IL NUOVO CODICE DELLA PRIVACY
(D.Lgs. 196/2003)

Corso di diritto dell'informatica

PRINCIPI GENERALI

- Il concetto di diritto alla riservatezza (autodeterminazione informativa) è mutato con l'evoluzione della società.
- In origine significava diritto ad essere lasciato da solo
- Oggi è sinonimo di diritto di controllare le informazioni personali

PRINCIPI GENERALI

- Necessità di riformulare la sequenza intorno alla quale è stato costruito il concetto di riservatezza:
- DA *persona – informazione - segretezza*
- A *persona – informazione – circolazione – controllo*

PRINCIPI GENERALI

- **Art. 1. Diritto alla protezione dei dati personali**
  1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano
- **Art. 2. Finalità**
  1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

DEFINIZIONI

- Il legislatore all'articolo 4 del Codice ha ritenuto opportuno definire le parole-chiave della normativa
- In sintonia con il legislatore comunitario le nozioni appaiono sufficientemente ampie al fine di garantire una più elastica applicazione delle stesse

DEFINIZIONI – 1° CO.

- a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

DEFINIZIONI – 1° CO

- b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

DEFINIZIONI – 1° CO

- c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

DEFINIZIONI – 1° CO

- e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

DEFINIZIONI – 1° CO

- f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

DEFINIZIONI – 1° CO

- l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

DEFINIZIONI – 2° CO

- g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

- m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

DEFINIZIONI

- a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

- b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

DEFINIZIONI

- c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

- d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

- e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- SCOPO DEL LEGISLATORE:

  Nella complessità planetaria della rete, le minacce alla sicurezza e alla riservatezza dei dati rientrano tra i principali problema da affrontare e risolvere per garantire e proteggere gli interessi collettivi, i soggetti, gli utenti ed i servizi.
- La corretta applicazione delle misure di sicurezza, minime e più ampie, consente non solo di adempiere agli obblighi di legge, ma anche di migliorare l'organizzazione aziendale (consapevolezza che i dati trattati sono corretti, integri, aggiornati che costituiscono vere informazioni).

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- Le misure adottate dovranno proteggere I DATI PERSONALI ED I SISTEMI e cioè:
  - PROGRAMMI INFORMATICI
  - GLI STRUMENTI ELETTONICI E NON
  - IL SISTEMA INFORMATIVO NEL SUO COMPLESSO
  - ATTI E DOCUENTI CARTACEI
  - GLI ARCHIVI (INFORMATICI E NON)

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- OBBLIGHI DI SICUREZZA RIGUARDANO:
  - IL TITOLARE DEL TRATTAMENTO
  - IL RESPONSABILE (SE è STATO NOMINATO)
  - GLI INCARICATI
  - E QUALUNQUE ALTRO SOGGETTO CHE E' TENUTO ALL'ADOZIONE DELLE MISURE DI SICUREZZA
- IL TITOLARE DOVRA':
  - VIGILARE E VERIFICARE CHE LE INFORMAZIONI DA LUI IMPARTITE SIANO RISPETTATE
  - NELL'APPLICAZIONE DELLE MISURE DI SICUREZZA DOVRA' TENERE CONTO DELL'ARTICOLO 15 DEL CODICE PER EFFETTO DEL QUALE NEL CASO DI RICHIESTA DI RISARCIMENTO DANNI DOVRA' DIMOSTRARE DI AVER ADOTTATO TUTTE LE MISURE IDONEE AD EVITARE IL DANNO

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- La nozione di misura di sicurezza esprime un concetto dinamico e non statico proprio perché richiede una ricognizione sempre aggiornata sulle possibili soluzioni per la sicurezza
- La protezione dei dati personali attraverso adeguate misure di sicurezza è prevista in più parti del codice:
  - A) definizioni (articolo 4 comma 3);
  - B) misure di sicurezza in generale (articoli 31-32);
  - C) misure minime di sicurezza (articoli 33 – 35);
  - D) modalità di attuazione delle misure minime contenute nel disciplinare tecnico (allegato B)
  - Sanzioni ed illeciti penali (articolo 169)
  - Danni cagionati per effetto del trattamento (articolo 15).

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- Sono state previste nuove misure di sicurezza per esempio:
  - A) adozione di procedure per la generazione e la custodia di copie di scurezza dei dati;
  - B) il ripristino della disponibilità dei dati e dei sistemi;
  - C) tutela della sicurezza soprattutto per quanto concerne la tutela dei dati sensibili e dei dati giudiziari;
  - D) l'aggiornamento periodico dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici;

SICUREZZA DEI DATI E DEI SISTEMI – TITOLO v – CAPO I

- Tutte le nuove misure minime di sicurezza sono inserite nel corpo del Codice e viene rimandato all'Allegato disciplinare tecnico l'elencazione di dettaglio che potrà essere modificata ed aggiornata periodicamente, con Decreto del Ministero di Giustizia in concerto con il Ministero per le innovazioni e le tecnologie senza la necessità di un intervento diretto sul Codice.
- Rimane la differenza (ugualmente al testo previgente) tra i trattamenti svolti con strumenti elettronici (art. 34) e quelli effettuati senza l'ausilio di tali strumenti (art. 35).

RESPONSABILITA' CIVILE

- **Art. 15. Danni cagionati per effetto del trattamento**
  1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

  2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.
- **Art. 2050 c.c. Responsabilità per l'esercizio di attività pericolose**

  1. Chiunque cagiona danno ad altri nellos volgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento se non prova di aver adottato tutte le misure idonee ad evitare tale danno.

RESPONSABILITA' CIVILE

- **Art. 11. Modalità del trattamento e requisiti dei dati**
  1. I dati personali oggetto di trattamento sono:
- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento intermini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

RESPONSABILITA' CIVILE

- Articolo 15 - specifica tutela risarcitoria per i danni provocati nell'attività di elaborazione dei dati.
- L'applicazione dell'articolo 2050 c.c. permette di considerare il trattamento dei dati come un'attività pericolosa.
- Il concetto civilistico di "pericolosità" è in continua evoluzione: prima dell'emanazione del Codice il concetto di "pericolosità" era legato alla lesione dell'integrità fisica della persona. Oggi viene superato tale limite, considerando come pericoloso un comportamento idoneo a creare danni anche ad un diritto della personalità.

RESPONSABILITA' CIVILE

- **<u>Peculiarità dell'articolo 2050 c.c.:</u>**
  criterio di imputabilità diverso da quello tradizionale che si traduce nell'inversione dell'onere della prova a carico di colui che svolge l'attività pericolosa, invece che al danneggiato, come previsto per la disciplina dell'illecito aquiliano (es. art. 2043 c.c.);
- Chiunque cagioni un danno, quindi, avrà l'onere di provare di aver posto in essere ogni misura idonea ad evitarlo.
- Il danneggiante dovrà fornire una prova positiva, ossia dimostrare di aver predisposto ogni accorgimento necessario tale da escludere il nesso eziologico tra l'attività pericolosa di trattamento dei dati e l'evento. - **misure minime ed idonee**

RESPONSABILITA' CIVILE

- Il titolare ed il responsabile dovranno perciò adottare le misure di prevenzione più idonee, oltre a quelle minime prescritte, tra quelle disponibili in relazione alle conoscenze acquisite ed allo sviluppo delle tecnologie, allo scopo di ridurre al minimo i rischi, possibili, probabili, prevedibili e prevenibili che incombono sui dati.
- Le scelte operate determineranno effetti diversi ai fini dell'eventuale risarcimento del danno e delle eventuali sanzioni.

RESPONSABILITA' CIVILE

- L'INOSSERVANZA DELLE NORME SULLA SICUREZZA POTRA' COMPORTARE RESPONSABILITA' CIVILI E PENALI DA PARTE DEL TITOLARE, DEL RESPONSABILE O DI CHIUNQUE, ESSENDOVI TENUTO, OMETTA DI ADOTTARLE:
  - A) PENALI: SE NON SONO ADOTTATE LE MISURE MINIME;
  - B) CIVILI: CON RISARCIMENTO DEL DANNO IN ASSENZA DI QUELLE PIU' AMPIE CHE DOVRANNO RISULTARE SEMPRE AGGIORNATE.

RESPONSABILITA' CIVILE

- Il secondo comma dell'articolo 15 del Codice prevede la risarcibilità del danno non patrimoniale (la giurisprudenza più recente è orientata a concedere il risarcimento di tale tipo di danno ogniqualvolta si verifichi la lesione di un interesse costituzionalmente protetto anche se il fatto non sia configurabile come reato – Cass. 03/8827 e Cass. 03/12124).
- Fa espresso riferimento all'articolo 11 del Codice (disposizione concernente le modalità di raccolta ed i requisiti dei dati personali).
- Per esempio i danni più frequenti saranno:
  - Divulgazione di notizie false o incomplete;
  - La conservazione dei dati oltre il tempo strettamente necessario al raggiungimento dei fini della raccolta

RESPONSABILITA' CIVILE

- In ogni caso il danno morale (non patrimoniale) sarà risarcibile SOLTANTO COME PREGIUDIZIO EFFETTIVAMENTE CONSEGUENTE AD UNA LESIONE.

- Il danneggiato dovrà dimostrare quindi l'entità del danno subito – dimostrazione del fatto che la lesione ha creato una diminuzione o privazione di un valore personale (non patrimoniale) alla quale il risarcimento deve essere equitativamente commisurato.

RESPONSABILITA' CIVILE

- **SOGGETTI TENUTI AL RISARCIMENTO**
- Il legislatore con la locuzione "chiunque" non ha chiaramente individuato i soggetti tenuti a rispondere dei danni cagionato per effetto del trattamento.
- La dottrina ha ritenuto che le norme del Codice siano più facilmente riferibili al titolare ed al responsabile del trattamento in funzione alla loro capacità di decidere in merito alle fasi del trattamento o alle operazioni che hanno causato o permesso la realizzazione del danno.
- In particolare per ciò che concerne il titolare del trattamento si ritiene che possa essere considerato responsabile tanto la persona fisica quanto quella giuridica, quanto la PA.

ILLECITI PENALI

- Articoli di riferimento dal 167 a 172 del Codice – contenuti al capo II del titolo III della parte III e si tratta di:
  - Reati di scopo
  - Reati propri, in alcuni casi si tratta di reati propri ed esclusivi
- Finalità del legislatore: tutelare la funzione del Garante (fase istruttoria e decisoria)

ILLECITI PENALI

- Motivi della scelta della norma penale:

  - Rilevanza costituzionale degli interessi coinvolti;
  - Necessità di garantire omogeneità a livello comunitario.

ILLECITI PENALI

- Nel nuovo Codice sono stati previsti:
  - Tre delitti (articoli 167, 168, 170)
  - Due contravvenzioni (articoli 169, 171)
  - Una pena accessoria (articolo 172)
- Il legislatore ha utilizzato il metodo del rinvio ad altre norme dello stesso Codice e anche a leggi differenti (es. legge 300/1970 richiamata dall'articolo 171)

ILLECITI PENALI DELITTI

- I delitti sono trattati agli articoli:
  - 167 *(Trattamento illecito di dati);*
  - 168 *(Falsità nelle dichiarazioni e notificazioni al Garante);*
  - 170 *(Inosservanza di provvedimenti del Garante).*

ILLECITI PENALI DELITTI

- Tutti i delitti contengono una “clausola di salvezza” – *“salvo che il fatto costituisca più grave reato”*;
- Pena edittale minima;
- Non è permesso l’utilizzo delle misure cautelari e di strumenti di investigazione come ad esempio le intercettazioni telefoniche.

ILLECITI PENALI DELITTI

- A livello pratico si avrà sempre una duplice incriminazione.

- Esempio: connubio tra l'articolo 168 rubricato "*Falsità nelle dichiarazioni e notificazioni al Garante"* e uno dei reati penali ad esso attinenti come il delitto di truffa (articolo 640) o di appropriazione indebita (articolo 646).