prestava alcuna particolare attenzione ai servizi nel *cloud*, forse perché ai tempi in cui la direttiva venne emanata essi non erano ancora molto diffusi. Di conseguenza, anche il decreto legislativo italiano non presta una particolare attenzione a questi servizi, che vanno inquadrati in un'ottica più generale.

Ad esempio, un tema di particolare importanza, quando si inseriscono dati nel *cloud*, è l'individuazione accurata di chi sia il titolare o il responsabile per il trattamento sicuro e affidabile di questi dati.

Non dimentichiamo che quando l'interessato affida i suoi preziosi dati personali al titolare del trattamento, quest'ultima si impegna a custodirli con pari diligenza anche se, per ragioni operative, decide di trasferire o comunicare questi dati ad un soggetto terzo.

La situazione è simile a quella del datore di lavoro che acquisisce e tratta un certo numero di dati personali dei propri dipendenti. Questi dati personali spesso vengono trasferiti ad un consulente, che sviluppa paghe e contributi, per evidenti necessità di elaborazione. Il titolare del trattamento, cioè il datore di lavoro, deve prendere ogni precauzione perché i dati forniti dai suoi dipendenti vengano custoditi e controllati con estrema diligenza dal consulente esterno.

Ma non basta.

Ove il titolare decida di interrompere il rapporto di lavoro con il consulente esterno, deve imporre a quest'ultimo di restituire tutti i dati personali dei dipendenti, che sin da allora aveva trattato, senza farne alcuna copia.

Tutti questi problemi, che non sono trascurabili quando si opera in ambienti fisicamente circoscritti, diventano assai più sfumati e difficilmente controllabili, quando la controparte, presso la quale vengono trasferiti i dati personali, è un'azienda che offre i servizi del *cloud*.

Su indicazione dell'autorità Garante, questa azienda deve essere designata responsabile del trattamento e quindi il titolare deve impartirgli tutte le appropriate istruzioni, che tutelino la sicurezza dei dati. Appare evidente che la capacità di negoziazione di un titolare del trattamento è direttamente legata alla sua dimensione e alla sua importanza, come cliente dell'azienda che offre servizi *cloud*. Le piccole e medie aziende per solito hanno un potere contrattuale estremamente ridotto e quindi devono talvolta accettare le condizioni imposte dall'azienda, con ben poco spazio per esigere, non diciamo miglioramenti del livello di sicurezza, ma perfino per richiedere chiarimenti!

Basti pensare all'ipotesi di richiesta di cancellazione dei dati, trattata in precedenza, per rendersi conto che il potere di verifica del titolare, circa l'avvenuta cancellazione dei dati nei confronti del responsabile del *cloud*, è estremamente ridotto. Sarà poi da vedere se, in caso di violazioni delle prescrizioni del regolamento, sarà sufficiente una dichiarazione scritta, da parte del responsabile del *cloud*, per esonerare da ogni responsabilità il titolare, che quei dati aveva inizialmente acquisito e di cui aveva la responsabilità primaria.

Bastano questi aspetti per capire come l'argomento sia alquanto complesso e, purtroppo, diventi ancora più complesso quando l'azienda, che fornisce servizi *cloud*, si offre in qualità di "agente di commercio", piuttosto che essere il proprietario vero e proprio. In questo caso l'azienda potrebbe non aveva la più pallida idea di dove si trovino i *server* nei quali sono archiviati i dati immessi nel *cloud*.

Se questi *server* si trovano all'interno dell'Unione europea, il problema è sotto controllo, ma se questi *server* si trovano in qualche altro paese terzo, i problemi crescono in maniera esponenziale.

Ci si augura che una maggiore concorrenzialità tra le aziende che offrono servizi nel *cloud*, induca le aziende stesse ad offrire spontaneamente clausole contrattuali garantistiche ai propri clienti, senza attendere che essi chiedano specifiche garanzie, che potrebbe essere difficile ottenere.

Se poi il lettore ritiene che le righe che precedono abbiano esaurito l'argomento, è bene si tenga stretto alla sedia, perché l'argomento verrà ripreso ancora una volta, in relazione all'uso

di *smartphone* che, quasi sempre, (e quasi sempre all'insaputa del proprietario dell'apparecchio) archiviano dati nel *cloud*!

NELL'ERA MODERNA, UN NUOVO RISCHIO: LE CHIAVETTE DI MEMORIA USB

È del tutto probabile che un lettore di questo volume abbia nelle tasche, nella valigetta del PC o nelle immediate vicinanze una o più chiavette di memoria USB.

La compattezza e la versatilità di questi dispositivi di memoria portatile spesso fanno perdere di vista all'interessato la necessità di conservare questi supporti con la stessa attenzione con la quale probabilmente l'interessato già custodisce dati su supporto cartaceo. Ormai, nell'educazione e sensibilizzazione degli interessati, i supporti cartacei sono custoditi con un'attenzione ben maggiore, rispetto a quella prestata a questi dispositivi, ognuno dei quali può custodire migliaia di pagine di documenti.

L'esperienza ha dimostrato che anche gli interventi di sensibilizzazione, sviluppati dal titolare del trattamento, dal responsabile e dal responsabile della protezione dei dati personali, non sempre hanno successo, proprio perché le piccole dimensioni della chiavetta fanno ritenere che l'attenzione da porre alla sua diligente custodia sia altrettanto piccola.

A questo punto, il titolare del trattamento, con i suoi collaboratori previsti dal regolamento per la protezione dati personali, deve trovare soluzioni alternative che possano unire un elevato livello di sicurezza ad una attenta custodia.

L'esperienza ha dimostrato anche che le raccomandazioni scritte, che talvolta diventano anche disposizioni imperative, lasciano il tempo che trovano, perché vi è sempre una notevole differenza fra le istruzioni impartite e la percezione che l'incaricato ha circa le stesse.

Oggi sono fortunatamente disponibili delle soluzioni tecniche che permettono di garantire un soddisfacente livello di protezione dei dati personali, custoditi su questi supporti di memoria, grazie all'adozione di applicativi di criptografia, che intervengono in forma automatica, ogniqualvolta un dato viene trasferito dal PC aziendale, fisso o mobile, a questi supporti. Gli applicativi crittografici devono avere la caratteristica di una grande rapidità di funzionamento dell'algoritmo, per non rallentare in modo eccessivo il trasferimento di dati dal PC client alla chiavetta. Parimenti, l'algoritmo deve essere in grado di operare in modalità reversibile, recuperando rapidamente i dati archiviati su una chiavetta e rendendoli nuovamente leggibili sul PC aziendale.

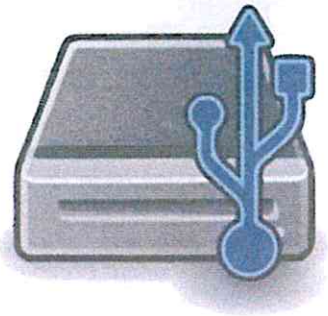
Oggi addirittura molte chiavette di memoria vengono vendute, con un lievissimo sovrapprezzo, con incorporato l'applicativo criptografico. A questo punto, la responsabilità che compete all'interessato è solo quella di custodire con diligenza la chiave criptografica, che permette di attivare, nei due sensi, l'algoritmo.

Un'altra soluzione, apparsa sul mercato qualche tempo fa, consiste nel realizzare una chiavetta un poco più complessa nell'architettura tecnologica, in quanto in essa è incorporato un lettore di impronta digitale. Perché la chiavetta possa essere

utilizzata, occorre che il proprietario, vale a dire l'incaricato del trattamento, appoggi un dito sul lettore. A questo punto la chiavetta, previa registrazione e riconoscimento dell'impronta digitale autorizzata, provvede ad abilitare le funzionalità di lettura e scrittura, proteggendo il contenuto anche in caso di smarrimento o furto della chiavetta.

Il costo di questi dispositivi è un poco più elevato, ma la sicurezza che garantiscono è decisamente superiore.

Infine, esiste una terza soluzione, alquanto radicale, che viene utilizzata in istituzioni bancarie ed altri contesti, in cui si ritiene che sia obbligatorio utilizzare misure radicali non già per proteggere il contenuto delle chiavette, ma addirittura per impedirne l'uso.



Se queste funzionalità vengono attivate sui PC aziendali, essi non sono in grado di riconoscere questi dispositivi di memoria, sia per le funzioni di scarico dei dati, sia per le funzioni di carico dei dati.

D'altro canto, prima che il lettore si stupisca per queste impostazioni radicali, ricordo che numerose grandi banche italiane, già negli anni '80, impedivano che un floppy disk potesse essere inserito nell'apposita feritoia di un PC da tavolo, in uso all'azienda stessa, proprio per impedire che i dati potessero essere copiati sul floppy o, peggio ancora, sui floppy potessero essere presenti degli applicativi, come ad esempio dei virus, in grado di danneggiare il PC aziendale.

In conclusione di questo paragrafo, è bene ricordare a tutti i soggetti coinvolti nella protezione dei dati personali, che l'attenzione da porre a questi supporti portatili deve essere oltremodo elevata.

Non potendo fare affidamento sul rispetto di pur precise

istruzioni di utilizzo, si raccomanda di rivolgere l'attenzione su supporti di memoria, offerti in comodato d'uso dal titolare del trattamento, dotati di adeguate protezioni. I computer aziendali non devono poter accettare di trasferire dati, oppure estrarre dati, altro che da supporti di memoria aziendali, debitamente validati e protetti.

L'utilizzo, da parte dell'interessato, di supporti di memoria non abilitati non solo deve essere proibito, ma devono essere anche introdotte misure tecniche che permettano di rispettare rigidamente questa disposizione.

CODICI IDENTIFICATIVI E PAROLE CHIAVE

Le parole chiave rappresentano oggi una componente essenziale della nostra vita informatica. Se il lettore preferisce usare l'espressione inglese **password** faccia pure, ma è meglio attenersi all'espressione italiana, che oltretutto è quella che è ufficialmente recepita nei documenti pubblicati dall'autorità Garante, relativi a questo tema.

Ogni giorno si utilizzano parole chiave come metodo di autenticazione per l'accesso a sistemi e servizi, sia nel posto di lavoro sia a casa.

Un recente studio, condotto in Gran Bretagna, ha affermato che in media ogni cittadino utilizza la bellezza di 22 parole chiave, vale a dire un numero di gran lunga superiore a quello che una normale persona può veramente ricordare.

Ecco perché numerose autorità, preoccupate di abbinare la sicurezza informatica alla facilità d'uso, hanno

pubblicato dei documenti che aiutano sia chi gestisce le parole chiave, sia chi le utilizza, ad affrontare in modo efficiente ed efficace questo delicato problema.

Un altro elemento, che desta le preoccupazioni degli esperti di sicurezza è il fatto che, nonostante si utilizzino molte parole chiave, ciò non significa che l'accesso sia più sicuro.

Per solito le parole chiave complesse non sono sufficienti per bloccare gli attacchi, mentre rendono certamente più difficile la vita dell'utente.

Queste parole chiave creano costi, ritardi, bloccano l'accesso per periodi più o meno lunghi e inducono gli utenti ad adottare delle metodologie meno sicure, ma più comode, che aumentano complessivamente il rischio.

Il paragrafo che segue è indirizzato quindi non soltanto agli utenti, ma anche a coloro che debbono impostare e gestire un sistema di parola chiave.

La soluzione più opportuna è quella di introdurre una semplificazione significativa a livello di sistema, piuttosto che imporre agli utenti di ricordare parole chiave sempre più complicate e sempre più difficili da ricordare.

Come vengono scoperte le parole chiave

Per inquadrare correttamente il problema, conviene illustrare subito quali sono le metodologie utilizzate dagli attaccanti per

scoprire le parole chiavi, che l'utente cerca faticosamente di nascondere.

Una delle tecniche più diffuse è l'ingegneria sociale o il *phishing*, che induce l'utente a rivelare autonomamente la sua parola chiave.

Altri sistemi sono legati al fatto che spesso la parola chiave discende da elementi caratteristici dell'utente, come la data di nascita, la via dove abita, il nome del suo cucciolo prediletto e via dicendo. Il fatto che l'utente introduca delle lievi modifiche non spaventa affatto l'attaccante.

Un'altra tecnica un poco più sofisticata consiste nell'intercettare una parola chiave, mentre viene trasmessa su una rete.

Un'altra tecnica assai diffusa è quella di catturare la parola chiave, osservando con aria indifferente, da sopra la spalla, l'utente che digita la parola chiave (*shoulder surfing*).

Una tecnica più sofisticata consiste nell'accedere all'infrastruttura informatica dell'azienda, per catturare le parole chiave, per

solito memorizzate in aree particolari.

Un'altra tecnica assai diffusa è quella brutale o esaustiva, che utilizza applicativi automatizzati per introdurre rapidamente un gran numero di parole chiavi, fino a trovare quella corretta.

Un'altra strategia consiste nel cercare, nelle vicinanze del terminale, ad esempio sotto la tastiera, nei cassetti, sotto il portapenne o simili, dei foglietti dove l'utente, timoroso di dimenticare la parola chiave, l'ha trascritta e, secondo lui, nascosta!

Alcuni consigli preziosi

Il primo consiglio che viene dato a tutti coloro che sono coinvolti nella gestione delle parole chiave è di cambiare immediatamente tutte le parole chiave di default, che spesso sono state già inserite per consentire l'accesso iniziale ad applicativi o sistemi informativi.

Si tratta di un accorgimento che sembra banale, ma in realtà è spesso trascurato. Occorre pertanto cambiare sempre tutte le parole chiave di default, ossia pre impostate, e verificare periodicamente che accidentalmente qualche parola chiave di default non sia stata dimenticata. L'accorgimento è simile a quello che viene attuato da un diligente padrone di casa, che cambiando abitazione, non utilizza la chiave che gli è stata fornita dal proprietario, ma installa una serratura nuova.

Il secondo consiglio tende ad aiutare l'utente a fronteggiare il gran numero di parole chiave che deve gestire. Oggi sono disponibili degli applicativi che permettono di custodire in modo sicuro molte parole chiave, facilitando l'utente nella reperibilità di quella che, volta a volta, è utile.

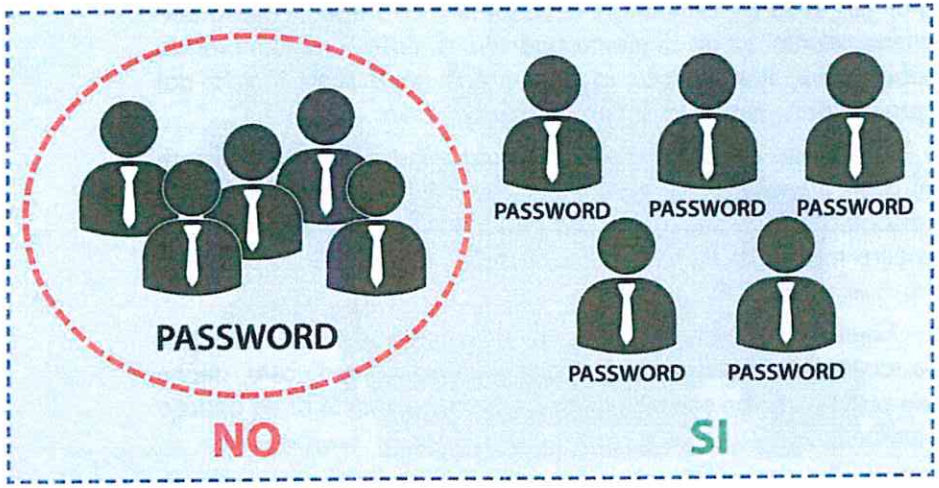
Questi applicativi si chiamano **software password manager** e sono indubbiamente di grande utilità e di basso costo, anche se purtroppo non sono davvero invincibili, a fronte di un attacco deliberato.

Un altro problema frequente discende dal fatto che l'utente viene obbligato a cambiare la parola chiave a intervalli, ad esempio di 30, 60, 90 giorni. Si rammenta che la nostra autorità Garante chiede di cambiare la parola chiave più frequentemente, quando si accede a dati sensibili, rispetto a dati tradizionali.

La realtà è che l'utente, obbligato a cambiare la parola chiave, introduce delle piccole variazioni rispetto alla precedente, e pertanto la modifica della parola chiave non rappresenta un elemento di maggior sicurezza.

Molto più efficace è l'adozione di applicativi che tengono sotto controllo l'utilizzo di parole chiave, mettendo in evidenza al titolare o al responsabile della protezione dei dati personali eventuali digitazioni ripetute ed errate, che potrebbero destare allarme, perché riconducibili al tentativo di individuazione della parola chiave per forza bruta.

Per contro, una prassi assai comune, che va scoraggiata in tutti i modi, è quella di condividere la propria parola chiave con altri colleghi di lavoro. È un elemento che indebolisce fortemente il sistema e contro il quale occorre stabilire regole vincolanti,



mettendo in guardia qualsiasi utente che non si attenga a queste precise disposizioni.

Un altro aspetto interessante riguarda il fatto che nella gran parte dei casi la parola chiave è generata dall'utente. L'utente per solito è pigro e genera una parola chiave che ha basse caratteristiche di sicurezza. D'altro canto, i sistemi che mettono a disposizione delle parole chiave, generate in forma automatica, per solito producono parole chiave che sono talmente complesse, che l'utente non può rammentarle e quindi è costretto a scriverle da qualche parte.

Si può utilizzare, a questo proposito, un generatore che mette a disposizione dell'utente non una sola parola chiave, ma tre o quattro, tra le quali l'utente potrà scegliere quella che egli più facilmente potrebbe ricordare.

Si faccia anche attenzione all'utilizzo di applicativi, che segnalano all'utente il livello di sicurezza della parola chiave che ha scelto. Questi applicativi possono certamente allontanare l'utente dalle parole chiave più banali, ma non tengono conto di altri fattori, che invece i malviventi utilizzano, come ad esempio la conoscenza del soggetto e di dati familiari a lui riconducibili.

Se è importante prestare attenzione alle parole chiave dell'utente, bisogna prestare la massima attenzione alle parole chiave degli amministratori di sistema. La compromissione di questi profili di accesso, infatti, può avere conseguenze assai gravi sulla funzionalità del sistema ed ecco perché tutte le attenzioni del responsabile informatico devono essere certamente indirizzate all'utente, in termini di guida nella scelta e gestione di parole chiavi, ma ancora più devono essere indirizzate agli amministratori di sistema.

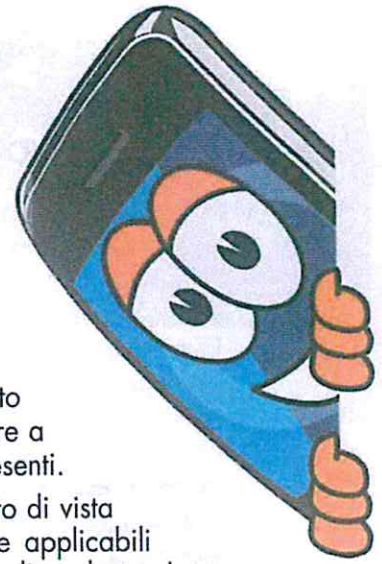
Altri applicativi assai efficaci, di cui uno è già stato illustrato, riguardano l'introduzione di metodologie di controllo del numero di volte che viene digitata una parola chiave errata. Ad esempio, alcuni *smartphone* dispongono di un applicativo che, ove venga digitata per tre volte una parola chiave errata, blocca l'accesso al sistema per alcuni minuti. Se l'operazione si ripete dopo alcuni minuti, la durata del blocco dell'accesso aumenta e così via. Sono sistemi che possono essere utili per fronteggiare attacchi di tipo esaustivo. Questi particolari applicativi si chiamano applicativi di *"throttling"*.

Sempre nel campo degli applicativi che aiutano l'utente, ve ne sono alcuni che bloccano la selezione di parole chiave banali, guidando in un certo senso l'utente a scegliere parole chiave un poco più sicure.

L'USO CORRETTO DI SMARTPHONE DI PROPRIETÀ ED AZIENDALI - BYOD

Per esigenze di continuità operativa, sempre più spesso oggi è consentito agli incaricati del trattamento, che dispongono di *smartphone*, di collegarsi via Internet al sistema informativo aziendale. Gli *smartphone* possono essere dati in comodato d'uso dal titolare del trattamento, oppure essere di proprietà dell'interessato, che ha ricevuto una specifica abilitazione al collegamento al sistema informativo aziendale (BYOD – *bring your own device*). Quest'ultima modalità si presta ad utilizzi assai meno sicuri, per la promiscuità di uso dello *smartphone* per usi personali e per usi aziendali. Tuttavia questo approccio sta incontrando una popolarità sempre crescente, perché consente all'incaricato di utilizzare un solo dispositivo, con il quale egli ha

probabilmente maggiore familiarità.



Nel caso lo *smartphone* venga affidato in comodato d'uso dall'azienda, questa potrà impostare nel dispositivo tutta una serie di applicativi di sicurezza che possono tenere sotto controllo lo scambio di dati personali fra lo *smartphone* e il sistema informativo aziendale, mantenendoli nell'ambito del profilo di accesso, che è stato già concesso all'incaricato. Inoltre è possibile attivare a distanza degli applicativi che, in caso di smarrimento o furto dello *smartphone*, possono provvedere a cancellare automaticamente tutti i dati ivi presenti.

Queste soluzioni garantistiche, da un punto di vista informatico, possono essere più difficilmente applicabili quando lo *smartphone* è di proprietà del dipendente. In questo caso, il titolare del trattamento, con il supporto del responsabile della protezione dei dati, provvederà ad installare sullo *smartphone* degli applicativi, che permettano di compartimentare le aree dove vengono archiviati e gestiti dati personali, trattati dall'azienda di appartenenza. In questo modo sarà possibile realizzare una separazione virtuale fra i dati personali, direttamente riconducibili alla vita di relazione del dipendente, e i dati personali, che vengono trattati per ordine e conto del titolare del trattamento. In quest'ultimo caso sarà anche possibile attivare procedure garantistiche che impediscano l'accesso all'area di memoria, dove questi dati sono custoditi, o perfino possono cancellare quest'area di memoria, in caso di emergenza, senza in alcun modo compromettere l'integrità dei dati, presenti sullo stesso dispositivo ed appartenenti alla vita di relazione del dipendente coinvolto.

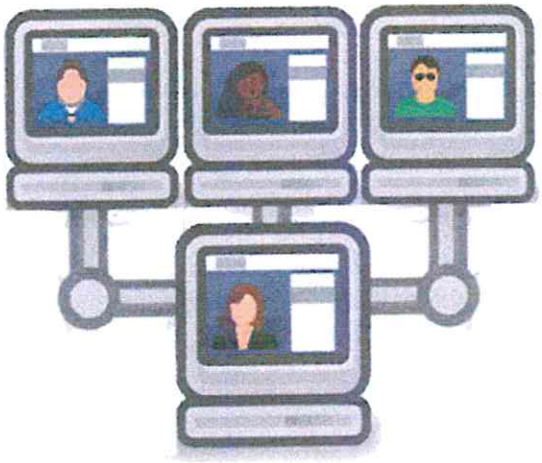
Questi aspetti devono essere chiaramente evidenziati in istruzioni d'uso che vengono impartite dal titolare all'interessato,

il quale deve dare adeguato riscontro per comprensione ed accettazione delle istruzioni stesse.

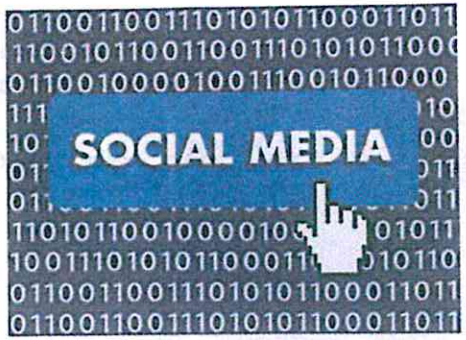
SOCIAL NETWORK E TUTELA DEI DATI PERSONALI

Seppur inavvertitamente, talvolta la presenza di un interessato sui *social network* può portare alla rivelazione o perfino diffusione incontrollata di dati personali, di cui l'interessato è venuto a conoscenza, per ragioni inerenti alla propria attività lavorativa. Il fatto che questo inserimento sui *social network* avvenga in perfetta buona fede non toglie nulla alla responsabilità dell'interessato, che può comportare conseguenze di natura civile e penale, se il soggetto, cui i dati personali si riferiscono, ritiene di essere danneggiato da questo inserimento di dati.

A questo proposito, è bene ricordare che il "considerando" 18 del regolamento stabilisce che esso non si applica al trattamento dei dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale e domestico e quindi senza una connessione con un'attività commerciale e professionale. Tra queste attività a carattere personale e domestico è compreso l'uso dei *social network*.



Questo è il motivo per cui è indispensabile che il titolare ed il responsabile del trattamento, con l'assistenza del responsabile della protezione dei dati, sensibilizzino, grazie ad apposite linee guida ed istruzioni, tutti gli incaricati sulle modalità con cui essi possono accedere ai *social media*, proteggendo però dati personali, cui essi hanno, per ragioni lavorative, la possibilità di accedere: occorre, quindi, mantenere una stretta separazione fra l'accesso a titolo personale, che non rientra nel campo di applicazione del regolamento, e l'accesso che in qualche modo possa essere collegato al ruolo attribuito all'incaricato nel contesto aziendale.



Ecco un esempio di queste linee guida.

I destinatari di queste linee guida sono tutti gli incaricati, appartenenti all'ente, che attivano profili social media, che in qualche modo siano riconducibili non alla persona fisica in questione, ma alla persona fisica in quanto incaricato del trattamento.

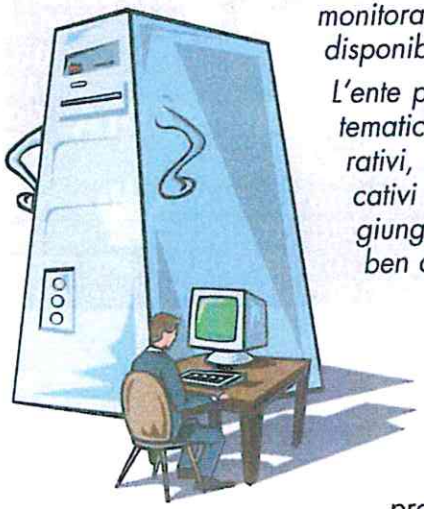
Le linee guida sono costantemente aggiornate secondo l'evoluzione della normativa e lo sviluppo dei diversi social media; queste linee guida sono costantemente portate a conoscenza degli interessati coinvolti.

I social media: profili istituzionali e tematici

L'ente, cui appartiene l'incaricato, si può dotare di profili sui principali social media con l'obiettivo di comunicare in modo efficace le proprie attività, nei confronti delle pubbliche istituzioni e la cittadinanza in genere.

I social media adottati dall'ente sono quelli più diffusi fra i cittadini o in grado di generare i maggiori benefici in termini di efficacia della comunicazione. Essi possono mutare in base alle evoluzioni del mercato e delle tecnologie disponibili.

L'uso che viene fatto dai cittadini dei diversi profili e la dif-



fusione delle informazioni pubblicate vengono monitorati costantemente tramite i sistemi statistici disponibili sulle diverse piattaforme social.

L'ente può anche dotarsi di profili social media tematici gestiti autonomamente dai settori operativi, per perseguire specifici obiettivi comunicativi dei servizi o delle aree specifiche e raggiungere più facilmente segmenti di pubblico ben definiti.

Attivazione di profili social media tematici gestiti autonomamente dal settore

La richiesta di attivazione di un nuovo profilo tematico su uno o più social media deve essere indirizzata al titolare del trattamento o responsabile. Quest'ultimo esercita un'attività di supporto e assistenza nella configurazione iniziale del profilo tematico e di formazione del personale, che eventualmente possa essere adibito alla gestione del profilo.

La responsabilità dei contenuti, dell'aggiornamento e del corretto funzionamento del profilo tematico è completamente a carico del soggetto che lo ha attivato.

I profili tematici attivati su richiesta di specifici soggetti fisici devono mantenere un carattere istituzionale e indicare chiaramente il riferimento all'ente di appartenenza.

Contenuti pubblicabili

I contenuti pubblicati sui profili social media istituzionali e tematici dell'ente riguardano prevalentemente attività istituzionali, iniziative, progetti, informazioni su servizi, eventi, messaggi di pubblica utilità, azioni di propaganda e promozione delle

attività dell'ente, con l'obiettivo di stimolare il coinvolgimento attivo dei cittadini, la partecipazione, il senso di appartenenza alla comunità.

Sui profili social dell'ente è possibile condividere e rilanciare anche contenuti e messaggi provenienti da soggetti terzi, enti pubblici, fondazioni, associazioni e gruppi presenti sul territorio, a patto che il loro contenuto sia di pubblico interesse e utilità e coerente con gli obiettivi comunicativi dell'ente.

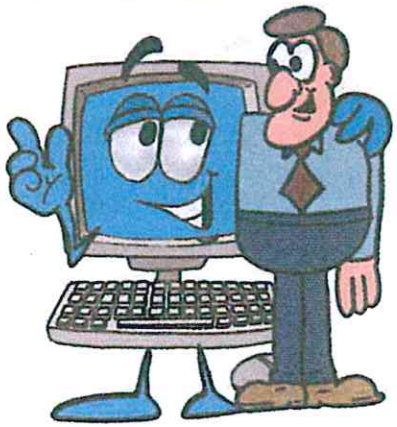
I profili social dell'ente possono essere usati per iniziative patrocinate o che coinvolgano l'ente stesso.

Non è consentito l'utilizzo dei profili social per scopi privati e/o personali (per fini politici, commerciali ...).

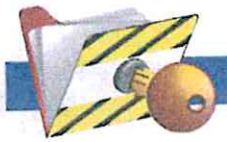
Stile comunicativo e interazioni con account personali

I profili social media dell'ente sono gestiti con un linguaggio semplice e diretto, evitando formulazioni burocratiche ed eccessivamente formali.

Lo stile è neutrale - è l'ente che parla in modo diretto ai destinatari dei messaggi, devono essere omessi i riferimenti personali, tenendo presente che i redattori dei messaggi comunicano per conto dell'ente.



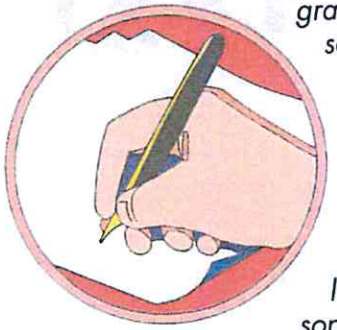
Gli account personali di dipendenti e collaboratori possono essere usati per l'accesso alle funzioni dell'ente sui social media solo nel caso risulti difficoltoso o inefficiente creare account dell'ente, come nel caso di Facebook. In ogni caso, quando si pubblicano contenuti o commenti sui profili istituzionali o tema-



tici in nome e per conto dell'ente, non devono essere usati gli account personali.

Nel caso occorra fornire una risposta circostanziata a sollecitazioni degli utenti dei social media da parte dei responsabili dell'ente, si consiglia di pubblicare la risposta adottando il profilo istituzionale o tematico, e apponendo in calce il nome e il ruolo di chi replica.

L'utilizzo improprio dei profili social dell'ente costituisce, per i dipendenti e collaboratori dell'ente, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro vigente, oppure previste dallo statuto e regolamento dell'ente, fatto salvo comunque il diritto dell'ente al risarcimento dei danni eventualmente patiti a causa della condotta del dipendente o del socio.



Il mancato rispetto delle regole e dei divieti sopraindicati costituisce, per i collaboratori esterni, violazione degli obblighi contrattuali.

Aggiornamento dei social media

I profili social media dell'ente, per essere efficaci, devono essere costantemente mantenuti aggiornati. In caso di commenti e domande dei fruitori, che richiedano una risposta da parte dell'ente, essa deve essere fornita nel minor tempo possibile, compatibilmente con i normali orari di lavoro del personale.

I soggetti che attivano profili tematici sono tenuti a organizzarsi e individuare il personale responsabile per:

- *mantenere aggiornati i profili pubblicando con continuità informazioni e notizie;*

- *rispondere nel minor tempo possibile alle domande dei cittadini o da altri soggetti interessati al profilo tematico;*
- *replicare nel minor tempo possibile in caso di commenti che necessitino di chiarimenti da parte dell'ente;*
- *eliminare eventuali commenti inadeguati, offensivi o scritti con linguaggi inappropriati;*
- *rispondere ad eventuali messaggi inviati direttamente al profilo.*

UNA "RINFRESCATA" SU PROBLEMI GIÀ ESISTENTI

L'incaricato del trattamento, per motivi ovviamente connessi allo svolgimento della sua attività, è certamente coinvolto in una frequente trasmissione di dati personali a soggetti terzi. Questa comunicazione può avvenire via telefono, per messaggi di posta elettronica, per *facsimile* o per SMS.

Anche se i problemi legati a questo tipo di comunicazione sono ormai ben noti, è opportuno riesaminare insieme le cautele che deve prendere l'interessato, per evitare che i dati personali possano essere comunicati a soggetti che non avevano titolo a conoscerli.

La comunicazione via telefono

Ragioni di efficienza ed efficacia, e soprattutto di rapidità di comunicazione, possono talvolta rendere necessaria la

comunicazione di dati personali via telefono ad un soggetto terzo. L'incaricato del trattamento deve accertarsi che colui che si trova all'altro capo della linea telefonica sia persona autorizzata a ricevere questi dati. Ad esempio, è meglio essere prudenti nel lasciare questi dati alla segretaria di un dirigente, al momento fuori posto, perché non è detto che essa sia autorizzata a prenderne conoscenza.

In caso l'incaricato abbia dei dubbi, è meglio richiamare; in occasione della richiamata, sarà anche possibile chiedere all'incaricato terzo coinvolto se, in una prossima occasione, sarà possibile lasciare questi dati alla segretaria, trasferendo quindi l'intera responsabilità di diligente custodia dei dati a questo soggetto terzo.

La comunicazione via posta elettronica

Anche in questo caso, occorre prestare estrema attenzione all'invio di dati personali ad indirizzi di posta elettronica di tipo generico, che spesso le aziende mettono disposizione per colloquiare con l'esterno (ad esempio - *info@xxx.it*). Poiché non si ha alcuna certezza circa i soggetti che potranno osservare questi messaggi di posta elettronica, è sempre bene inviare questi dati soltanto a indirizzi riconducibili ad un soggetto specifico.

In caso di dubbio, è meglio fare una telefonata preventiva, per accertarsi che questo invio sia legittimo. Si tratta di una precauzione che deve avere non solo chi invia il messaggio, ma anche chi lo riceve: ancora una volta, la sicurezza del trattamento dei dati si raggiunge con procedure di cooperazione e collaborazione. Infine, un'ulteriore parola di attenzione merita l'invio di messaggi di posta elettronica con allegati.

Spesso queste allegati presentano aspetti critici, che occorre valutare attentamente, studiando eventualmente la possibilità di inviare gli allegati con altri mezzi più sicuri di comunicazione.

La comunicazione via fax

Sono ormai numerosi i casi, registrati dalle cronache, in cui un unico numero di fax viene utilizzato da numerose entità, come ad esempio nell'ambito di studi medici associati. Questi studi medici, per ragioni di economia, utilizzano un unico numero di fax, al quale vengono inviati messaggi, contenenti dati sanitari talvolta sensibili, senza avere la certezza che il fax verrà raccolto proprio dal medico coinvolto.

Anche in questo caso, occorre accertarsi che l'invio di fax avvenga in un contesto garantistico, eventualmente preceduto da una telefonata di preavviso.

Le comunicazioni via SMS

Anche se in genere queste comunicazioni sono piuttosto brevi, è sempre possibile che in esse siano presenti dati personali, anche sensibili, che il mittente inserisce senza prestare troppa attenzione al profilo del soggetto, cui il messaggio viene inviato.

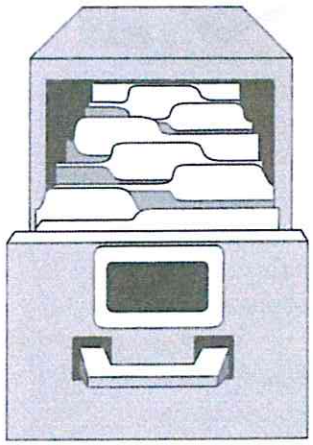
Le precauzioni da prendere, in questo caso, sono molto simili a quelle da prendere quando si avvia una conversazione telefonica; anzi, in questo caso le precauzioni devono essere ancora maggiori, in quanto i dati personali vengono scritti, anziché scambiati verbalmente.

CUSTODIA E CONTROLLO DI DOCUMENTI CARTACEI

Come è facilmente intuibile, il regolamento europeo non dà indicazioni specifiche in merito alle modalità di tutela dei documenti cartacei sui quali si trovano dati personali.

Questo compito viene affidato, nel quadro delle responsabilità globale del titolare, del responsabile e del responsabile della protezione dei dati a questi tre soggetti, secondo una scala di priorità, che il regolamento ben identifica.

Il **titolare del trattamento** è l'autorità di vertice, che ha la facoltà di farsi assistere, nella messa a punto di strategie di protezione dei dati personali, che il titolare tratta, da un **responsabile del trattamento**.



Infine, se vengono rispettate determinate condizioni, afferenti a speciali tipologie di trattamento, il titolare deve individuare un **responsabile della protezione dei dati**. Nulla impedisce che, anche laddove questa individuazione non sia obbligatoria, il titolare possa comunque farsi assistere anche da questo soggetto, che ha tutt'una serie di incombenze, chiaramente illustrate nel regolamento.

Ad esempio, tra le incombenze che gli possono essere assegnate v'è anche la messa a punto di un piano di formazione per gli incaricati del trattamento. È proprio nel quadro di questo piano di formazione che potranno essere sensibilizzati ed informati gli incaricati sia sugli aspetti relativi alla protezione dei dati personali residenti su un computer aziendale, oppure su strumenti mobili, sia sugli aspetti relativi alla protezione dei dati su supporto cartaceo.

NON È VERO CHE LA CARTA SIA SPARITA!

Anche se i messaggi relativi ad una civiltà digitale, nella quale poco o nulla si stamperà, in quanto tutto sarà disponibile con documentazione elettronica, archiviata su *personal computer*, su *smartphone*, o sul *cloud*, la realtà, come ben si sa, è completamente diversa.

Anche se oggi in alcuni uffici postali è possibile firmare utilizzando uno strumento elettronico, anche se alcuni corrieri fanno firmare la ricevuta della consegna di un pacco su un altro strumento elettronico, anche se oggi è possibile prelevare e movimentare denaro via internet senza avere bisogno di un foglio di carta od una penna, sono in realtà ancora moltissime le circostanze nelle quali un documento cartaceo, magari sottoscritto dall'interessato al trattamento, rappresenta un aspetto fondamentale per dare validità ad un contratto, confermare una transazione, stipulare una polizza assicurativa e via dicendo.

Lo stesso regolamento, che pure cerca di convalidare un elevato livello di digitalizzazione dei dati personali, si trova obbligato a riconoscere che senza documenti scritti certi trattamenti potrebbero non avere sufficiente validità.

Ad esempio nel "considerando" 80, il titolare del trattamento, che si trova all'esterno dell'Unione europea, deve obbligatoriamente designare un responsabile, avente sede in un paese dell'Unione europea, mediante un contratto scritto.

Il titolare del trattamento, che deve fornire all'interessato un'adeguata e accurata informativa circa le finalità per le quali acquisisce i dati personali dell'interessato, deve dare questa informativa in forma scritta, innanzitutto, anche se il regolamento consente che possano essere utilizzate, in seconda battuta, anche altre forme (articolo 12).

Ma non è finita.

Quando un titolare del trattamento ha sviluppato una valutazione di impatto ed il risultato lo pone davanti ad alcuni dubbi afferenti al trattamento che sta per iniziare, egli deve rivolgersi all'autorità Garante nazionale grazie alla procedura di consultazione preventiva, prevista dall'articolo 36. L'autorità Garante deve dare il proprio parere scritto entro otto settimane da quando il titolare ha avviato la pratica di consultazione preventiva.

Questa rassegna potrebbe continuare ancora a lungo, prendendo, ad esempio, in esame le richieste di assunzione, accompagnate da un *curriculum vitae* stampato secondo il formato europeo.

Non parliamo poi delle prescrizioni per medicinali, che si vorrebbero trasformare in ricette elettroniche, ma che per adesso continuano ad avere una forte componente cartacea.

Sono queste ragioni sufficienti perché, nel programma di formazione di un incaricato del trattamento, particolare attenzione debba essere prestata alla gestione di dati personali su supporto cartaceo.

COSA SIGNIFICA CUSTODIA E COSA SIGNIFICA CONTROLLO

Le disposizioni legislative in vigore in Italia, convalidate e supportate dall'autorità Garante, fanno riferimento al fatto che i dati su supporto cartaceo debbono essere custoditi e controllati dall'interessato che li detiene.

L'utilizzo di due diverse parole, che ad una prima occhiata potrebbero sembrare simili, merita invece un'attenta disamina.

Con l'espressione "custodire" si fa riferimento al fatto che l'interessato, ad esempio, ha preso in consegna un raccoglitore, all'interno del quale sono inseriti numerosi documenti cartacei,

sui quali sono riportati dati personali.

La responsabilità di custodia consiste nel prendere in consegna questo raccoglitore e custodirlo, appunto, con diligenza, senza lasciarlo abbandonato sulla scrivania del posto di lavoro, ma riponendolo all'interno di un cassetto chiuso a chiave, quando i documenti contenuti in questo raccoglitore non devono essere consultati. Anzi, spesso l'incaricato del trattamento deve solo custodire il raccoglitore per metterlo a disposizione, ad esempio, di un altro incaricato, il quale sì potrebbe aver bisogno di consultare i documenti contenuti all'interno del raccoglitore.

Il gestore di un archivio, racchiuso in un armadio dove si trovano alcune dozzine di raccoglitori, ha appunto la funzione di custodire questi raccoglitori, e non certo quella di esaminarne il contenuto.

Andiamo adesso, invece, a vedere cosa significa "controllare" un raccoglitore.

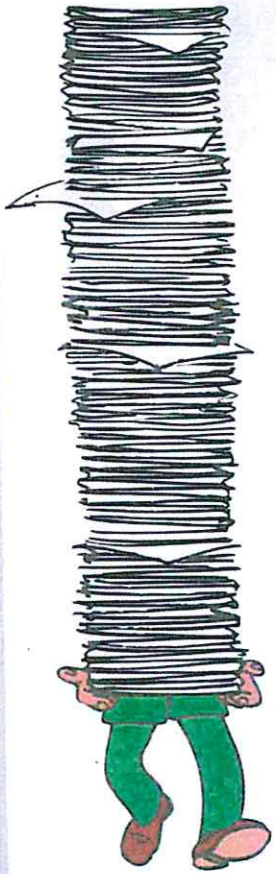
Controllare un raccoglitore fa riferimento al fatto che l'interessato in questione deve poter aprire il raccoglitore, esaminare e quindi controllare ogni singolo documento in esso contenuto, non solo per acquisire informazioni specifiche, ma anche per verificare la completezza della documentazione raccolta, ad esempio per confronto con un indice, posto sulla prima pagina del raccoglitore.

L'operazione di controllo è evidentemente assai più impegnativa, rispetto alla più semplice funzione di custodia: poiché non è detto che lo stesso interessato debba svolgere sia funzioni di custodia, sia funzione di controllo, ben si capisce perché nelle istruzioni di trattamento, impartite all'incaricato, si faccia distinzione tra le due funzioni.

TROPPE FOTOCOPIE!

In tutti i corsi di formazione afferenti ad una diligente gestione di documentazione cartacea, contenente dati personali, si avanza sempre la specifica raccomandazione che non venga fatta alcuna fotocopia di questa documentazione, se non necessaria.

Deve essere, quindi, cura dell'incaricato che tratta, su delega del titolare del trattamento, questi documenti cartacei, prendere ogni appropriata cautela perché la documentazione che egli deve custodire con diligenza, non sia prelevata a sua insaputa e fotocopiata. Un malvivente, che approfitta della distrazione dell'incaricato che ha lasciato il raccoglitore incustodito sul tavolo, può estrarre documenti, anche oltremodo sensibili, e farne fotocopia, senza che l'incaricato si accorga di nulla.



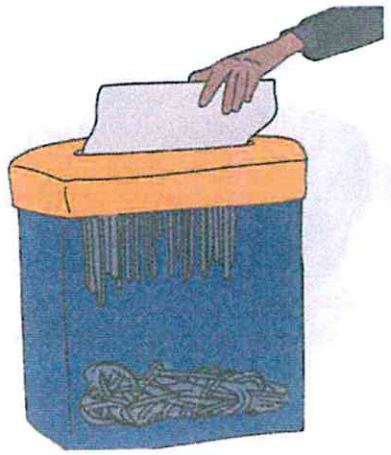
Ecco perché anche la semplice funzione di custodia richiede comunque un elevato livello di diligenza.

Supponendo che il caso sopra illustrato non si sia verificato, grazie proprio alla diligenza dell'incaricato, vediamo cosa bisogna fare, quando si deve effettuare una fotocopia e questa fotocopia purtroppo non è di soddisfacente qualità.

Un obbligo tassativo che incombe all'incaricato, che si trova davanti a questa fotocopia mal riuscita, è quello di renderla illeggibile per chiunque altro.

La soluzione perfetta, che dovrebbe essere predisposta dal titolare del trattamento, con il supporto dei suoi collaboratori, è quella di mettere a disposizione degli incaricati un distruggitore per documenti, con appropriate caratteristiche. Stiamo parlando di un piccolo distruggitore da ufficio, poco più grande di un cestino della carta straccia, che in pochi secondi

può distruggere alcune pagine fotocopiate in modo difettoso.



Poiché purtroppo in molti uffici questo distruggitore non sempre è disponibile, un comportamento diligente da parte dell'incaricato coinvolto è quello di strappare i fogli di carta in piccoli pezzi, con dimensioni dell'ordine di un francobollo o poco più, in modo che sia difficile per chiunque recuperare dal cestino della carta straccia i frammenti, che non dovrebbero comunque consentire di ricostruire il documento originale.

CONSERVARE VA BENE, MA PER QUANTO?

Nel caso precedente è stata illustrata la situazione in cui l'incaricato provvede immediatamente alla distruzione della copia superflua.

Ma il regolamento europeo va molto più in là, perché addirittura prescrive che, in determinate circostanze, anche il documento originale debba essere distrutto.

Vediamo perché.

Una prescrizione tassativa del regolamento europeo è quella che i dati personali, che il titolare ha raccolto dall'interessato, debbano essere custoditi soltanto per il tempo necessario a soddisfare le finalità della raccolta.

In certi casi, le autorità Garanti nazionali possono imporre anche delle limitazioni vincolanti, come ad esempio nel caso di

una videoregistrazione, che non può essere conservata per più di una settimana, salvo richiedere specifica deroga all'autorità Garante nazionale (nel caso dell'Italia).

Ma un'attenta lettura del regolamento ci dice che la durata massima di una settimana, indicata dall'autorità Garante, è proprio la durata massima! Ciò significa che anche la conservazione della videoregistrazione per 24 ore deve essere comunque motivata, proprio per dimostrare che le finalità per cui il titolare conserva la videoregistrazione sono soddisfatte nell'arco delle ventiquattro ore.

Passato tale termine, la videoregistrazione dev'essere cancellata.

Lo stesso ragionamento si applica ai documenti cartacei e, più in generale, a qualunque dato personale, su supporto cartaceo o digitale, che viene raccolto dal titolare.

Nel momento stesso in cui un titolare raccoglie dati personali, deve anche indicare il tempo massimo di conservazione di questi dati, dopodiché occorre procedere alla distruzione.

Tornando all'esempio fatto in precedenza, circa un'indagine di mercato che viene svolta presso i clienti di un supermercato, è del tutto normale che, in fase di intervista, si compilino delle schede cartacee. Al termine delle interviste e a conclusione della ricerca di mercato, non solo i dati acquisiti devono essere trasformati in forma anonima, come ad esempio l'indicazione percentuale di gradimento del prodotto, ma

le schede originali debbono essere distrutte.

Un'altra circostanza nella quale un dato deve essere distrutto è legata ad esempio al fatto che l'interessato, dopo aver esercitato il diritto di accesso, si è reso conto che alcuni suoi dati in possesso del titolare sono errati.

A seconda di quale sia il supporto sul quale i dati sono conservati, il titolare deve necessariamente procedere alla rettifica del dato, se possibile, o alla cancellazione del dato stesso.

È sufficiente leggere il "considerando" 39 per vedere come questa indicazione sia priva di qualunque ambiguità. Il concetto è ribadito nel "considerando" 59.

Infine, il colpo di grazia viene dato dal **diritto all'oblio**, che il regolamento generale europeo pone in particolare evidenza, come già ha fatto la Corte di giustizia europea.

È evidente che il diritto all'oblio viene garantito con la cancellazione informatica dei dati digitalizzati e con la distruzione fisica dei dati su supporto cartaceo.

L'articolo 4 del regolamento, che offre le definizioni delle parole utilizzate in prosieguo, definisce così il trattamento di dati:

*2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la **cancellazione o la distruzione**;*

Accertato quindi il fatto che fra le operazioni di trattamento è posta in bella evidenza la cancellazione o la distruzione, facendo appunto riferimento a supporti digitali o supporti fisici, vediamo come sia possibile procedere in modo corretto.

Il vero problema non si pone certo quando si devono distruggere due o tre fotocopie mal riuscite, ma si pone quando ci troviamo davanti a grandi quantità di dati, perfino a livello di quintali di carta, che devono essere distrutti.

LA DISTRUZIONE CARTACEA PROFESSIONALE

Oggi esistono delle aziende specializzate che sono in grado di prelevare grandi quantità di documenti cartacei e procedere alla loro distruzione, con tecniche oltremodo sofisticate che sono specificamente illustrate in una norma europea.

Quando il titolare decide che è giunta l'ora di distruggere supporti cartacei, perché le finalità per cui vennero raccolti i dati ivi presenti sono esaurite, deve prendere di conseguenza anche una seconda decisione.

La seconda decisione fa riferimento alla modalità di distruzione del supporto cartaceo, che è direttamente proporzionale alla delicatezza dei dati presenti sui supporti cartacei stessi.

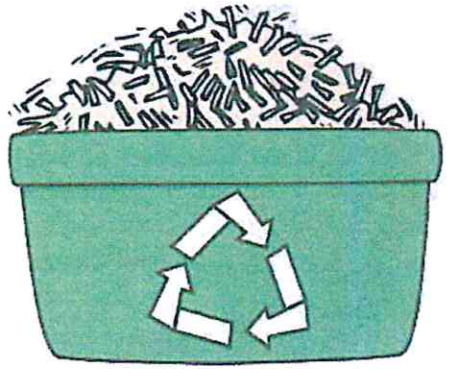
La norma europea prevede vari livelli di distruzione, che vanno dalla suddivisione in strisce, di larghezza variabile da 10 millimetri fino a due millimetri, fino alla suddivisione in frammenti, di dimensioni sempre più piccole, fino a giungere alla polverizzazione.

Come appare evidente, questi aspetti tecnici devono essere supportati da adeguati e garantistici aspetti procedurali.

Ad esempio, se la ditta incaricata della distruzione controllata della carta si trova a qualche distanza dall'archivio ove la carta si trova, occorre che il trasporto sia effettuato da soggetti ben individuati, addestrati specificamente, su automezzi protetti da impianto antintrusione.

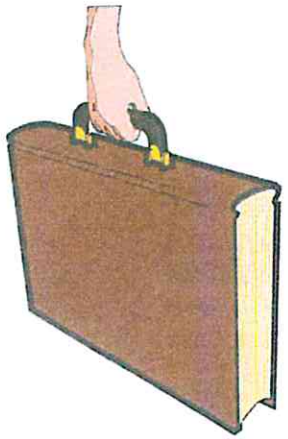
Una volta giunti presso l'insediamento dove si procederà alla distruzione, i documenti cartacei devono essere tenuti sotto stretto controllo, inquadrati da un impianto di videosorveglianza e protetti da un impianto antintrusione, fino a che non viene completata l'operazione di taglio in strisce o frammentazione o polverizzazione.

Solo a questo punto il responsabile dell'azienda in causa rilascerà al titolare del trattamento una dichiarazione liberatoria e sarà possibile, per la salvaguardia dell'ambiente, recuperare questi frammenti, macerarli in appositi mulini a pale e trasformarli in carta riciclata.



In passato si usava una tecnica assai più brutale, vale a dire l'utilizzo della carta come combustibile negli inceneritori. Oggi la nostra accresciuta sensibilità alla tutela dell'ambiente fa sì che questa soluzione sia stata in pratica del tutto abbandonata, mentre le aziende che offrono un servizio di distruzione con riciclo stanno prosperando.

QUANDO E COME È POSSIBILE TRASFERIRE ALL'ESTERO DATI PERSONALI



In un mondo sempre più globalizzato, appare del tutto chiaro che sia possibile che, in fase di trattamento di dati personali, procedere al trasferimento di questi dati verso paesi terzi, vale a dire paesi non compresi nell'Unione europea.

Al proposito, si rammenta che tutte le nazioni dell'Unione europea, da questo punto di vista, rappresentano un'entità omogenea, in quanto in tutte queste nazioni si utilizzano le stesse regole di trattamento di dati personali.

Occorre anche sottolineare il fatto che tra i paesi non compresi nell'Unione europea sono anche incluse le organizzazioni internazionali, come l'Unesco, in quanto tali organizzazioni possono spostare i dati in una qualunque parte del mondo, ove hanno una rappresentanza od ufficio, ed occorre quindi prendere appropriate cautele, dove i dati siano trasferiti a queste organizzazioni internazionali.

Il regolamento, come prescrizione generale all'articolo 44, impedisce che i dati personali di interessati europei, trattati da titolari del trattamento europei, possano essere trasferiti all'esterno dell'Unione europea, se non vengono verificate alcune condizioni, illustrate di seguito.

TRASFERIMENTI BASATI SU UNA VALUTAZIONE DI ADEGUATEZZA

Poiché anche altri paesi del mondo hanno adottato delle regole, in merito alle modalità sicure di trattamento di dati personali, potrebbe non essere appropriato impedire comunque un trasferimento verso questi paesi, che in certi casi potrebbero perfino garantire una protezione di questi dati, forse anche maggiore di quella disponibile in Europa.

Per questa ragione, in conformità a quanto illustrato nell'articolo 45 del regolamento, la Commissione europea pubblica un elenco, costantemente aggiornato, dei paesi o delle organizzazioni internazionali che garantiscono un soddisfacente livello di protezione. In questo caso non è richiesta alcuna specifica autorizzazione per il trasferimento dei dati.

Si offre di seguito un'elencazione, solo esemplificativa, dei principali paesi verso i quali è possibile trasferire dati personali senza problemi:

- Islanda, Liechtenstein, Norvegia, Svizzera, Argentina, l'isola di Guernesey e quella di Jersey, l'Isola di Man ed il Canada.

Ovviamente, i criteri in base ai quali la Commissione europea inserisce una nazione terza in questo elenco dipende da un'attenta valutazione delle modalità con cui i dati personali vengono protetti. L'elenco, come accennato, è costantemente aggiornato, in quanto la Commissione europea tiene sotto stretto controllo le regole adottate in questi paesi e, ove si abbia la sensazione che il livello di protezione dei dati non sia più soddisfacente, può provvedere, con provvedimento d'urgenza, a cancellare il paese dall'elenco.

TRASFERIMENTO IN PRESENZA DI APPROPRIATE SALVAGUARDIE

Il titolare del trattamento o il responsabile del trattamento possono trasferire dati personali di un paese terzo, a condizione che essi abbiano introdotto delle appropriate salvaguardie, e sotto condizione che i diritti degli interessati siano rispettati ed esistano anche rimedi ad eventuali violazioni dei diritti degli interessati.

Le modalità con cui può essere raggiunto questo appropriato livello di salvaguardie sono diverse e sono puntualmente elencate nell'articolo 46.

Giova rilevare che la presenza di queste salvaguardie permette ad un titolare o responsabile del trattamento di trasferire dati personali ad un altro titolare e responsabile del trattamento, residente in questo paese terzo, ma che potrebbe non avere alcuna relazione particolare, ad esempio di appartenenza allo stesso gruppo d'azienda multinazionale, con il titolare che effettua il trasferimento.

Ove invece il trasferimento avvenga fra due aziende appartenenti allo stesso gruppo, si devono applicare le norme appresso illustrate.

TRASFERIMENTO IN PRESENZA DI NORME VINCOLANTI D'IMPRESA

In precedenza è stato già accennato al fatto che la movimentazione di dati personali fra diversi paesi rappresenta oggi

quasi una necessità, per la dimensione multinazionale che molte aziende hanno acquisito. In questo contesto, è evidente che vi può essere differenza fra il trasferimento di un dato gestito da un titolare, appartenente ad un'azienda, ad un titolare di altra azienda, residente in altro paese, ma appartenente allo stesso gruppo aziendale.

In questo caso infatti è più facile introdurre delle norme vincolanti d'impresa, che legano tutte le aziende, che appartengono allo stesso gruppo multinazionale, facilitando quindi il trasferimento di dati da un'azienda all'altra. La capogruppo multinazionale ha infatti ben maggiori poteri nell'imporre queste norme a tutte le aziende del gruppo.

Proprio a questa situazione fa riferimento l'articolo 47, che illustra in particolare come devono essere concepite queste norme vincolanti d'impresa, gli obblighi di applicazione, nonché il rispetto dei diritti degli interessati, che costituiscono forse la parte preminente dell'intera serie normativa.

Devono anche essere indicate con chiarezza le responsabilità dei soggetti coinvolti, facendo sì che, ove un titolare residente in una nazione terza non rispetti queste regole, ne risponda comunque il titolare, basato nell'Unione europea, che ha autorizzato il trasferimento dei dati personali. Si garantisce così a un interessato, residente in una nazione europea, la possibilità di esercitare i suoi diritti, senza dover necessariamente esercitarli in un paese terzo, con tutte le evidenti difficoltà connesse.

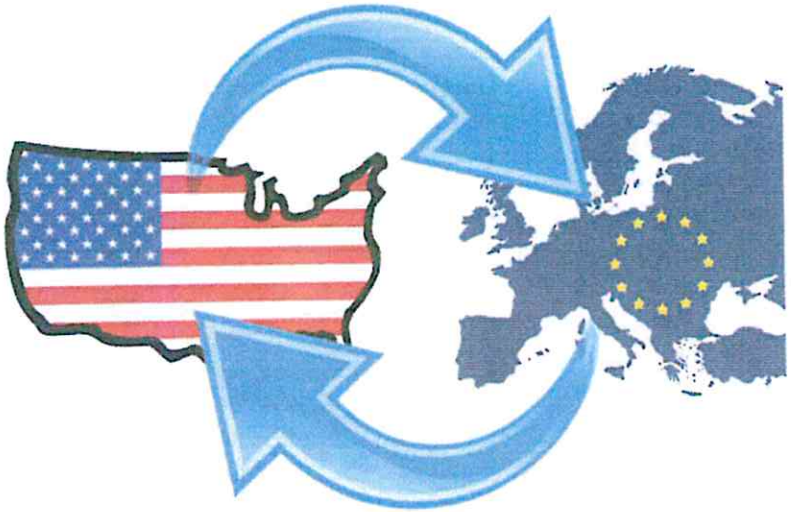
È facoltà della Commissione europea indicare degli schemi generali per l'impostazione e articolazione di queste norme vincolanti d'impresa, nel rispetto di procedure specifiche e garantistiche, illustrate al comma 2 dell'articolo 93.

I RAPPORTI CON GLI STATI UNITI D'AMERICA

Appare evidente che il trasferimento di dati personali tra l'Europa e gli Stati Uniti di America rappresenti un aspetto particolarmente critico, per la straordinaria quantità di dati che vengono costantemente scambiati fra questi due mondi, che da soli costituiscono la grande maggioranza dei rapporti commerciali nel mondo.

Per semplificare questo scambio di dati, anni fa si mise a punto un protocollo specifico, chiamato ***safe harbor***, vale a dire ***porto sicuro***: il protocollo era concepito in maniera tale che un'azienda americana potesse ricevere dati provenienti dall'Europa, a condizione che si impegnasse per iscritto a garantire il rispetto di questo protocollo di sicurezza, concordato fra le autorità statunitensi e le autorità europee.

Questo protocollo ha regolato per anni questo trasferimento di dati, finché una sentenza della Corte di giustizia europea, nell'ottobre 2015, ha dichiarato che questo protocollo non era



più in grado di garantire un sufficiente livello di protezione al trasferimento di dati personali di interessati europei: la Corte ha posto marzo 2016 come termine ultimo per abolire questo accordo.

È facile immaginare come questa situazione abbia gettato nello scompiglio non solo moltissime aziende americane ed europee, ma anche i governi, rispettivamente nella veste del dipartimento americano del commercio, negli Stati Uniti, e la Commissione europea, in Europa.

Queste due entità si sono messe freneticamente al lavoro e sono riuscite a pubblicare un documento congiunto, che è stato battezzato ***EU-USA privacy shield***. Questo documento rappresenta indubbiamente un grande passo avanti rispetto al precedente accordo, perché i diritti degli interessati europei sono tutelati in maniera assai più specifica.

Ad esempio, viene istituita la figura di un *ombudsman*, vale a dire un referente americano, cui qualunque cittadino europeo può rivolgersi, ove non riesca a trovare un punto di accordo circa una presunta violazione dei suoi diritti da parte di un'azienda americana.

Vengono introdotti dei tempi certi di risposta e viene sancito il principio, già in vigore in Europa, che l'interessato non deve pagare una somma per far valere i suoi diritti, in particolare il diritto di accesso, di rettifica, di cancellazione, nonché l'ormai famoso diritto all'oblio.

Questo accordo deve però essere sottoposto all'approvazione di altri organi legislativi dell'Unione europea e attualmente la procedura è in corso.

Ciò significa che, almeno al momento, il trasferimento di dati personali fra aziende aventi sede in Europa ed aziende aventi sede negli Stati Uniti può avvenire sulla base non di un accordo quadro, ma di una delle altre modalità di trasferimento, illustrate in precedenza.

QUANDO IL TRASFERIMENTO È COMUNQUE POSSIBILE

L'articolo 49 fa riferimento a circostanze specifiche, nelle quali il trasferimento di dati in una nazione terza è comunque possibile.

Tra queste eventualità si pone in particolare evidenza il fatto che l'interessato, che alla fin fine è signore e padrone dei suoi dati, abbia dato esplicito consenso a questo trasferimento, dopo essere stato informato circa i rischi cui i suoi dati personali potrebbero essere soggetti.

Parimenti, in casi di urgenza, quando ad esempio si deve salvaguardare la vita di un interessato, che si trova all'estero, i suoi dati personali anche particolari possono essere immediatamente trasferiti, perché il principio di salvaguardia della vita umana ha evidentemente priorità rispetto alla tutela dei dati personali.

Parimenti, se il trasferimento è necessario per la conclusione di un contratto, che è stato sottoscritto dall'interessato, i dati possono essere trasferiti.

L'articolo 49 prende in esame anche qualche altra modalità autorizzata.

Infine, è bene chiudere questo capitolo ricordando che i limiti sopra indicati rappresentano una delle principali cause per cui il trasferimento di dati nel *cloud* spesso può portare a violazioni di queste prescrizioni. Non sempre infatti è possibile avere certezza dell'ubicazione fisica del *server*, verso il quale i dati vengono trasferiti e potrebbe accadere che tale *server* si trovi in un paese terzo, verso il quale il trasferimento non sarebbe autorizzato. È questo solo un esempio dei problemi che si pongono nel proteggere in modo adeguato i dati personali, in un contesto sempre più globalizzato.

RICORSI, RESPONSABILITÀ E SANZIONI

Il capo VII del regolamento è tutto dedicato al tema dei ricorsi, della responsabilità e delle sanzioni.

Mentre alcuni aspetti non sono molto diversi, rispetto alle disposizioni attualmente vigenti in Italia, il tema delle responsabilità e delle sanzioni è stato modificato in maniera significativa. Vediamo di prendere in esame questi tre diversi argomenti.

IL RECLAMO

Qualunque interessato al trattamento, che abbia delle lagnanze nei confronti di un titolare di trattamento, o suoi collaboratori, può avanzare un reclamo all'autorità Garante nazionale.

Sin qui nulla è diverso da quanto oggi in essere, salvo il fatto che in Italia l'autorità Garante ha ritenuto bene suddividere queste tipologie di lagnanze in tre categorie:

- il ricorso,
- il reclamo,
- la segnalazione.

Il ricorso viene presentato esclusivamente per violazioni afferenti al diritto di accesso da parte dell'interessato; il reclamo viene presentato per qualunque altro tipo di violazione che vede comunque sempre coinvolto l'interessato, mentre la segnalazione viene

presentata da chiunque abbia rilevato una violazione nel trattamento dei dati, che potrebbe però non riguardare direttamente il segnalante.

Questa suddivisione in tre categorie può certamente continuare a rimanere in essere, anche con l'entrata in vigore del nuovo regolamento, in quanto serve esclusivamente a fare ordine e in nulla limita le modalità con cui l'interessato può far valere i propri diritti.

Parimenti, poco o nulla è cambiato nel fatto che è facoltà dell'interessato rivolgersi inizialmente all'autorità Garante, vale a dire un'autorità amministrativa, oppure direttamente alla magistratura, vale a dire un'autorità giurisdizionale.

Il ricorso all'autorità giurisdizionale può anche essere presentato, ove l'interessato, persona fisica o giuridica che sia, non sia soddisfatto dell'eventuale pronunzia dell'autorità amministrativa.

Anzi, il regolamento diventa più vincolante, perché l'articolo 78 impone che l'autorità di controllo dia riscontro al reclamo o comunichi l'esito, entro tre mesi dalla presentazione. Questo limite temporale è importante, perché oggi in Italia questo limite non è chiaramente evidenziato.

Significativa è l'indicazione dell'articolo 80 che in un certo senso permette l'avvio di una cosiddetta *"class action"*, vale a dire concede ad un interessato, o categorie di interessati, di *"farsi rappresentare da organismi, organizzazioni*

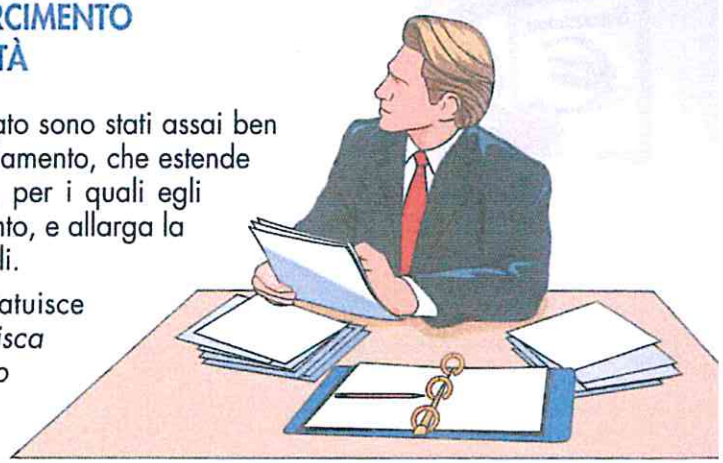
o associazioni senza scopo di lucro, i cui obiettivi statutari siano di pubblico interesse e siano attive nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali."

Questo diritto di rappresentanza si estende anche al **diritto di risarcimento**.

Infine, nel rispetto del principio di coerenza, l'autorità giurisdizionale, vale a dire la magistratura che abbia notizia di azioni riguardanti lo stesso oggetto avanzate nei confronti di titolari del trattamento, che fanno riferimento ad un altro Stato membro, deve prendere contatto con tale autorità dell'altro Stato membro per confermare l'esistenza delle azioni. In caso, essa può sospendere le sue azioni in modo da evitare che lo stesso tema venga giudicato contemporaneamente da autorità giurisdizionali residenti in paesi diversi dell'Unione europea.

IL DIRITTO AL RISARCIMENTO E LE RESPONSABILITÀ

I diritti dell'interessato sono stati assai ben difesi dal nuovo regolamento, che estende le tipologie di danni, per i quali egli ha diritto al risarcimento, e allarga la platea dei responsabili.



L'articolo 82 statuisce che *"chiunque subisca un danno materiale o immateriale, causato dalla violazione*

del presente regolamento, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento od al responsabile del trattamento."

L'inserimento dei danni anche immateriali allarga indubbiamente il livello di responsabilità del titolare. Parimenti si allarga la platea dei soggetti contro i quali l'interessato può avviare un'azione di risarcimento, perché egli può operare indifferentemente nei confronti del titolare del trattamento o del responsabile del trattamento.

Se poi questi due soggetti sono ubicati in paesi terzi, rispetto all'Unione europea, nessun problema: essi infatti hanno l'obbligo, se trattano dati di cittadini europei, di nominare un loro rappresentante in Europa che ne assume tutte le responsabilità.

Appare evidente il sensibile miglioramento del livello di protezione offerto agli interessati.

PARLIAMO ORA DI SANZIONI

Sotto questo aspetto, il regolamento generale applica appieno il concetto, purtroppo consolidato dall'esperienza, che afferma che tra il bastone e la carota, purtroppo il bastone è assai più efficace!

È ormai da un pezzo terminato il periodo di tolleranza, caldeggiato dal primo presidente dell'autorità Garante, Stefano Rodotà, che aveva motivato il suo approccio *soft* con la necessità che il titolare del

trattamento imparasse a leggere a comprendere le nuove disposizioni in tema di *privacy*.

Adesso si passa a un atteggiamento sanzionatorio assai più incisivo.

L'articolo 83, che stabilisce le condizioni generali per infliggere sanzioni amministrative pecuniarie (mai sanzioni penali, che devono essere oggetto di disposizioni legislative nazionali), sono ben articolate, perché vi è una prima fascia di sanzioni che arriva fino a 10.000.000 di euro oppure, per le imprese, fino al 2% del fatturato mondiale totale annuo, in corrispondenza della violazione di tutta una serie di articoli, puntualmente illustrati nel regolamento.

La sanzione amministrativa sale fino a 20.000.000 di euro o, rispettivamente per le imprese, fino al 4% del fatturato mondiale totale annuo, se vengono violati i principi base del trattamento, comprese le condizioni relative al consenso, i diritti degli interessati, o vengono trasferiti i dati personali a un destinatario in un paese terzo, senza rispettare le disposizioni del regolamento, nonché l'inosservanza di un ordine da parte dell'autorità di controllo nazionale.

Resta salva la facoltà degli Stati membri di stabilire eventuali altre sanzioni per violazioni, che non siano puntualmente elencate nell'articolo 83.

In armonia con il principio di coerenza, queste disposizioni nazionali devono essere notificate alla Commissione europea.

Anche se queste sanzioni possono sembrare estremamente

elevate, non dimentichiamo che la nostra stessa autorità Garante si è resa conto, nel corso degli anni, che solo sanzioni significative portavano a una modifica degli atteggiamenti dei titolari del trattamento.

È ormai noto il fatto che i grandi gestori dei servizi di telecomunicazione tengono costantemente sotto controllo il bilanciamento fra i profitti legati all'acquisizione di contratti di telefonia o simili, anche in violazione delle modalità di contatto con gli interessati, e le sanzioni applicabili dal Garante, per queste stesse violazioni.

Se il bilancio è a favore dell'aumento degli incassi, per i contratti di telefonia stipulati, si persegue nella violazione. Se invece la sanzione applicata dal Garante è veramente sostanziosa, le tecniche di *marketing* aggressive vengono abbandonate.

Come diceva il saggio, con le buone si impara, ma con le cattive si impara ancora di più e più in fretta!