La cultura della *privacy* e la gestione sicura delle informazioni

Riflessioni sul recepimento del diritto alla protezione dei dati personali e sulla definizione dei Sistemi di Gestione *Privacy*

a cura dell'**Ing. Francesco Amendola** – Nextel Italia s.r.l.

Profilo del relatore

Francesco Amendola è laureato in Ingegneria Elettronica con Lode presso l'Università degli Studi di Roma Tre ed è un laureato del Collegio Universitario "Lamaro-Pozzani".

Attualmente ricopre la carica di *IT Security Specialist* all'interno della Nextel Italia s.r.l. – www.nextel.it – società multinazionale di telecomunicazioni, specializzata nella progettazione di sistemi VoIP.

Gestisce anche un sito personale all'indirizzo www.ingamendola.com, dove sono disponibili articoli e presentazioni in materia di sicurezza informatica e protezione dei dati personali.

Sommario

1. La *privacy*: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione *Privacy* (SGP)
7. Conclusioni

La *privacy*: diritto o dovere?

- Definizione di *Privacy*
  - *Right to be let alone* (Warren e Brandeis, *Right to Privacy*, Harvard Law Review, vol. IV, 1890)
  - Tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali (*Direttiva 95/46/CE*)
  - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (*L. 675/96*)
  - Diritto alla protezione dei dati personali (*D.Lgs. 196/03*)

La *privacy* come diritto

Riservatezza della sfera privata dell'individuo

↓

Garanzia che i trattamenti di dati personali si svolgano 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

La *privacy* come diritto

- **L'interessato, prima di fornire il consenso al trattamento dei propri dati, ha il diritto di conoscere:**
  - le finalità e modalità del trattamento
  - la natura obbligatoria o facoltativa del conferimento dei dati, e le conseguenze di un eventuale rifiuto
  - i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza, e l'ambito di diffusione dei dati
  - gli estremi identificativi del titolare e, se designato, del responsabile del trattamento

La *privacy* come diritto

- **L'interessato, una volta fornito il consenso al trattamento dei propri dati, ha il diritto di accesso ai medesimi, ovvero di ottenere:**
  - la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile
  - l'indicazione dell'origine dei dati personali e del contenuto dell'informativa al trattamento
  - l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, con l'attestazione che tali operazioni siano portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi
- L'interessato ha diritto di opporsi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta, per motivi legittimi ovvero a fini di invio di materiale pubblicitario, comunicazioni commerciali, etc.

Diritto di esercitare un controllo sulle informazioni che riguardano l'individuo

La *privacy* come dovere

- **Chiunque tratti dati personali dovrà fornire sufficienti ed idonee garanzie agli interessati al trattamento, facendo in modo che i dati personali oggetto di trattamento siano**:
  - trattati in modo lecito e secondo correttezza
  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi
  - esatti e, se necessario, aggiornati
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati
  - 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
- In caso di danni causati da trattamenti illeciti, l'onere della prova è a carico di chi è responsabile del trattamento

La *privacy* come dovere

- Obbligo di sicurezza dei sistemi e dei dati
- Chiunque tratti dati personali dovrà custodire e controllare tali dati in modo da ridurre al minimo i rischi di:
  - distruzione o perdita anche accidentale
  - accesso non autorizzato
  - trattamento non consentito o non conforme alle finalità della raccolta
- La riduzione del rischio deve avvenire mediante l'adozione di idonee e preventive misure di sicurezza
- La scelta delle misure idonee deve avvenire in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento

La *privacy* come dovere

- **Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime di sicurezza:**
  - autenticazione informatica
  - adozione di procedure di gestione delle credenziali di autenticazione
  - utilizzazione di un sistema di autorizzazione
  - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
  - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
  - segue...

La *privacy* come dovere

- **Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime di sicurezza:**
  - segue...
  - adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati e dei sistemi
  - tenuta di un aggiornato documento programmatico sulla sicurezza
  - adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

La *privacy* come dovere

Dovere di assicurare un elevato livello di tutela del diritto alla protezione dei dati personali dell'interessato

La *privacy* come dovere

- **Di fatto il titolare dei trattamenti di dati personali è colui che insindacabilmente sceglie le modalità operative, gli strumenti, le misure di sicurezza in base ai rischi individuati, etc.**

- **Gli interessati ne possono al più prendere atto, ma non possono influenzare le scelte operative del titolare, che dunque ha il dovere di rispettare tutto quanto previsto codice**

Sommario

1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione *Privacy* (SGP)
7. Conclusioni

Chiunque ha diritto alla protezione dei dati personali che lo riguardano

(art.1 D.Lgs. 196/2003)

Il diritto alla protezione dei dati personali

- **Ha suscitato notevole attenzione ed interesse in quanto, riconoscendone l'esigenza, questo nuovo diritto afferma:**
  - il rispetto dell'identità personale
  - la tutela della dignità dell'individuo
  - il diritto alla riservatezza

- **È stato tuttavia mal interpretato nel momento in cui:**
  - è stato ridotto al significato originario di privacy, ovvero diritto alla riservatezza della sfera privata
  - è stato contrapposto ad altri diritti di rango superiore (es. sicurezza) e sminuito nella sua portata

Il diritto alla protezione dei dati personali

Emerge un legame profondo tra libertà, eguaglianza, democrazia, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo

(Prof. S. Rodotà)

Il diritto alla protezione dei dati personali

- **Libertà**
  - minacciata da profilazione, rintracciabilità, (geo)-localizzazione, (video)-sorveglianza
- **Eguaglianza**
  - minacciata da discriminazioni razziali, religiose, filosofiche, politiche, relative allo stato di salute o alla vita sessuale
- **Democrazia**
  - minacciata dalla mancanza di tutela di opinioni politiche, adesione a partiti, sindacati, associazioni od organizzazioni politiche
- **Dignità**
  - minacciata da intrusioni nella sfera privata, controlli e verifiche per esigenze di sicurezza sociale

Il diritto alla protezione dei dati personali

- **Esempi di recenti ambiti di applicazione della tutela del diritto alla protezione dei dati personali, oltre la sfera privata dell'individuo**
  - Aziende, anche multinazionali
  - Biometria
  - Comunicazioni elettroniche
  - Credito
  - Lavoro
  - Media
  - Politica
  - Sanità
  - Tecnologia
  - Telecomunicazioni

Sommario

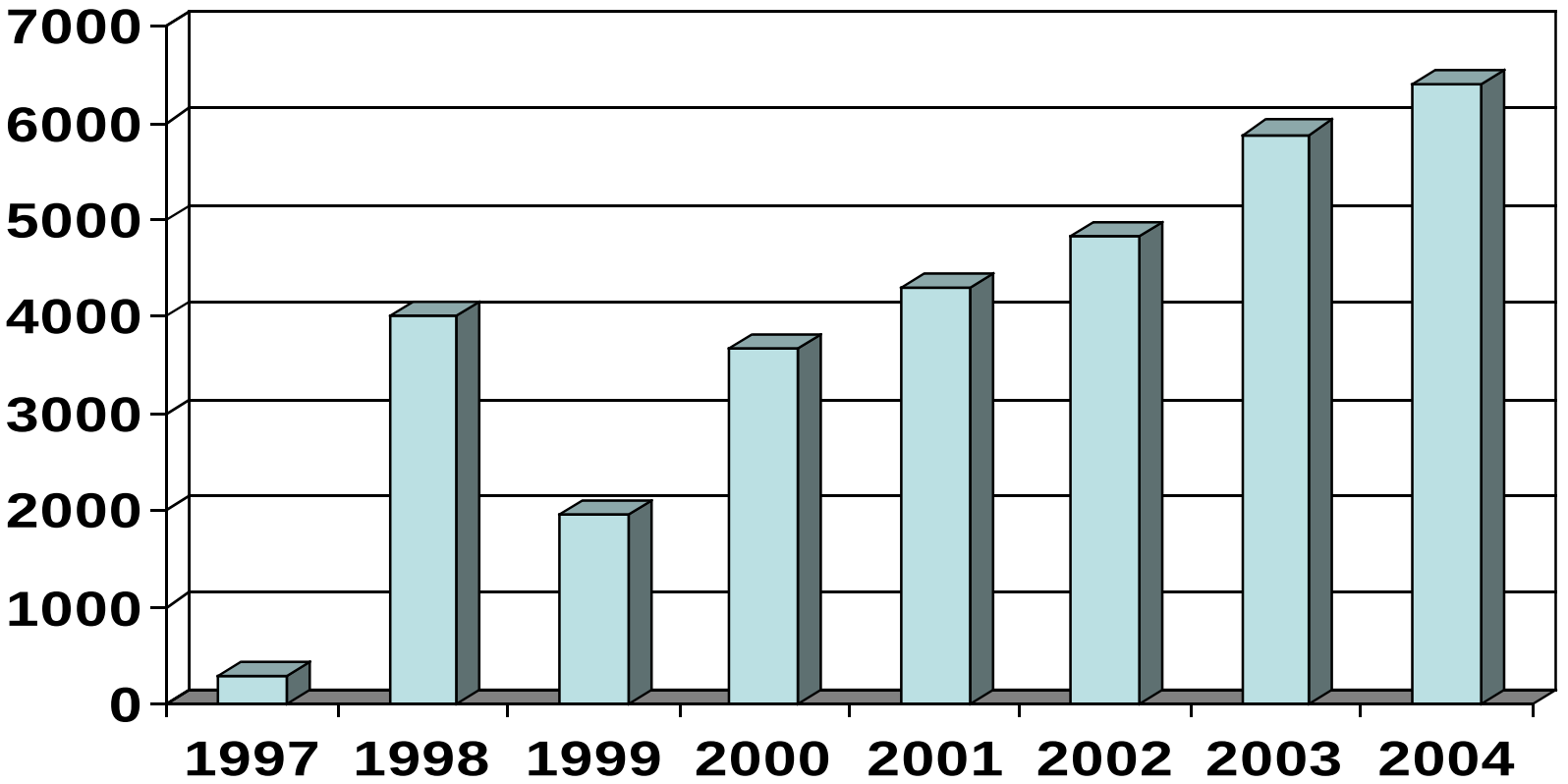
1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione *Privacy* (SGP)
7. Conclusioni

Il recepimento del D.Lgs. 196/03

- **La scarsa sensibilizzazione e la generale sfiducia verso la tutela dei dati personali, sia da parte dei titolari che degli interessati ai trattamenti, rischia di concretizzarsi in:**
  - assenza di informativa o informative generiche e poco dettagliate
  - difficoltà nell'esercizio del diritto d'accesso ai dati personali
  - inefficacia delle richieste di cancellazione dei dati personali
  - conservazione dei dati personali oltre il periodo necessario al trattamento
  - acquisizione di dati superflui alle finalità del trattamento
  - utilizzo dei dati personali per finalità diverse da quelle dichiarate
  - trattamenti affidati a terze parti non dichiarate

Il recepimento del D.Lgs. 196/03

- **Segnalazioni pervenute all'autorità Garante per la *privacy***



Fonte www.garanteprivacy.it

Il recepimento del D.Lgs. 196/03

- **Il D.Lgs. 196/03 non è ancora entrato pienamente in vigore**
  - Per i trattamenti di dati personali iniziati prima del 1 gennaio 2004, l'identificazione con atto di natura regolamentare dei tipi di dati sensibili e giudiziari trattati, è effettuata entro il 31 dicembre 2006
- **L'adempimento di alcune importanti disposizioni è entrato in vigore piuttosto di recente**
  - Le misure minime di sicurezza che non erano previste dal D.P.R. n. 318/99, sono adottate entro il 31 marzo 2006
  - Il titolare che alla data di entrata in vigore del codice disponeva di strumenti elettronici che non consentivano l'immediata applicazione delle misure minime, doveva adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti, adeguando i medesimi strumenti al più tardi entro il 30 giugno 2006

Il recepimento del D.Lgs. 196/03

- **I continui rinvii dell'entrata in vigore di parte del Codice, hanno ingenerato l'erronea convinzione che l'applicazione dell'intero codice venisse differita. In realtà:**
  - l'intento originario dei rinvii era concedere un lasso di tempo maggiore per adeguarsi pienamente agli adempimenti del decreto
  - il continuo posticipo della data ultima di adeguamento ha accentuato il disinteresse verso l'effettiva applicazione del Codice privacy
  - vi è stata scarsa o errata informazione da parte dei media
  - talvolta la stessa Autorità Garante è stata contraddittoria nei suoi comunicati
  - l'attività ispettiva, di controllo e sanzionatoria da parte dell'Autorità Garante non incide significativamente sulla percezione che di essa ne hanno titolari ed interessati di trattamenti di dati personali

Il recepimento del D.Lgs. 196/03

- **Il comune sentire dei titolari di trattamenti di dati personali è stato spesso riluttante a considerare di per sé precettive le parti del D.Lgs. 196/03 già in vigore, a volte addirittura ponendole in contrasto con altri adempimenti normativi e dunque rifiutandole**

- **Gli interessati ai trattamenti di dati personali non hanno percepito sufficienti garanzie al rispetto delle norme da parte dei titolari che trattano i loro dati e ne scelgono insindacabilmente gli strumenti e le modalità di trattamento**

Il recepimento del D.Lgs. 196/03

- Atteggiamento superficiale da parte dei titolari di trattamenti di dati personali, nel momento in cui ritengono sufficienti le misure minime di sicurezza previste dal codice
- Celare dietro il termine *privacy* l'incapacità o la mancanza di volontà di fornire le informazioni richieste non migliora affatto la percezione che si ha dell'intero sistema
- Sfiducia nel sistema di protezione di dati personali da parte dei cittadini interessati da trattamenti, che a volte associano al termine *privacy* il concetto di silenzio o addirittura di "omertà" da parte dell'istituzione che non può fornire i dati richiesti, piuttosto che di tutela della riservatezza degli stessi

Il recepimento del D.Lgs. 196/03

- Sistema di tutela della protezione dei dati personali visto solo come un insieme di meri adempimenti formali da attuare onde evitare sanzioni, tra l'altro in apparente contraddizione con altri sistemi di garanzia dei diritti dei cittadini interessati da trattamenti, quali ad esempio i codici di deontologia degli Ordini professionali
- Nell'analizzare i trattamenti di dati effettuati, per verificarne la conformità a quanto previsto dal codice, spesso si cerca di trovare le motivazioni idonee ad escludere il maggior numero di adempimenti possibili, piuttosto che valutare in modo puntuale e compiuto la natura, le modalità e le finalità, oltre che le possibili criticità, dei trattamenti stessi

Sommario

1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione *Privacy* (SGP)
7. Conclusioni

Privacy come Qualità

- Anche se da un punto di vista formale tutti gli obblighi previsti dal D.Lgs. 196/03 vengono adempiuti, spesso non si coglie il vero spirito che ha portato alla promulgazione di questo codice, ovvero la cultura di tutela e protezione dei dati personali oggetto di trattamento

- Questa cultura della *privacy* si estrinseca principalmente:
  - nella proattività degli interventi
  - nell'adozione di misure di sicurezza idonee
  - nella percezione di un beneficio, che ben ripaga i costi da sostenere per l'adeguamento

Privacy come Qualità

- Proattività degli interventi
  - non occorre attendere l'obbligo normativo per la messa in sicurezza dei sistemi IT, per la gestione del rischio e per la predisposizioni di piani di business continuity e disaster recovery
  - il codice *privacy* va letto alla luce della filosofia che ne è alla base, non cercando le incongruenze ed i cavilli, anche linguistici, per dubitare dell'interpretazione corretta
  - l'adeguamento a quanto previsto dal codice privacy è solo un punto di partenza per un Sistema di Gestione per la Sicurezza delle Informazioni, nell'ottica di un miglioramento continuo (*sistema dinamico*)

Privacy come Qualità

- Le misure di sicurezza idonee vanno oltre le misure minime
  - Password di almeno 8 caratteri
  - Aggiornamento semestrale del software Anti-virus
  - Aggiornamento semestrale del Sistema Operativo
  - Back-up con cadenza settimanale
  - Cifratura dei dati sensibili da parte degli organismi sanitari
  - Obbligo di redazione del Documento Programmatico sulla Sicurezza
- L'adozione delle sole misure minime solleva da responsabilità penali, ma non da quelle civili, nel caso in cui si arrechi un danno (*responsabilità aggravata o oggettiva*)
  - Le misure idonee possono evitare danni maggiori, più difficili da risolvere ex post ed economicamente meno sostenibili

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - un DPS ben strutturato ed articolato è senza dubbio, per il titolare di trattamenti di dati personali, un validissimo strumento per valutare il proprio sistema di gestione, i propri processi e le criticità che potrebbero condurre ad una loro deviazione dallo standard
  - è importante redigere un DPS che non si limiti a considerare soltanto le contromisure minime di sicurezza per contrastare possibili minacce ai trattamenti, bensì vada oltre e prenda in esame tutte le misure di sicurezza idonee a garantire che, ragionevolmente, i fattori di rischio siano tenuti sotto controllo

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - il rispetto del codice ha come intrinseca finalità quella di indurre un miglioramento dell'organizzazione e della gestione aziendale, in particolare dei processi e degli standard di lavoro, ma anche della qualità e della rispondenza dei risultati ai requisiti prestabiliti
  - la redazione del DPS si configura come un valido ausilio all'individuazione delle fonti di rischio, alla loro classificazione in base alla gravità dell'impatto che possono produrre, alla pianificazione temporale delle priorità di intervento per l'abbattimento, o quanto meno per il controllo, dei fattori di rischio ritenuti maggiormente nocivi in relazione alle attività svolte

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - la capacità di gestire contenuti e dati in modo sicuro, affidabile ed efficiente è sempre più importante per la continuità del lavoro (*business continuity*) e la gestione delle emergenze (*disaster recovery*), ovvero per il mantenimento dei livelli qualitativi prefissati, ed è pertanto questa capacità che distingue fra loro le aziende di successo da quelle che, non riuscendo ad adeguarsi alle continue evoluzioni imposte dal mercato, non sono in grado di affermarsi nel loro settore di competenza

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - la corretta applicazione delle misure di sicurezza, ovvero di soluzioni tecnologiche specificamente progettate per la tutela della *privacy* (*Privacy Enhancing Technologies*), consente non solo di adempiere agli obblighi ed alle formalità di legge, ma soprattutto di migliorare l'organizzazione e la gestione aziendale, ottimizzando e controllando i processi di lavoro in aggiunta alla ragionevole certezza e consapevolezza di operare sempre con dati esatti, corretti, leciti, legittimi, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti, oltre che integri, disponibili ed aggiornati

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - con questa visione e cultura, la stessa organizzazione avrà quindi la garanzia di operare in sicurezza ed in ottemperanza agli adempimenti previsti dal contesto normativo vigente, trasmettendo agli *stakeholder* (clienti, fornitori, creditori, azionisti, etc.) fiducia nei propri riguardi, con un *feed-back* senz'altro positivo per la propria attività

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - una gestione sicura, affidabile ed efficiente non va semplicemente intesa come prevenzione della perdita accidentale di dati aziendali, o assicurazione contro eventuali danni, o ancora più semplicemente un modo per evitare le sanzioni previste in caso di inadempienza, bensì soprattutto come vantaggio competitivo tramite l'adozione di procedure di gestione delle informazioni che permettano di superare tutte le eventuali criticità che potrebbero sorgere da una mancanza di controllo dei processi: così facendo si trasforma la sicurezza da un costo passivo in un investimento lungimirante e dunque in un vantaggio competitivo

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - *La privacy è una combinazione di strumenti giuridici diversi, ma, anzitutto una privacy condivisa, una privacy orientata spontaneamente al rispetto della persona, concepita come una trave portante e non come un fardello*

    (G. Buttarelli)
  - *La privacy, considerata nel quadro delle relazioni tra soggetti economici, è destinata a delinearsi come il valore fondante di un patto tra imprese e consumatori che consentirà lo sviluppo economico in un mercato composto da soggetti in grado di realizzare scelte consapevoli e libere*

    (G. Rasi)
  - *La privacy rappresenta una risorsa che, se intelligentemente impiegata, può rendere più efficiente l'attività d'impresa*

    (S. Rodotà)

Privacy come Qualità

- La *privacy* come vantaggio competitivo
  - *Permission e direct marketing*, contrapposti a *interruption marketing* e SPAM
  - Soddisfazione del cliente e fidelizzazione
  - CRM (*Customer Relationship Management*)
  - *Binding Corporate Rules*

- *Esempi*
  - utilizzo di carte di credito per commercio on-line solo se l'utente si fida del sistema
  - consenso a ricevere e-mail pubblicitarie basate sui reali bisogni del consumatore
  - assistenza post-vendita più diretta e mirata alle reali esigenze

Privacy come Qualità

- Privacy e trasparenza
  - rischio di giudizi falsati dalle sole informazioni che si decide di diffondere e far circolare
  - rischio di giudizi falsati da informazioni parziali, errate, non aggiornate
- Reperimento di informazioni in poco tempo
  - Internet e motori di ricerca
  - ci si ferma alle prime informazioni trovate
  - un eccesso di informazioni a volte è peggio di poche informazioni mirate e corrette
- Informazioni errate o datate possono ingenerare pregiudizi e discriminazioni

Sommario

1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione *Privacy* (SGP)
7. Conclusioni

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Esigenza di gestire al meglio la sicurezza delle informazioni**
  - Riservatezza
  - Integrità
  - Disponibilità

  - Autenticazione
  - Autorizzazione
  - Non ripudio
  - Affidabilità

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **L'informazione è un *asset*, un bene di valore al pari di quelli materiali**
  - va protetta, in tutte le sue forme, al pari di un bene patrimoniale
  - in una realtà fortemente interconnessa la tutela delle informazioni è il punto di partenza per la continuità del servizio, per la riduzione di rischi e minacce, per massimizzare il ritorno degli investimenti e le opportunità di guadagno
  - consolidamento di un profilo competitivo, del flusso di cassa, del profitto, della conformità normativa, della reputazione sul mercato

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI) - *Information Security Management Systems (ISMS)***
- **ISO/IEC 17799:2005** *Information technology -- Security techniques -- Code of practice for information security management*
  - scopo: fornire le linee guida, i principi generali e le best practices per pianificare, implementare, controllare, revisionare, e migliorare la gestione della sicurezza delle informazioni
- **ISO/IEC 27001:2005** *Information technology -- Security techniques -- Information security management systems -- Requirements*
  - scopo: fornire un modello per pianificare, implementare, organizzare, controllare, revisionare, gestire, e migliorare un SGSI

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

1. **Policy della sicurezza delle informazioni**
   - impegno della Direzione nel promuovere la sicurezza delle informazioni in accordo con gli obiettivi aziendali e gli obblighi normativi
2. **Organizzazione della sicurezza delle informazioni**
   - gestione dell'implementazione del SGSI all'interno dell'organizzazione
   - gestione della sicurezza delle informazioni elaborate da terze parti esterne
3. **Gestione del patrimonio aziendale**
   - protezione dei beni aziendali, materiali o immateriali, e delle persone
   - classificazione delle informazioni da proteggere

4. **Sicurezza delle risorse umane**
   - consapevolezza dei propri compiti e responsabilità prima di prendere servizio
   - corretta gestione delle risorse umane durante lo svolgimento dei compiti affidati
   - corretta gestione delle risorse umane in caso di cambio mansioni o di cessazione del rapporto di lavoro
5. **Sicurezza fisica e ambientale**
   - aree sicure ad accesso controllato
   - protezioni degli apparati e dei sistemi

6. Gestione delle comunicazioni e delle operazioni

- procedure operative e responsabilità
- gestione dei servizi affidati in *outsourcing*
- progettazione del sistema ed accettazione prima dalla sua messa in esercizio
- protezione dai codici malevoli
- *back-up*
- gestione delle sicurezza della rete
- gestione dei dispositivi di memorizzazione
- scambio di informazioni
- servizi di commercio elettronico (*e-commerce*)
- monitoraggio e *audit*

7. Controllo degli accessi

- controllo degli accessi basato sui requisiti dell'attività (*business*)
- gestione dei profili di autorizzazione degli utenti
- responsabilità degli utenti
- controllo degli accessi alla rete
- controllo degli accessi ai Sistemi Operativi
- controllo degli accessi alle informazioni ed alle applicazioni
- computer portatili e telelavoro

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

8. **Acquisizione, sviluppo e gestione dei sistemi informativi**
   - requisiti di sicurezza dei sistemi informativi
   - elaborazione corretta dai dati da parte degli applicativi
   - utilizzo delle crittografia
   - sicurezza dei file di sistema e dei codici sorgenti
   - sicurezza nei processi di sviluppo, manutenzione ed assistenza
   - gestione delle vulnerabilità tecniche
9. **Gestione degli incidenti**
   - notifica degli eventi dannosi per la sicurezza delle informazioni e delle vulnerabilità del sistema che si riscontrano
   - gestione degli impatti dannosi alla sicurezza delle informazioni e miglioramento del sistema

10. Gestione delle continuità del servizio

- piani di *business continuity* relativi alla sicurezza delle informazioni

11. Conformità

- conformità normativa
- conformità alle *policy* di sicurezza, agli standard ed alla tecnica
- *audit* di conformità del sistema

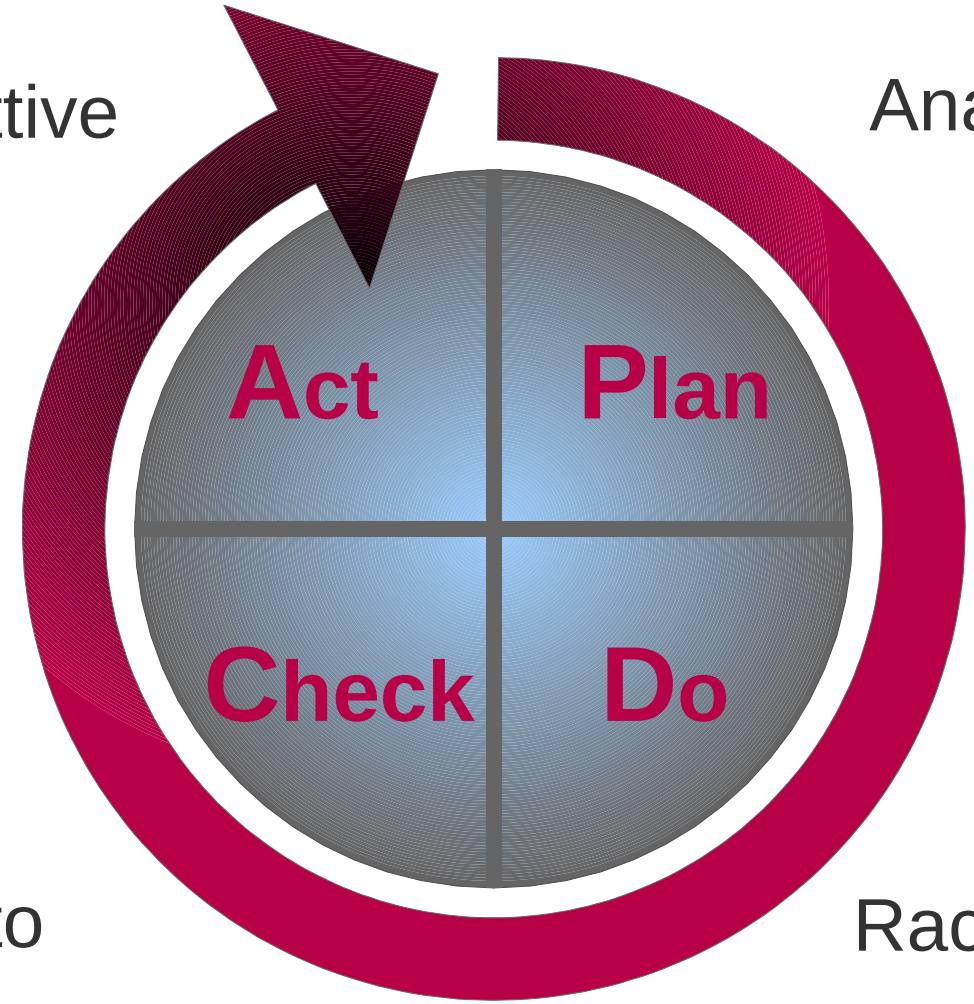
Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Gestione del rischio**
  - analisi del rischio: identifica le fonti di rischio e ne stima il livello
  - valutazione del rischio: considera l'impatto del rischio sulle attività
  - accettazione del rischio: definisce la soglia decisionale al di sotto della quale il rischio è tollerato
  - trattamento del rischio: valuta le contromisure da adottare per ridurre i livelli di rischio che oltrepassano la soglia
  - rischio residuo: rischio rimanente a seguito del trattamento
  - comunicazione del rischio: notifica dei risultati a cui si è pervenuti

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **ISO/IEC 27001:2005 è il recepimento da parte dell'ISO del BS7799-2**
  - specifica i requisiti necessari per pianificare, implementare, organizzare, controllare, revisionare, gestire e migliorare un SGSI
  - approccio per processi (PDCA)
  - compatibilità ed integrazione con altri Sistemi di Gestione (SGQ ISO 9001:2000, SGA ISO 14001:2004)
  - controlli derivano da ISO 17799:2005
  - permette di certificare la conformità del sistema

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)



Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Plan:** pianificare il sistema
  - comprendere i requisiti dell'organizzazione e stabilirne le politiche, gli obiettivi, i processi e le procedure di maggior rilievo per la gestione del rischio ed il miglioramento della sicurezza delle informazioni

- **Do**: implementare ed organizzare il sistema
  - porre in essere le politiche, gli obiettivi, i processi e le procedure di maggior rilievo per la gestione dei rischi relativi alla sicurezza delle informazioni di tutto il contesto aziendale

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Check**: controllare e revisionare il sistema
  - Valutazione del rendimento del sistema rispetto alle politiche, agli obiettivi, ai processi ed alle procedure pianificati nonché alle esperienze accumulate
  - Valutazione anche dell'efficacia del sistema
  - Riesame della direzione

- **Act**: gestire e migliorare il sistema
  - Adozione di azioni correttive e preventive, sulla base degli obiettivi misurati, dei risultati degli audit interni al sistema e del riesame della direzione
  - Perseguimento del miglioramento continuo

Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)

- **Realizzazione di un SGSI**
  - Definizione delle finalità e dei limiti del sistema
  - Definizione di una *policy* della sicurezza delle informazioni
  - Definizione di un approccio alla analisi e valutazione del rischio
  - Gestione del rischio
  - Definizione degli obiettivi e dei relativi controlli
  - Definizione della *Statement of Applicability* ed implementazione

Sommario

1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione Privacy (SGP)
7. Conclusioni

Sistema di Gestione Privacy (SGP)

- **La gestione della sicurezza delle informazioni si può ottenere partendo da un insieme di *common practice***
  - *policy* della sicurezza delle informazioni
  - piano delle deleghe delle responsabilità
  - consapevolezza, sensibilizzazione e formazione
  - elaborazione corretta dai dati da parte degli applicativi
  - gestione delle vulnerabilità tecniche
  - gestione della continuità del servizio
  - gestione degli impatti dannosi alla sicurezza delle informazioni e miglioramento del sistema

Sistema di Gestione Privacy (SGP)

- **In aggiunta alle *common practice*, occorre considerare anche la conformità normativa**
  - dati tutelati dal diritto d'autore o dal segreto d'ufficio
  - privacy e protezione dei dati personali

Sistema di Gestione Privacy (SGP)

- **Policy della sicurezza delle informazioni**
  - informativa agli interessati
- **Piano delle deleghe delle responsabilità**
  - nomina di responsabili e incaricati, individuando puntualmente l'ambito del trattamento consentito
- **Consapevolezza, sensibilizzazione e formazione**
  - previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare

Sistema di Gestione Privacy (SGP)

- **Elaborazione corretta dai dati da parte degli applicativi**
  - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici
- **Gestione delle vulnerabilità tecniche**
  - analisi dei rischi che incombono sui dati
- **Gestione della continuità del servizio**
  - adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati e dei sistemi
- **Gestione degli impatti dannosi alla sicurezza delle informazioni e miglioramento del sistema**
  - tenuta di un aggiornato Documento Programmatico sulla Sicurezza (DPS)

Sommario

1. La privacy: diritto o dovere?
2. Il diritto alla protezione dei dati personali
3. Il recepimento del D.Lgs. 196/03
4. *Privacy* come Qualità
5. Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI)
6. Il Sistema di Gestione Privacy (SGP)
7. Conclusioni

Conclusioni

- **Sensibilizzare alla *cultura* della *privacy* implica un naturale processo in grado di offrire tutte le garanzie dovute agli interessati dei trattamenti, indipendentemente dai vincoli giuridici, e di assicurare il pieno rispetto dei diritti fondamentali, tra cui principalmente la tutela della riservatezza dei dati personali**
  - la *privacy* non deve essere tutelata ex-post, ovvero solo a seguito di segnalazioni, reclami o violazioni sanzionate
  - il “ravvedimento operoso” deve aiutare a favorire la sensibilizzazione verso i nuovi principi introdotti con il Codice e ad agevolarne l'applicazione; non deve essere considerato un modo per non rispettare gli adempimenti previsti sino all'effettivo accertamento del reato

Conclusioni

- **L'equilibrio tra *privacy* e trasparenza deve essere raggiunto in base alle reali esigenze della realtà e del contesto in cui si collocano i rapporti tra titolari ed interessati**
  - una mancanza di privacy comporterebbe l'impossibilità di controllare i propri dati personali, di vedersi tutelata la propria riservatezza, dell'espressione serena della propria identità personale

  - un eccesso di privacy rischierebbe di ingolfare il necessario scambio di informazioni alla base dell'ordinario svolgimento delle attività sociali

Conclusioni

- **L'impiego di tecnologie a supporto della *privacy (PET – Privacy Enhancing Technologies),* associato alla consapevole esigenza di riservatezza degli utilizzatori, è in grado di catalizzare la realizzazione di un Sistema di Gestione della Sicurezza dei dati e delle informazioni**
  - cifratura del *file system*
  - e-mail crittografata
  - *remailer* anonimi
  - navigazione web anonima
  - pubblicazione di contenuti anonimi
  - *Trusted Computer* (?)

Grazie per l'attenzione!

info@ingamendola.com www.ingamendola.com