Corso 196/03

a cura del Prof. Aristide Reginelli e dell'Ing. Arcangelo Pirozzi

Introduzione

Il legislatore, dopo sette anni di applicazione della cosiddetta "legge sulla privacy", la numero 675 del 1996, ha ritenuto opportuno riordinare in un testo unico, le norme vigenti in materia, articolandole in un sistema unitario che assume le caratteristiche di un codice, chiamato Codice Privacy, introdotto con il D. Lgs. del 30 giugno 2003 n. 196. Esso si configura come il primo intervento di codificazione organica della materia in questione. Non vuole solo essere un corpus unitario di articoli, ma vuole assurgere a valida guida per il cittadino che, nell'addentrarsi nel vasto campo delle regole, possa individuare l'itinerario da percorrere in una rapida ricognizione dei suoi diritti e doveri. Del resto, e tale concetto appare lampante, il diritto alla riservatezza, non può essere concepito nell'esclusivo significato del momento di isolamento del soggetto, come voleva la prima formulazione del diritto stesso fatta ai primi del '900, ma anche in adeguamento ad una direttiva comunitaria, deve tendere al contemperamento dell'esigenza di privacy, con l'esigenza che tali dati personali possano circolare, garantiti, e rendere partecipativo il soggetto stesso, contribuendo con ciò al benessere economico e sociale, allo sviluppo degli scambi, al benessere degli individui.

Rispetto al sistema previgente, numerose sono state le semplificazioni, ad esempio in materia di obbligo di notifica al Garante, che se in precedenza era generalizzato, oggi, al contrario ha carattere residuale, essendo obbligatorio solo in casi particolari, che in seguito approfondiremo. Analizzeremo la struttura del Codice Privacy, con riferimento particolare alle disposizioni inerenti alla nostra realtà, punteremo l'attenzione sulle pesanti sanzioni amministrative e penali previste dal legislatore per i casi di mancato rispetto delle norme in esame e fisseremo l'attenzione sul "famigerato" allegato B, ossia il disciplinare tecnico contenente le misure minime di sicurezza.

Percorso formativo responsabili/incaricati

Vi sono state consegnate in una alla lettera di incarico, le linee guida del trattamento dei dati che quotidianamente nello svolgimento della vostra professione affrontate. Nulla quaestio per i pre-requisiti, ma per quanto concerne gli obiettivi, faremo una panoramica sul sistema privacy, analizzando la normativa, anche e soprattutto analizzandone le ragioni ossia i motivi per i quali il legislatore ritiene così importante il bene "dato personale", vedremo quali sono i nostri obblighi in materia.

Unità 1 – Quadro normativo

Quando parliamo di "sistema privacy", facciamo riferimento ad un quadro normativo complesso che non comprende solo il Codice Privacy, ma che si intreccia fino a formare un tuttuno con le norme in materia penale in tema di criminalità informatica,

che hanno novellato il Codice Penale e con le misure minime di sicurezza rivisitate e meglio chiarite dal legislatore con il disciplinare tecnico (allegato B al Codice Privacy). L'applicazione corretta del sistema privacy, consente un'immediata risposta alle sollecitazioni esterne, ossia alla capacità del titolare del trattamento di rispondere entro i termini di legge alle richieste che vengono dall'interessato, in merito ai propri dati personali nell'esercizio dei diritti di cui agli artt. 7 e seguenti del Codice. Concetti che analizzeremo in seguito.
Perché è sorta l'esigenza di tutelare i dati personali dei soggetti? Quali sono i dati meritevoli di tale tutela? Chi sono i soggetti interessati ad ottenere tutela legale? Come tutelare i dati? Queste sono le domande a cui questo corso di formazione vuole dare risposta.
Cosa è la privacy? La risposta più immediata, sintetica e intuitiva è che la privacy è il diritto di essere lasciati in pace! Ma nella società attuale, in cui il bene informazione ha assunto una rilevanza economica non indifferente, è nata l'esigenza di contemperare il diritto alla riservatezza con l'esigenza della circolazione del bene informazione. Possiamo quindi affermare che la privacy consiste nel diritto alla auto determinazione informativa, in cui il soggetto decide con autonomia quando e con quali limiti far circolare informazioni che lo riguardano. Si noti che volontariamente parlo di "SOGGETTO" e non di individuo, utilizzando una accezione più generale. L'art 1 del D.lgs. 196/03 statuisce che "chiunque ha diritto alla protezione dei dati personali che lo riguardano", chiunque: dunque anche enti, persone giuridiche, associazioni. Fanno eccezione come è ovvio gli enti pubblici nello svolgimento delle proprie funzioni, la cui attività pubblica esclude per definizione che possa configurarsi l'esigenza di tutelare dati personali. Quale è la finalità del Codice Privacy? Quella di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali e della dignità dei soggetti interessati, che ottengono protezione per i propri dati personali. Il legislatore ha elevato dunque il diritto alla riservatezza al rango di un diritto della personalità con ciò adeguandosi al quadro normativo comunitario, che nella carta dei diritti fondamentali del cittadino europeo, non solo tutela la libertà dell'individuo, ma anche la protezione dei dati personali che lo riguardano, e il diritto di accedere agli stessi, in ogni momento, potendone chiedere la rettifica, la cancellazione ecc.
Ancora, parlando dei principi fondamentali del diritto alla riservatezza, meglio specificati con l'introduzione del codice privacy, rileviamo che l'art. 3, stabilisce che il trattamento dei dati personali deve essere improntato al principio di necessità e non eccedenza, per cui i sistemi informativi e i programmi informatici sin dalla loro configurazione devono garantire l'anonimato dei dati in essi raccolti e conservati, e la possibilità di collegarli all'interessato consentendone l'identificazione solo in caso di necessità. I dati raccolti non devono essere eccedenti le finalità della raccolta stessa, né a livello quantitativo, né a livello temporale essendone consentito il trattamento solo per il tempo necessario al trattamento stesso.
In parole povere, il legislatore in generale e semplificando il concetto al massimo, ha ritenuto opportuno, impedire che grazie ad una tecnologia sempre più avanzata, si possano creare enormi database di schedatura dei soggetti.

Il codice privacy, rappresenta una porta sempre aperta verso il futuro, poiché la protezione dei dati personali assume importanza crescente in relazione all'impetuoso emergere di nuovi settori, quali le innovazioni tecnologiche, che comportano l'intervento da parte delle istituzioni di garanzia, onde garantire uno sviluppo tecnologico sostenibile ed eticamente compatibile. E la validità delle istituzioni si misura anche attraverso la loro capacità di sincronizzarsi col futuro, nel senso però, appena accenato.

Dopo questi primi tre articoli portanti i principi generali dell'istituto privacy, il decreto in esame continua con le disposizioni a carattere generale, approfondisce le disposizioni a carattere particolare che fanno da eccezione o completamento alle prime per trattamenti particolari, si dedica poi alle sanzioni amministrative e penali per i casi di mancato rispetto della normativa de quo. Al Codice sono poi allegati i Codici di deontologia delle varie categorie professionali che trattano dati personali, approvati fin ora in base alle disposizioni del codice stesso, il disciplinare tecnico o allegato B in materia di misure minime di sicurezza, l'allegato C, che riguarda i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

In un mondo iper tecnologico, anche il legislatore penale ha dovuto adeguarsi: pertanto ha enumerato una serie di reati informatici, novellando il Codice Penale a partire dall'art. 615 bis, introducendo i concetti di reati informatici più specifici: essi vanno dall'intromissione non autorizzata in sistemi informatici o telematici, alla detenzione o diffusione di codici che consentono l'accesso ai sistemi di cui sopra, alla diffusione di programmi diretti al danneggiamento alla interruzione di sistemi informatici.
L'allegato B, in materia di misure minime di sicurezza sarà analizzato in seguito con dovizia di particolari, qui basti accennare al fatto che il legislatore ha previsto che siano poste in essere come misure di sicurezza (dei dati personali) misure idonee ossia in grado di tutelare il bene-dato, ma che per ritenersi al sicuro, ossia per sapere di aver fatto quanto necessario, per non incorrere nelle sanzioni, le misure minime da approntare per la sicurezza sono codificate e meglio chiarite in tale allegato.

Come accennato sopra, se il trattamento dei dati avviene con tali modalità, quindi nel rispetto della legge il sistema è in grado di reagire alle sollecitazioni esterne nei tempi sufficienti a garantire al soggetto interessato l'esercizio dei diritti relativi agli articoli 7 e segg. che consistono innanzi tutto nell'accesso ai propri dati, nel conoscere le finalità del trattamento, nell'opporsi in tutto o in parte a tale trattamento chiedendo la modifica, il blocco o, ove possibile, la cancellazione degli stessi. Qualora non si riuscisse ad ottemperare a tali richieste nel termine di 15 giorni, prolungabili di altri 15 se le operazioni necessarie sono complesse (art. 146), si corre il rischio che l'interessato proponga ricorso al Garante per far valere i propri diritti…! Il secondo obiettivo raggiunto consiste nel fatto di poter attuare una difesa più incisiva in un eventuale causa di risarcimento dei danni che ci venga perpetrata, producendo le

prove di aver ottemperato alle prescrizioni normative per essere scagionati (mi si passi il termine), come meglio si vedrà in seguito.

Progetto Privacy

A: Informative e consensi	B: Piano sicurezza informatico	C: Formazione
•Dipendenti •Clienti •Fornitori •Altro	•Rilevazione patrimonio informativo •Classificazione dati, hardware e software •*Stato dell'arte* •Linee guida •Formalizzazione dei ruoli •Analisi dei rischi •Misure minime •Misure Idonee •Notifica •DPS	•Titolare •Responsabile •Incaricato

Questo è lo schema che sintetizza il "progetto Privacy". Mostra quali sono i soggetti interessati dalle informative e consensi, quali sono i necessari adempimenti da porre in essere per la tutela della sicurezza informatica, a chi è rivolta la formazione, punto chiave del progetto anch'essa obbligatoria.

Panoramica D.lgs. 196/03

Figure coinvolte. Art. 4.

Titolare del trattamento è la persona fisica, giuridica, l'ente, la pubblica amministrazione, associazione od organismo, cui competono le decisioni, anche assieme ad altro titolare, in merito alle finalità, alle modalità del trattamento dei dati personali, e agli strumenti che sono utilizzati, anche in merito al profilo della sicurezza.

Responsabile è il soggetto (persona fisica giuridica ente ecc.) preposto dal titolare al trattamento dei dati, non è una figura obbligatoria.
Incaricati sono le persone fisiche autorizzate al trattamento dei dati dal titolare o dal responsabile.
Interessato è la persona fisica, giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
Garante è l'organo composto di quattro persone, due nominate dalla Camera due dal Senato, scelte tra esperti di informatica e di diritto, preposto a funzioni di vigilanza, intervento, tutela, consiliari, giudiziarie in materia di privacy. Vedi art. 153.

Trattamento e natura dei dati.
Il trattamento dei dati consiste in una qualunque operazione anche se effettuata senza l'ausilio di mezzi elettronici che può essere raccolta (ossia reperimento delle informazioni), registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, interconnessione, blocco cancellazione e distruzione (che fanno parte dei trattamenti evidentemente interni delle informazioni raccolte), raffronto, utilizzo, comunicazione, diffusione, cessione (trattamenti con l'esterno) dei dati stessi. Bisogna distinguere in primis tra raccolta di dati in senso generico, ad esempio durante una cena vengo a sapere che un amico è iscritto ad un partito politico (non ho quindi alcun obbligo), ma se tale informazione la registro onde renderla utilizzabile e in senso generico trattarla, sono soggetto alla legge privacy.
Natura dei dati.
Ma cosa sono questi dati personali che mi assoggettano o meno alla disciplina in esame? Per dato personale si intende una informazione su un soggetto (soggetto inteso nel senso ampio di cui sopra). A volte non è il dato in sé a caratterizzarsi come personale, ad esempio Abramo Levi nato il 10/10/10 non è un dato personale, ma se dico anche che è nato a Tel Aviv posso svelare una informazione generica circa la sua appartenenza ad un popolo e ad una fede religiosa.
Il Garante in un suo chiarimento ha stabilito che bisogna interpretare estensivamente il concetto di dato personale, utilizzando il massimo rigore e nell'incertezza si deve propendere per la soluzione positiva ossia che esso è un dato personale e quindi meritevole di tutela, anche le valutazioni di carattere soggettivo vanno interpretate come dato personale (valutazione sul grado di affidabilità di un soggetto per una banca o di un dipendente per il datore di lavoro). Altro esempio: il capo del personale di una fabbrica nelle notazioni personali su una dipendente scrive "bellissima", bene questa è una valutazione personale che nulla toglie e nulla mette, ma se a scriverlo è chi fa il casting delle modelle la situazione cambia notevolmente poiché è un giudizio che pur se personale è correlato all'attività professionale della ragazza. Raccolta di dati e quindi dati sono anche immagini e suoni: registrazioni video o registrazioni di telefonate ad esempio. Si pensi alle proposte di adesione ai contratti di operatori telefonici fatte in telemarketing: l'operatore del call-center, ci chiederà il consenso al

trattamento dei dati personali che raccoglierà attraverso una registrazione telefonica, dopo averci fornito l'informativa relativa al trattamento stesso.
Per essere personale l'informazione deve essere correlata ad un soggetto identificato o identificabile (in modo diretto o indiretto), quindi nell'ambito di applicazione della legge non rientrano i dati anonimi, cioè quelli che in origine o dopo essere stati trattati non sono comunque associabili al soggetto identificato o identificabile. L'8interessato, ha tra i suoi diritti (artt. Da 7 a 10), inoltre quello di rendere anonimi i propri dati.
Nell'ambito dei dati personali è possibile comunque stabilire in base alla loro diversa natura dei sottotipi: distinguiamo allora oltre ai dati personali, dati sensibili, dati giudiziari, dati che comportano rischi specifici (art. 17). Questi dati ricevono una particolare forma di tutela.

I dati sono detti sensibili quando sono idonei a rivelare lo stato di salute, le abitudini sessuali, l'origine razziale o etnica, la fede religiosa, le convinzioni filosofiche, l'appartenenza a partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. La legge è precisa: il dato per essere sensibile deve essere idoneo a rivelare etc. etc. quindi non esistono di per sé dati sensibili o meno, ma quello che li rende tali è l'uso che ne fa il titolare del trattamento. *(Ricordare l'esempio dell'associazione sindacale che ha chiesto il parere al Garante riguardo l'indirizziario, e quello della ginecologa alla trasmissione Forum sul caso della sterilità del marito e della gravidanza della moglie.)*
I dati giudiziari costituiscono invece una precisa elencazione a numero chiuso fatta dalla legge stessa, e non lasciano pertanto spazi a dubbi. Possiamo ricordare per esempio nell'ambito dei provvedimenti iscritti nel casellario giudiziale sono considerati dati "giudiziari" i provvedimenti penali di condanna definitivi, quelli concernenti le pene, le misure di sicurezza, gli effetti penali della condanna, la dichiarazione di abitualità o professionalità del reato, la tendenza a delinquere, i provvedimenti relativi a pene accessorie, le misure alternative alla detenzione etc. etc. La qualità di imputato o di indagato. Per l'elenco completo rinvio alla legge. L'art. 17 prevede una norma di chiusura: per tutti quei dati che sono diversi da quelli sensibili e giudiziari ma il cui trattamento presenta rischi specifici per il soggetto interessato il titolare deve preventivamente adire il Garante onde ottenere una verifica preventiva, ed in tale sede il Garante può dettare particolari accorgimenti per tale trattamento.

Qual'è l'ambito di applicazione del Codice Privacy? Esso si applica a chiunque è stabilito nel territorio dello Stato o nei luoghi soggetti alla sovranità nazionale, anche per i dati detenuti all'estero, a chiunque è stabilito nel territorio di un paese extra UE, per trattamenti effettuati con strumenti situati nel territorio dello stato italiano, salvo che tali strumenti siano utilizzati solo a fini di transito nel territorio della UE.

I diritti dell'interessato

Come in precedenza chiarito l'interessato è la persona fisica, giuridica, l'ente o l'associazione cui si riferiscono i dati. L'interessato è dunque il garante di se stesso.
In primis ha il diritto di accesso ai suoi dati: ottenere la conferma dell'esistenza o meno di dati che lo riguardano, pur se ancora non registrati e ha diritto di ottenerne comunicazione in forma chiara; l'interessato ha diritto altresì di ottenere informazioni circa l'origine dei dati personali, delle finalità e modalità del trattamento, di come vengono trattati in caso di utilizzo di strumenti elettronici, degli estremi relativi al titolare al responsabile all'eventuale rappresentante, dei soggetti o categorie di soggetti a cui i dati possono essere comunicati. Può ottenere l'aggiornamento, la rettifica o l'integrazione dei dati, la cancellazione, trasformazione in forma anonima o il blocco dei dati, può ottenere certificazione che tali operazioni sono state comunicate a coloro i quali hanno ottenuto la comunicazione o diffusione dei dati. Può opporsi al trattamento dei dati che lo riguardano per legittimi motivi, o al trattamento ai fini di invio di materiale pubblicitario, vendita diretta o comunicazione commerciale.
La richiesta di accesso non può però essere reiterata prima che siano decorsi 90 giorni dalla prima, e qualora non risultino dati inerenti l'interessato a costui può essere richiesto un rimborso spese in misura però non eccedente i 10,33 €: la ratio voleva essere la prevenzione di abusi da parte dell'interessato, si pensi ad un disturbatore che decide di bersagliare un'azienda o un ente…
Il titolare del trattamento deve essere comunque pronto a fornire le informazione richieste nel termine di 15 giorni, prorogabili dietro motivazione per altri 15 giorni qualora la ricerca o l'estrazione siano complicate, in caso contrario l'interessato può proporre ricorso al Garante. (E' questa la capacità reattiva del sistema alle sollecitazioni esterne osservata in precedenza). Le informazioni vanno rese in forma intelligibile e devono essere complete, comprese ad esempio eventuali registrazioni televisive o audio, qualora esse debbano essere registrate su supporti particolari, o la loro estrazione abbia richiesto notevole impiego di mezzi in relazione alla complessità delle richieste, il Garante ha previsto che il titolare possa richiedere un contributo spese. La richiesta da parte dell'interessato è posta al titolare o al responsabile del trattamento, senza particolari formalità, può anche essere delegata mediante conferimento di una semplice procura sia a persone fisiche sia ad enti od associazioni etc., ma non può riguardare tutti i tipi di dati: l'art. 8 difatti enuclea una serie di casi in cui i diritti di cui all'art. 7 non sono esercitabili (ad esempio in materia di riciclaggio o in caso di contenzioso aperto tra le due parti).

Lasciamo un attimo in sospeso il trattamento dei dati particolari, ossia i sensibili e i giudiziari, che andiamo ad approfondire successivamente, e sorvoliamo per ora anche sulle sanzioni amministrative e penali. Ci dedichiamo alla parte applicativa: come si trattano i dati comuni in generale.

Modalità del trattamento

Il principio di fondo nel trattamento dei dati personali è quello della correttezza, riconducibile al concetto di trasparenza. Chiunque tratti dati personali di altri soggetti deve essere ispirato dalla "buona educazione", deve effettuare un trattamento leale, lecito, ossia non contrario a norme imperative, all'ordine pubblico o al buon costume. Il principio della finalità: attiene i motivi per cui si trattano i dati. Raccolta e registrazione devono avvenire per fini determinati, espliciti e legittimi. Il trattamento non deve essere eccedente riguardo la pertinenza dei dati ai fini del trattamento stesso. I dati difatti non devono essere eccedenti né da un punto di vista quantitativo, né da un punto di vista temporale rispetto a quello necessario agli scopi per cui i dati sono stati raccolti o trattati. I dati devono essere esatti ed aggiornati (si consideri una banca dati sulla solvibilità). Il trattamento deve essere inoltre necessario: abbiamo visto sopra che l'art. 3 stabilisce il principio della necessità del trattamento onde evitare schedature in enormi database. I dati personali trattati in violazione di tali principi non possono essere utilizzati, il Garante può ordinarne il blocco fino alla regolarizzazione della posizione del titolare al riguardo, o la cancellazione nel caso limite in cui essa non sia possibile.

Informativa

Il primo adempimento di ordine pratico imposto a chiunque tratti dati personali, è di informare il soggetto interessato che si raccolgono e trattano dati sul suo conto, essa va resa però anche alla persona da cui si raccolgono i dati, qualora fosse diversa dall'interessato stesso. Deve essere comunque sempre antecedente la raccolta dei dati.

L'informativa resa al soggetto interessato.

Viene resa sia nel caso in cui si intenda procedere alla raccolta dei dati, sia quando, avendo già a disposizione tali dati, si intenda effettuare una diversa operazione di trattamento. Ovviamente la si può rendere una sola volta se essa è completa altresì di tali evenienze. Deve contenere: finalità e modalità del trattamento, natura obbligatoria o facoltativa del conferimento dei dati, conseguenze di un eventuale rifiuto di rispondere, la filiera del trattamento dei dati in questione (chi li tratta, a chi vengono comunicati etc.), i diritti dell'interessato, estremi identificativi del titolare, del responsabile, del rappresentante in Italia, se si tratta di dati sensibili, i soggetti pubblici fanno riferimento alla normativa particolare che li riguarda. Può essere fornita oralmente o per iscritto, ma è assolutamente necessario che essa sia antecedente alla raccolta. Il Garante, in senso estensivo ha chiarito che l'informativa deve essere resa anche nel caso di cessazione del trattamento.

Consenso

Il consenso è strettamente necessario per il trattamento dei dati, che sia essi comuni o sensibili, da parte di privati ed enti pubblici economici. Il consenso dell'interessato deve essere espresso, quindi non implicito, deve essere libero, quindi frutto della libera manifestazione della volontà del soggetto e non frutto di errore, violenza o dolo; deve essere specifico ossia riferirsi ad un preciso genere di trattamento chiaramente individuato, a cura di un ben determinato titolare, deve essere documentato per iscritto, può essere totale o parziale. Il Garante ammette anche il consenso per conto di terzi.

Non è sempre necessario ottenere il consenso per il trattamento dei dati: l'art. 24 stabilisce che esso non è necessario per adempiere ad un obbligo legale, comunitario o di regolamento, per eseguire obblighi derivanti da contratto nel quale è parte l'interessato, o per adempiere, prima della conclusione dello stesso a specifiche richieste dell'interessato, riguarda dati "pubblici", riguarda dati relativi allo svolgimento di attività economiche, pur nel rispetto delle norme in materia di segreto aziendale e industriale, è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo o dell'interessato, è necessario per lo svolgimento di attività di investigazione, per perseguire un interesse legittimo dell'interessato, è effettuato per scopi statistici o storici, nel rispetto dei codici di deontologia. Inoltre i soggetti pubblici, ad eccezione degli esercenti professioni sanitarie, non devono richiedere il consenso (resta fermo l'obbligo dell'informativa).

Risulta chiaro che informativa e consenso viaggiano insieme: **il consenso validamente prestato è di certo frutto di una attenta e precisa informativa resa all'interessato.**

Specifiche regole per i soggetti pubblici.

(Parte specifica per ogni singolo titolare interessato da cambiare di volta in volta).

L'art. 18 prevede come anticipato, che per i soggetti pubblici non è obbligatorio richiedere il consenso dell'interessato, fatta eccezione per gli esercenti le professioni sanitarie, questa regola è da porre in relazione con il fatto che le funzioni svolte dal soggetto sono di pubblica utilità.

Altra regola fondamentale è che è consentito solo il trattamento per le funzioni istituzionali proprie dello specifico soggetto pubblico.

La diffusione e la comunicazione dei dati sono vietate, qualunque sia la natura dei dati trattati quando: è stato vietato dall'autorità giudiziaria o dal Garante; in riferimento ai dati per i quali è stata ordinata la cancellazione o quando è decorso il tempo entro cui è lecito conservare i dati; per finalità diverse da quelle indicate nella notificazione del trattamento al Garante, se il soggetto è tenuto a tale adempimento.

Trova applicazione le deroghe previste, per le quali è fatta salva la possibilità di procedere alla comunicazione o alla diffusione dei dati in conformità a prescrizioni di legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza, o altri soggetti pubblici impegnati nella difesa o sicurezza dello Stato, prevenzione, accertamento o repressione di reati.

Per i dati di natura comune, il trattamento è consentito solo per fini istituzionali.
Nell'ambito di tale contesto, attività diverse dalla diffusione e/o comunicazione, sono consentita anche se non espressamente prevista da una norma di legge o da un regolamento; attività di comunicazione ad altri soggetti pubblici, se non espressamente previste da leggi o regolamenti, rendono necessaria una previa comunicazione al Garante e decorsi 45 giorni dalla stessa, può essere iniziato il trattamento sia che il Garante abbia risposto sia che abbia taciuto, si applica quindi la regola del silenzio – assenso; attività di comunicazione a privati o enti pubblici economici, è ammessa solo quando espressamente prevista da leggi o regolamenti; così pure la diffusione.
Per quanto concerne il trattamento di dati sensibili e giudiziari, esso è consentito solo se autorizzato da disposizione di legge espressa, nella quale siano specificati tutti i tipi di dati che possono essere trattati, con le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
Nel caso in cui la disposizione di legge manchi, il soggetto pubblico può interpellare il Garante onde ottenere l'autorizzazione al trattamento. Se al contrario esiste una disposizione di legge che prevede il trattamento senza però specificare il tipo di dati da trattare e le operazioni di trattamento eseguibili, il soggetto pubblico deve individuare e rendere pubblici con atto di natura regolamentare adottato richiedendo il parere del Garante quali tipi di dati possono essere trattati e le operazioni di trattamento che intende porre in essere, tale individuazione deve essere aggiornata ed integrata periodicamente.
A tale scopo il Garante ha pubblicato i Regolamenti sul trattamento dei dati sensibili da parte della Pubblica Amministrazione, nel quale ribadisce che i soggetti pubblici che operano senza tale presupposto regolamentare operano senza un presupposto di liceità.
L'art. 22 stabilisce come i dati sensibili e giudiziari debbano essere trattati: i dati sono quelli strettamente indispensabili ai fini istituzionali che non possono essere perseguiti mediante uso di dati anonimi o diversi da quelli sensibili o giudiziari. Di tali dati, comunque la P.A. è tenuta a verificare l'esattezza e l'aggiornamento periodicamente, in una alla loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite.
Come si nota è particolarmente incisiva la protezione di tali dati quando sono trattati dall'ente pubblico, protezione che si rivela anche nel sistema di raccolta dei dati, nell'informativa, nella custodia dei dati stessi, nelle limitazioni particolari imposte nell'uso degli stessi.

Adempimenti

I fondamentali adempimenti da porre in essere da parte dei soggetti che intendono effettuare trattamento dei dati personali ai sensi del d. lgs. 196/03 consistono nella notificazione al Garante, nell'obbligo di comunicazione, nella necessità di ottenere una autorizzazione. Alla luce della nuova stesura della legge privacy tali

adempimenti che in precedenza erano pressoché generalizzati, oggi assumono carattere residuale.
La notificazione al Garante, art. 37, difatti ha subito un drastico ridimensionamento, essa è obbligatoria quando si intende porre in essere trattamenti che riguardano:
dati genetici o biometrici,
dati relativi all'ubicazione geografica di persone attraverso una rete di comunicazione elettronica,
dati idonei a rivelare salute e/o vita sessuale delle persone ai fini di procreazione assistita, prestazione di servizi sanitari in via telematica relativi a banche dati o alla fornitura di beni, oppure relativi ad indagini epidemiologiche, o su malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti, monitoraggio della spesa sanitaria,
dati idonei a rivelare salute e/o vita sessuale delle persone trattati da associazioni varie, anche non riconosciute,
dati trattati con l'ausilio di banche mezzi elettronici volti a definire il profilo o la personalità dell'interessato,
dati trattati come sopra ai fini propagandistici o pubblicitari, ricerche di mercato etc.
dati volti a monitorare l'uso dei mezzi di comunicazione elettronica,
dati relativi alla tenuta di banche dati ai fini di ricerca del personale per conto terzi,
dati detenuti nelle cosiddette centrali rischi.
Il Garante ha facoltà di modificare tale elencazione in base alle eventuali nuove esigenze che dovessero sorgere. Tutte le notificazioni pervenute al Garante sono inserite nel registro dei trattamenti. Esse vengono presentate prima dell'inizio del trattamento stesso, una sola volta a prescindere dal numero delle operazioni che si pongono in essere sui dati stessi, e sono validamente presentate solo se spedite in via telematica attraverso il modello predisposto dallo stesso Garante, osservando le istruzioni da questo impartite, essa deve comunque indicare tutti gli elementi necessari alla individuazione del titolare, dei responsabili, dei trattamenti, delle finalità, delle modalità, della natura dei dati, della comunicazione o diffusione degli stessi, ed ancora una sommaria descrizione delle misure di sicurezza approntate per la salvaguardia dei dati stessi. La notifica va ripetuta solo prima della cessazione del trattamento o al mutare di uno degli elementi contenuti nella notifica stessa e che sono oggetto appunto di notificazione.
L'obbligo di comunicazione preventiva, art. 38, riguarda i soggetti pubblici che intendono effettuare trattamenti di dati ai fini della comunicazione ad altro soggetto pubblico di dati comuni, qualora tale attività non sia prevista da una norma di legge o regolamento; trattamento di dati idonei a rivelare lo stato di salute che rientri in un programma di ricerca biomedica. Il Garante, anche per l'obbligo di comunicazione preventiva può individuare altre fattispecie. La comunicazione è inoltrata utilizzando il modello predisposto e reso disponibile dal Garante, viene trasmessa o in via telematica, o via telefax, o mediante lettera raccomandata. Anche qui vige la regola del silenzio assenso, per cui in caso di mancata risposta del Garante dopo i 45 giorni dalla ricezione della comunicazione il trattamento può essere iniziato.

Le autorizzazioni generali, previste dall'art 40, sono il frutto dell'esperienza di questi anni. Il Garante rilascia autorizzazioni generali al trattamento dei dati non ad un singolo titolare ma bensì ad una categoria di titolari. Sino ad oggi ne sono state rilasciate sette: a mo di esempio ricordiamo la aut. 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro; la numero 4/2002 al trattamento dei dati da parte dei liberi professionisti; la numero 6/2002 al trattamento dei dati sensibili da parte degli investigatori privati. La regola è che se il trattamento che si intende porre in essere rientra nell'ambito di una autorizzazione generale rilasciata non vi è obbligo di richiederla nuovamente, a meno che il trattamento differisca in alcuni elementi sostanziali o abbia delle modalità specifiche particolari. Per i casi che non sono ricoperti da autorizzazione generale, il soggetto che intende trattare i dati deve richiedere l'autorizzazione (attraverso il modello predisposto dal Garante). Al momento della richiesta il Garante istruisce la pratica, può richiedere informazioni e chiarimenti, poi si pronuncia: se non si pronuncia nei 45 giorni il silenzio stavolta vale come rigetto della domanda.

Profili di responsabilità e sanzioni.

Prima di affrontare la parte pratica di questo corso, è opportuno soffermarci sui profili di responsabilità civile, amministrativa e penale, derivanti dal mancato rispetta del sistema privacy e dei precetti di sicurezza in esso contenuti.
Ad una prima occhiata ci si rende subito conto che il legislatore ci è andato giù pesante, andiamo a capire perché.
In primo luogo all'art. 15 del Codice ha stabilito che il profilo di responsabilità civile in cui incorre chi provoca un danno ad altri per effetto del trattamento dei dati personali è quello risultante dal combinato disposto di detto articolo con l'art. 2050 c.c., il quale è rubricato "Responsabilità per l'esercizio di attività pericolose", ed impone il risarcimento del danno se sono si prova di aver fatto tutto il possibile per evitare il danno stesso (con l'adozione di misure idonee). Inoltre, vi è obbligo di risarcimento anche dei danni non patrimoniali. La norma punisce "chiunque" cagiona ad altri un danno, quindi titolare, responsabili, incaricati, chi tratta dati senza autorizzazione (qui sfociamo addirittura nel penale!). Il titolare del trattamento dovrà provare onde difendersi di aver fatto tutto il possibile per evitare il danno (inversione dell'onere della prova), ossia di aver adottato tutte le misure idonee, non solo, ma tutte le misure idonee offerte dalla tecnica allo stato attuale del momento in cui si verifica il danno. Per i trattamenti di cui all'art. 11, *modalità del trattamento e requisiti dei dati personali*, è prevista anche la risarcibilità del danno non patrimoniale, sofferto dal soggetto interessato.

Al di la del risarcimento danni patrimoniali e personali come sopra delineato, la legislazione privacy ha previsto tre ordini di sanzioni: quelle amministrative, quelle penali e quelle cosiddette indirette.
Osserviamole brevemente. Le violazioni amministrative consistono

nella omessa o inidonea informativa all'interessato, che prevede una variabilità nell'entità delle sanzioni, che vanno per i dati comuni da 3000 a 18000 €, che viene elevata per eventuali pregiudizi arrecati per effetto del trattamento da 5000 a 30000 €, stesse cifre previste nel caso di trattamenti di dati sensibili, giudiziari o particolari, anche se non vi è stato pregiudizio alcuno, ed infine, tali somme, qualora la situazione patrimoniale del contravventore sia tale da renderle esigue, possono essere aumentate sino al triplo;
nella cessione di dati ad altro titolare in violazione del principio di compatibilità dei trattamenti, la sanzione va dai 5000 ai 30000 €, qualora la violazione riguardi gli esercenti la professione sanitaria, che devono rendere noti i dati relativi all'interessato solo tramite altro medico o similare, la sanzione va dai 500 ai 3000 €;
nella omessa o incompleta notificazione, per cui chiunque essendovi tenuto non la effettua, o la effettua in modo incompleto, è punito con una sanzione che va da 10000 a 30000 €, oltre alla sanzione accessoria della pubblicazione della ordinanza in uno o più giornali;
nella omessa informazione o esibizione al Garante (di documenti richiesti dallo stesso), in tale caso il contravventore paga una sanzione da 4000 a 24000 €.
E' sempre prevista la possibilità della sanzione accessoria della pubblicazione dell'ordinanza ingiunzione sulle testate giornalistiche.

Illeciti penali.
Trattamento illecito di dati: evitando di scendere nell'elencazione completa che l'art. 167 riporta, al quale rimando per comodità, la norma in questione stabilisce che salvo che il fatto non costituisca più grave reato, chiunque al fine di trarre un profitto per sé o per altri, procede al trattamento illecito di dati è punito con la reclusione da 6 a 18 mesi, o se si tratta di comunicazione o diffusione da 6 a 24 mesi; le violazioni più gravi, sono punite con la reclusione da 1 a 3 anni.
Falsità nelle dichiarazioni e notificazioni al Garante: il reo è punito con la reclusione da 6 mesi a tre anni, salvo che il fatto costituisca un più grave reato.
Misure di sicurezza: chiunque essendovi tenuto, omette di adottare le misure minime di sicurezza, è punito l'arresto sino a due anni o con l'ammenda da 10000 a 24000 €.
L'autore di tale reato, all'atto dell'accertamento o successivamente con provvedimento del Garante, può essere posto nella condizione entro 6 mesi di adeguarsi alle misure minime, se l'adeguamento ha luogo esso in una al pagamento della sanzione di un quarto del massimo dell'ammenda stabilita per la contravvenzione, estingue il reato.
Inosservanza dei provvedimenti del Garante: reclusione da tre mesi a due anni.
Altre fattispecie: il legislatore si è richiamato alle violazioni comprese nello Statuto dei Lavoratori, al quale per comodità rinvio.
C'è sempre la pena accessoria della pubblicazione della sentenza per i reati previsti dal codice privacy.

UNITA' DIDATTICA 2

Ora che siamo abbastanza edotti su cosa ci può accadere se non rispettiamo le prescrizioni del Codice in esame, possiamo passare all'analisi delle misure di sicurezza.

Misure di sicurezza

Il Codice Privacy impone le misure di sicurezza la cui violazione abbiamo visto essere sanzionata addirittura come reato, quindi dalla legislazione penale. L'art. 31 disciplina le misure che sono comunemente indicate come idonee, esse sono da adottare in via preventiva onde ridurre al minimo i rischi di distruzione o perdita anche accidentali di dati, accesso non autorizzato ai dati, trattamento non consentito o non conforme alle finalità della raccolta. La sicurezza dei dati non deve essere intesa solo come riduzione del rischio di cui sopra, ma anche come limitazione degli effetti negativi causati dal verificarsi di eventi "traumatici" che abbiano ad oggetto i dati.
Come è ovvio esse vanno aggiornate costantemente onde tenerle al passo con l'evoluzione tecnologica.
Il legislatore non si ferma qui, difatti all'art. 33 codifica le misure minime di sicurezza, al di sotto delle quali non è assolutamente possibile scendere….L'allegato B al Codice Privacy, anche definito disciplinare tecnico, delinea meglio specificandole e soprattutto concretizzandole, le misure minime da adottare. Esse sono definite come il complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dal'articolo 31.
Con l'aiuto dei soliti slides, addentriamoci nel dedalo delle misure di sicurezza.

Le risorse dell'azienda sono: i dati, le informazioni, la manualistica, gli utenti, le apparecchiature elettroniche, i programmi.

Gli obiettivi fondamentali della sicurezza delle risorse, quindi sono la loro disponibilità, la loro riservatezza, la loro integrità. i servizi devono essere preservati nel loro stato, nella loro capacità di soddisfare le esigenze dell'utente, in termini di durata, di tempo di risposta, di priorità di tolleranza alla degradazione. Chiunque non sia autorizzato ad usufruire degli stessi, assolutamente non avrà diritto di accesso. Le risorse devono essere protette dalla distruzione, dall'alterazione e dall'uso non autorizzato.

Anche questi slides si commentano da soli. Mi preme solo chiarire che maggiore è il danno prodotto da una minaccia alla risorsa da tutelare maggiore è il valore della risorsa stessa. Per dirla al positivo il valore di una risorsa è facilmente intuibile e calcolabile in base al danno che un'eventuale minaccia, sia essa volontaria o involontaria, può provocare.

Ed ecco quindi un elenco che non ha la presunzione di essere esaustivo, delle minacce volontarie o involontarie che occorrono alle nostre risorse.

In base dunque al valore della risorsa e al danno che si verificherebbe se essa venisse "attaccata", calcoliamo il cosiddetto Fattore di Rischio, la cui conoscenza è fondamentale per poter implementare le giuste misure di sicurezza, o per meglio dire, l'analisi dei rischi ci aiuta a definire il controllo degli stessi e a porre le necessarie barriere di protezione alle nostre preziose risorse.
Il decreto 196/03 la fa breve: i rischi possono consistere nella distruzione o perdita anche accidentale dei dati, nell'accesso non autorizzato o nel trattamento non consentito o non conforme dei dati. Di certo nel panorama vastissimo dei rischi cui è sottoposto un sistema complesso di risorse, questi sono i più frequenti.

È pertanto necessario, adottare contromisure tecniche e non tecniche di protezione. Le prime sono proprie del sistema informatico, le seconde sono propriamente fisiche e procedurali, riguardano inoltre il personale.
Altra distinzione possibile tra le misure di sicurezza è mostrata da questo slide: esse sono misure di prevenzione atte cioè a prevenire il danno, misure di contenimento e/o riduzione dello stesso, misure di trasferimento del danno, proprie dei contratti assicurativi, esse aiutano l'azienda a non sopportare tutto il peso di un risarcimento ma non aiutano a prevenire il danno stesso, né pongono rimedio alcuno.

Analizziamo le misure di sicurezza dei centri di elaborazione. Rifacendoci alla distinzione di cui sopra, possiamo dividerle in misure di sicurezza fisiche, elettroniche e procedurali.
Nel primo gruppo introduciamo tutte le misure di tipo fisico, ossia quelle che impediscono o rallentano fisicamente il verificarsi di un sinistro: porte blindate, vetri stratificati, inferriate, armadi ignifughi (o al contrario antiallagamento) con serratura, sistemi di spegnimento di incendi ecc.
Le difese elettroniche che non possono impedire ma solo rilevare e segnalare il verificarsi di un sinistro sono ad esempio impianti antifurto, impianti di rilevazione degli incendi, impianti di videoregistrazione a circuito chiuso…
Le difese di tipo procedurale, infine, hanno il compito di garantire la corretta funzionalità delle difese esaminate or ora, e consistono nelle procedure per l'attivazione delle difese, per il controllo delle stesse, per il loro ripristino in caso di anomalia, procedure per l'intervento in caso di sinistro.
È essenziale per una perfetta protezione del centro elaborazione, che le misure di sicurezza siano molto impattanti: ciò vuol dire che il tempo di reazione della misura di sicurezza deve essere molto minore rispetto al tempo di penetrazione (da parte del "sinistro") delle nostre difese. Un esempio pratico: un buon impianto antincendio segnalerà lo stesso alla primo filo di fumo che colpisca i sensori, anche qualora dovesse essere un falso allarme! Ciò valga per tutte le misure analizzate finora.

Quanto sinora detto vale naturalmente per la protezione esterna dell'ambiente in cui si trova il centro di elaborazione, ma è naturale che lo stesso debba essere protetto anche da tutta una serie di misure di sicurezza informatica, di hardware e software che ne garantiscano l'incolumità.
Osserviamo l'elencazione esemplificativa delle stesse ed analizziamole una per volta. Ricordiamo sempre che per legge le misure minime devono essere predisposte, pena sanzioni penali ed amministrative molto pesanti.
IDENTIFICAZIONE.
Essa consente al sistema di individuare l'utente che sta richiedendo l'accesso allo stesso. Normalmente, nei casi più semplici, consiste in un nome utente o user name, che viene richiesto all'ingresso del sistema stesso, o all'ingresso di quella parte di sistema nel quale è possibile l'accesso. Il codice utente, consente non solo di attribuire la responsabilità delle azioni all'utente stesso, ma anche di stabilire i cosiddetti privilegi di accesso. La legge prescrive che esso possa essere utilizzato dallo stesso utente nel tempo, ma non possa essere trasmesso da un utente all'altro (ad esempio se il dipendente X viene trasferito da un reparto all'altro, non potrà cedere il suo codice utente a colui il quale andrà a sostituirlo.
AUTENTICAZIONE
Una volta identificato l'utente che chiede l'accesso al file interessato dalla misura di sicurezza, è necessario provvedere alla sua identificazione. Essa, normalmente, avviene attraverso l'uso di password segrete con specifiche caratteristiche che le rendono sicure, e che vengono introdotte all'atto dell'accesso. Le password devono essere abbastanza lunghe, almeno otto caratteri, o comunque il massimo dei caratteri che il programma in questione può supportare. Ovviamente non devono essere relative a dati facilmente intuibili come il nome del marito o della moglie, le date di nascita o nomi di personaggi famosi, reali o inventati (Paperino, Pippo Baudo ecc.). ancora un quarto o la metà dei caratteri devono essere numerici, introducendo ad esempio la @ al posto di una a ecc. insomma seguire accorgimenti atti a rendere particolarmente difficile se non impossibile intuire e decifrare la nostra chiave di accesso personale. Le linee guida presentano una tabella relativa alle caratteristiche delle password, in base al grado di rischio presentato dalle risorse. Ancora le password devono essere modificate all'atto della ricezione ed ogni sei mesi, mentre per quelle aree di accesso che contengono dati sensibili o giudiziari il termine è di tre mesi. Di certo è intuibile che la password personale non deve essere lasciata in giro, magari su un post-it accanto allo schermo del pc! Se inutilizzate per sei mesi, o alla perdita di qualità dell'incaricato le credenziali di autenticazione sono disattivate.
Qualora l'accesso ai dati e strumenti elettronici sia consentito solo attraverso l'utilizzo delle credenziali di autenticazione, in caso di assenza prolungata o impedimento dell'incaricato, se l'intervento è indifferibile ed è in gioco la sicurezza del sistema, se ricorrono tutte queste caratteristiche contestualmente il titolare deve aver preso le opportune misure affinché si possa intervenire. Ossia deve aver impartito istruzioni scritte agli incaricati affinché essi: predispongano una copia della parola chiave, provvedendo quindi a trascriverla, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e,

possibilmente, sigillata);
consegnino tale copia ad un soggetto incaricato della sua custodia preventivamente (l'incaricato della custodia delle parole chiave); in caso di necessità come sopra chiarito, si interviene e dell'intervento è data immediata notizia all'incaricato.

VIRUS INFORMATICI

I virus sono programmi scritti per danneggiare un computer o una rete, i dati in esso contenuti, o i programmi che lo compongono, l'interruzione totale o parziale o il loro rallentamento. Il nostro sistema penale, ha codificato i reati informatici, e tra essi ci sono anche gli attacchi con virus (art. 615quinquies e segg. c.p.). Essi non sono tutti seri o distruttivi, ma la percentuale di attacchi informatici con virus è molto alta. Si rende dunque necessario proteggere il computer dal "codice maligno", e renderlo poi in grado di riparare i danni eventuali portati da un attacco del genere.
Come è possibile "prendere un virus"? Quali sono i fattori di rischio per un sistema?
Diamo un'occhiata agli slides. Riutilizzo di dischetti, uso di programmi prelevati da internet o da riviste, uso di floppy preformattati, collegamenti a siti della rete nei quali il client è sottoposto al rischio di contaminazione poiché ad esempio il browser esegue il virus sulla sua pagina web, prelievo di file, ricezione di applicazioni dall'esterno, utilizzo del pc da più persone, collegamento in internet ed applicazione degli applets java, esecuzione di file attached della posta elettronica. L'enumerazione è solo esemplificativa e non esaustiva.
Quali sono dunque i comportamenti da tenere per tentare di evitare l'attacco del virus?

NORME DI COMPORTAMENTO

Bisogna possedere un programma antivirus che sottoponga a scansione i vari supporti utilizzati; prima di aprire un file o eseguire un'applicazione contenuti in un supporto esterno, bisognerebbe controllarlo; non utilizzare il proprio disco sistema su un pc diverso se non è protetto in scrittura; proteggere in scrittura tutti i propri floppy; non avviare da floppy un sistema basato su hard disk, se il disco non è sicuramente pulito; limitare la trasmissione di file eseguibili e di sistema; non utilizzare il server come pc di lavoro; non modificare mai i floppy di programmi originali.
Di conseguenza le regole operative sono facilmente spiegate: osserviamo gli slides….

SINTOMI DI INFEZIONE

Ma come si fa a riconoscere un virus? Dai sintomi del pc! Come un medico ci diagnostica la malattia in base ai sintomi, così osservando il comportamento anomalo del nostro pc possiamo renderci conto se siamo stati attaccati da un virus, e prima lo facciamo maggiori sono le probabilità di limitare i danni.
Quali sono i sintomi: ad esempio una riduzione dello spazio su disco rigido, la tastiera che produce suoni strani, i programmi che impiegano più tempo a caricarsi, i

file che appaiono e scompaiono, o cambiano nome, le unità disco sono spesso in attività o inaccessibili, appaiono oggetti o testi inusuali sullo schermo: e tutto quello che la fantasia malata di questi programmatori riesce a concepire.

DIFESA INFORMATICA PREVENTIVA

Le misure minime di sicurezza, in materia di antivirus e firewall, sono probabilmente troppo ottimiste. La legge prescrive che l'aggiornamento di tali programmi sia annuale, ma qualora si tratti di dati sensibili o giudiziari, avvenga con cadenza semestrale. Chiunque conosca la mola dei virus che circola e abbia un minimo di dimestichezza con internet, tanto per fare un esempi, sa che l'aggiornamento dell'antivirus è almeno quindicinale!

Così come per ciò che riguarda il back up dei dati, la legge prescrive che sia settimanale, ma sappiamo che se fosse giornaliero sarebbe decisamente più sicuro.

Analizziamo il firewall: letteralmente il muro di fuoco, ossia una barriera insormontabile che blocca l'accesso ad un qualcosa. L'obiettivo del firewall è quello di proteggere una rete da un'altra con la quale comunica che sia esterna o una parte della stessa rete interna privata, consentendo comunque lo scambio di traffico tra le due. Esso determina se un pacchetto di dati o una richiesta di connessione di un utente alla nostra rete abbiano o meno il diritto di passare. Sono di due tipi, quelli software, che sono economici ma penalizzano le caratteristiche della rete, o hardware, che al contrario impongono una notevole spesa, ma non penalizzano le prestazioni della rete, possono essere anche concepiti come una combinazione di uno o più computer, software e networking. L'ente che certifica la validità di un prodotto firewall è l'ICSA che ha tra l'altro individuato tre tipi di firewall.

1) **Packet filtering** che consiste nel porre tra le reti i router che filtrano i pacchetti di dati e consentono il passaggio solo a quelli con indirizzi IP o dati contenuti nella testata del messaggio che sono stati autorizzati diciamo legalizzati da chi ha impostato il firewall ossia l'amministratore di rete, ma la garanzia di tale firewall è labile poiché un host è in grado di cambiare un indirizzo IP, trasformarlo in uno consentito ed accedere alla rete indisturbato.
2) **Application gateway**, esso intercetta il traffico ed autentica gli utenti. Un utente privato accede a questo proxy, viene autenticato, e così avrà accesso al server remoto che si trova sulla rete esterna. Sarà necessario predisporre un proxy per ogni applicazione. Tutti gli host della rete interna presenteranno l'indirizzo del proxy, nascondendo così i loro indirizzi sulla rete esterna.
3) **Packet Inspection**, a differenza degli altri, questo firewall presenta maggiori garanzie, poiché esso analizza non solo l'indirizzo IP ma il contenuto del pacchetto stesso che sta tentando di entrare e scambiare traffico con la nostra rete.

I firewall in commercio comunque sono vari e disparati, essi combinano più tecniche e visto che nulla possono contro i virus, oggi i produttori inseriscono in essi anche programmi antivirali, che combinano le due cose e rendono maggiormente sicura la nostra rete.

È opportuno sapere che esistono i cosiddetti IDS ossia Intrusion Detection Sistem, strumenti evoluti che consentono riconoscere gli attacchi attraverso il monitoraggio, rilevamento e prevenzione della violazione in tempo reale.

Dei back up abbiamo parlato in precedenza, aiutiamoci con lo slide e notiamo che non è solo necessario effettuare il back up, ma anche poi conservare questi supporti, verificarne la validità ecc. un buon sistema di back up consente di recuperare tutti i dati persi al momento del disastro e riportare il sistema allo stesso stato in cui si trovava.

GRUPPI DI CONTINUITA'
Guardiamo lo slide.

AUDITING
Consente di controllare gli accessi al sistema e alle risorse permettendo altresì di attribuire la responsabilità delle operazioni effettuate agli operatori. Un *audit trail* è un metodo automatico per registrare tutte le transazioni che si verificano su una rete, e gli eventi che si verificano in un sistema. Consente, pertanto, di individuare attacchi dall'esterno, nonché l'attività degli utenti autorizzati. Le misure di verifica a posteriori degli attacchi, non sono dalla legge contemplate, ma sono necessarie onde stabilire, a livello interno le responsabilità.

CIFRATURA E CRITTOGRAFIA
Le misure minime di sicurezza impongono per il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale contenuti in elenchi o registri o in banche dati con l'ausilio di strumenti elettronici, devono essere cifrati. Essi cioè devono essere resi non intelligibili se non si possiede la chiave di decodifica. Più in generale che cosa è la crittografia?
Essa consiste in una tecnica che consente di trasmettere i dati in sicurezza poiché solo il destinatario che possieda la chiave di decodifica potrà leggerli.
Può essere a chiave semplice o simmetrica e a chiave pubblica o asimmetrica. Nella prima entrambi i soggetti utilizzano la stessa chiave di codifica e decodifica: esempio banale ad ogni lettera corrisponde il numero che essa occupa nell'alfabeto, per convenzione tra i soggetti. È chiaro che tale accordo deve essere scambiato prima della trasmissione e su canale sicuro, non impone l'uso di attrezzature troppo potenti ma devono essere utilizzate chiavi diverse per ogni persona o gruppo di persone che comunicano scambiandosi i dati.
Al contrario la seconda prevede che i soggetti abbiano due chiavi una segreta che va custodita e conservata ed un pubblica che può essere distribuita con tranquillità perfino a concorrenti. Il mittente codifica il messaggio da spedire con la chiave pubblica del destinatario e per la caratteristica dei logaritmi di questa chiave non può più leggere il messaggio a meno che non ne abbia una copia (del messaggio). Il

destinatario legge con la sua chiave privata il messaggio, che è arrivato in tutta sicurezza e protezione. Sugli stessi algoritmi si basa la firma digitale che consente tra l'altro non solo di attribuire con certezza un documento ad un soggetto, ma anche di evitare, quindi, che lo stesso soggetto che lo ha firmato possa ripudiarlo (si pensi a quanto è importante nella stipula di contratto nello scambio di informazioni ecc.) oggi, poiché la legge ha attribuito validità alla firma digitale, esistono delle autorità che certificano la autenticità della firma, un po' come il Comune che rilascia la autentica delle firme.
Attraverso poi la funzione di hash monodirezionale, si garantisce l'autenticità del testo con un sistema semplice nella sua complessità: immaginiamo di passare al tritacarne il corpo del messaggio, ottenendo come risultato un numerosi "n" cifre, all'arrivo al destinatario del messaggio stesso, questi con la stessa funzione di hash, passerà anch'egli il messaggio al tritacarne: il risultato dovrebbe coincidere, e se così non fosse significherebbe che il messaggio è stato alterato nel corso del suo viaggio dal mittente al destinatario.

DISASTER RECOVERY
Il piano di disaster recovery, contenuto nel dps, riassume nel dettaglio tutte le operazioni da effettuare per porre rimedio alla catastrofe eventualmente occorsa alle nostre risorse. Non è più nella sfera preventiva quindi che ci si strova, ma in quella successiva al verificarsi dell'evento dannoso. Qui entra in gioco tutto il lavoro svolto, vengono messe alla prova le sinergie dell'azienda, siamo dunque alla svolta decisiva: se il dps è stato ben redatto se la formazione ha dato i suoi frutti, se le regole di base sono state rispettate il danno sarà minimo, a volte inesistente.
Ricordiamo che la legge prescrive che entro 15 giorni dalla richiesta di informazioni avanzata dall'interessata, il titolare deve provvedere ad una risposta: di conseguenza bisogna essere pronti a ristabilire il normale andamento del trattamento dei dati, entro 15 giorni.
Dunque: il piano di disaster recovery deve elencare quali sono i rischi a cui va incontro il nostro sistema e quali tipi di improduttività potrebbe causare il verificarsi di un evento classificato come rischio; ancora deve stabilire quali sono le funzioni prime che devono essere ripristinate in base alla loro essenzialità.
Bisogna inoltre scrivere le istruzioni di ripristino, che riguardano ad esempio le persone da contattare di ciascun reparto, i luoghi in cui sono conservati i supporti con i dati di back up, i fornitori di nuovi pc, ecc. E' ovvio, che il piano di disaaster recovery, va revisionato, reso comprensibile anche ai non addetti ai lavori, tenuto aggiornato in base all'avanzare dello sviluppo tecnologico dell'azienda. Non è una unità cristallizzata che viene posta in essere una volta per tutte.

Ora qualche raccomandazione.
Osserviamo le slides.