Walter Martino per Lhg12

Il garante per la tutela dei dati personali.

Crimini informatici.

Introduzione alle leggi sulla protezione dei dati personali.

- È ormai noto a tutti che ogni giorno vengono raccolti da parte di ogni tipo di aziende, associazioni o enti vari, informazioni riguardanti i singoli soggetti.

- Con l'utilizzo dell'informatica la creazione di banche dati per la raccolta e la selezione delle informazioni relative alle scelte, ai consumi ed alle abitudini dei cittadini è diventata una cosa all'ordine del giorno.
- Sono ormai cosa comune le tessere fedeltà o le raccolte punti per premi.

- Da tempo è intervenuta la Comunità Europea con la Direttiva 95/46/CE del 24 ottobre del 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

- Il Parlamento italiano per adeguarsi a tale direttiva pubblica la legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. G.U. n. 5 del 8 gennaio 1997.
- Diverse sono le modifiche successive e le deleghe al Governo per arrivare al **Decreto Legislativo del 30 giugno 2003 n. 196**, Codice in materia di protezione dei dati personali. G.U. n. 123 del 29 luglio 2003.

Decreto Legislativo del 30 giugno 2003 n. 196.

- **Codice in materia di protezione dei dati personali.**

- **Il dato personale** identifica il soggetto per nome, data e luogo di nascita, professione, sesso, ecc..
- **Il dato sensibile** riguarda la persona in modo particolare ed è in grado di rivelare le origini razziali, la religione, le opinioni politiche, ecc.
- **Il dato sensibilissimo** riguarda lo stato di salute e le abitudini sessuali.

- Le informazioni devono quindi essere gestite nel rispetto delle norme vigenti che riguardano le seguenti attività:
- La raccolta,
- L'elaborazione,
- La diffusione,
- La comunicazione a terzi delle informazioni raccolte,
- Il trasferimento all'estero e la distruzione finale dei dati raccolti.

- Il mancato rispetto delle norme prevede sanzioni penali e civili.
- La responsabilità sulla corretta applicazione del Codice è affidata al Garante per la protezione dei dati personali, organo collegiale formato da quattro componenti.

La raccolta dei dati personali.

- Durante la raccolta dei dati personali l'interessato deve dare il proprio consenso (per i dati sensibili in forma scritta) all'utilizzo degli stessi ed ha diritto ad essere informato:

- Sull'uso che ne verrà fatto, (finalità, modalità e limiti del trattamento dei dati),
- Sull'eventuale comunicazione e/o invio a terzi dei dati,
- Sul diritto, di accesso, rettifica, aggiornamento ed eventuale cancellazione dei dati da parte di chi presta il consenso al trattamento.

- L'uso dei dati contenuti in un elenco non è soggetto ad autorizzazione purchè sia rispettato lo scopo per il quale è stato formato l'elenco stesso.
- Esempio: Elenco telefonico

- Prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni - 19 gennaio 2011
(Gazzetta Ufficiale n. 24 del 31 gennaio 2011)

Figure principali nel trattamento dei dati personali

- **Il Garante**, organo collegiale che opera in piena autonomia e con indipendenza di giudizio e di valutazione.
- L'**interessato**, il cittadino, l'azienda o la persona giuridica cui i dati si riferiscono.
- Il **titolare del trattamento**, colui che raccoglie, gestisce o tratta i dati.
- Il **responsabile del trattamento**, colui che sotto il controllo diretto del titolare del trattamento provvede alla gestione del sistema dei dati e a tutte le attività di natura tecnica e organizzativa nel rispetto degli obblighi del trattamento dei dati.
- L'**incaricato del trattamento**, colui che svolgendo mansioni ben definite, impiegato, tecnico, ecc., opera con i dati personali raccolti.
- Gli **amministratori di sistema**, coloro che hanno il compito di sovraintendere alle risorse di un sistema operativo o di un sistema di base dati per consentirne l'utilizzazione.

Il Garante per la protezione dei dati personali.

- Sorveglia sulla regolare applicazioni del D. L.vo 196/2003 il Garante per la protezione dei dati personale,
- organo formato da 4 componenti eletti 2 dal Senato della Repubblica e 2 dalla Camera dei Deputati.

- Sede dell'Ufficio del Garante è:

  Piazza di Monte Citorio n. 121

  00186 Roma

- Diverse sono le funzioni del Garante in particolare è bene ricordare l'attività di controllo e di ispezione che può esercitare nei confronti di tutti coloro che per i più svariati motivi trattano dati personali.

- A tal fine è stato appositamente creato un sito internet dove è possibile reperire una completa rassegna legislativa e le attività svolte dall'ufficio stesso.

Sito web del Garante per la protezione dei dati personali.

- Indirizzo url http://www.garanteprivacy.it/garante/navig/jsp/index.jsp

Relazione sull'attività del Garante della privacy 2010

- **Informazioni pubblicate dal Garante nella relazione sull'attività 2010**
- L'Autorità Garante per la protezione dei dati personali, composta da Francesco Pizzetti, Giuseppe Chiaravalloti, Mauro Paissan e Giuseppe Fortunato, ha presentato la relazione sul quattordicesimo anno di attività e sullo stato di attuazione della normativa sulla privacy.
- Traccia il bilancio del lavoro svolto dall'Autorità e indica le prospettive di azione verso le quali occorre muoversi nell'obiettivo di costruire una autentica ed effettiva protezione dei dati personali, in particolare riguardo all'uso delle nuove forme di comunicazione e dei nuovi sistemi tecnologici.
- Le telefonate pubblicitarie indesiderate; Internet e le nuove tecnologie cloud computing; i sistemi di videosorveglianza; il fenomeno sempre più esteso dei social network; la trasparenza on line della Pubblica amministrazione; il servizio di Google Street View; i nuovi servizi in farmacia. E ancora: il delicato settore della sanità; il corretto rapporto tra diritto di cronaca e dignità delle persone; la protezione dei dati giudiziari; la tutela dei minori; la ricerca scientifica e farmacologica; le esigenze di semplificazione per le imprese.
- Sono solo alcuni dei principali e complessi ambiti nei quali il Garante ha assicurato il suo intervento nel corso del 2010 a difesa di singoli individui e collettività. Intervento rafforzato dai maggiori poteri sanzionatori ora a disposizione dell'Autorità.
- Numerose sono state le Audizioni parlamentari: tra le più rilevanti, quelle sulle problematiche legate alle politiche di immigrazione, all'anagrafe tributaria, alla semplificazione dei rapporti tra PA e cittadini.

Le cifre sull'attività del Garante della privacy 2010

- I provvedimenti collegiali adottati nel 2010 sono stati circa 600.
- Si è dato risposta a circa 4000 tra quesiti, reclami e segnalazioni (in particolare, riguardo a telefonia, credito, centrali rischi, marketing, videosorveglianza, Internet, assicurazioni).
- I ricorsi decisi dal Garante sono stati 350 (in maggioranza relativi a banche e finanziarie, attività di marketing, datori di lavoro pubblici e privati, sistemi di informazioni creditizie, operatori telefonici e telematici), confermando il trend dello scorso anno.
- Il Collegio ha reso 16 pareri al Governo e al Parlamento (in particolare in materia di attività di polizia e sicurezza, giustizia, Codice dell'amministrazione digitale, informatizzazione e banche dati della PA, formazione).
- Le ispezioni effettuate nel 2010 sono state circa 500. I controlli hanno riguardato numerosi settori: in particolare, gli operatori telefonici, le strutture sanitarie pubbliche e private, i sistemi di videosorveglianza, il sistema della fiscalità, le società di marketing, gli istituti di credito.
- Le violazioni amministrative contestate, compreso il primo semestre 2011, sono state oltre 500: una parte consistente ha riguardato le attività promozionali indesiderate, l'attivazione di servizi non richiesti e le strutture sanitarie pubbliche e private.
  55 le violazioni segnalate all'autorità giudiziaria nel 2010.
- Tenendo conto anche del primo semestre 2011 ammontano a più di 4 milioni di euro le sanzioni amministrative già riscosse.
- L'attività di relazione con il pubblico ha fatto registrare nel 2010 oltre 26.000 tra contatti telefonici ed e-mail esaminate, in particolare riguardo al telemarketing, alle e-mail e i fax indesiderati, alla videosorveglianza, a Internet, al lavoro pubblico e privato.

Introduzione ai crimini informatici.

- Molti sono i reati che si possono commettere frequentando la rete anche se in generale si può pensare alla violazione della privacy perché con troppa facilità vengono pubblicati dati senza il necessario consenso delle persone interessate.
- **Il fatto che ci si trova in un mondo virtuale non significa che i reati non esistono o che possano essere trascurati**. Le pene previste per i reati commessi in rete non sono poi così "leggere" in alcuni casi prevedono diversi anni di reclusione.
- **Alcuni reati sono nati con l'utilizzo del PC e della rete in generale,** in quanto si possono realizzare solo nell'ambiente virtuale, pensiamo per esempio all'accesso abusivo in una banca dati introdotto con la Legge 547/1993 che ha modificato il codice penale introducendo l'art. 615 ter,
- **altri erano già previsti dalle nostre leggi prima dell'arrivo di internet ma hanno trovato in questo nuovo strumento per comunicare una più facile realizzazione,** come per esempio le truffe, la pedopornografia o la sostituzione di persona.
- Altro importante distinguo è la divisione in due categorie tra coloro che compiono reati in rete:
- **1)** Quelli che accedono alla rete al solo **scopo di delinquere** (spamming, raccolta dati personali, truffe, trasmissione virus o materiale illegale, accesso abusivo, ecc);
- **2)** quelli che, pur utilizzando la rete per gli **scopi più nobili**, ossia **comunicare** con il resto del mondo compiono, **per ignoranza, per incoscienza o semplicemente per maleducazione, azioni** che il nostro legislatore ha previsto come **reati**.

Ingiuria, diffamazione e sostituzione di persona.

- Tra i reati che si commettono con maggior facilità in rete ne troviamo alcuni che peraltro rientrano tra quelli già previsti nel mondo reale:

- **L'ingiuria e la diffamazione** disciplinati dal c.p. agli **artt. 594 e 595**
- **La sostituzione di persona reato** disciplinato dall'art. **494 c.p.** In particolare incorrono in questo tipo di reato molti cybernauti che non si accorgono di compierlo perché ignari delle regole e delle norme in essere.

- Per quanto riguarda i primi due è bene ricordare che sempre più spesso vengono raccolte in rete le informazioni relative alla nostra persona, le nostre abitudini o il nostro modo di pensare. Sono nate aziende che ci consentono di controllare la nostra reputazione on line:

- http://www.reputazioneonline.it/

Sostituzione di persona.

- Il codice penale colloca questo reato tra i **delitti contro la fede pubblica** al capo IV della falsità personale.
- ***Sostituzione di persona***. *Chiunque, al fine di procurare a sè o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sè o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno.*
- Elemento essenziale del reato è la condotta idonea a generare dubbi sull'identità personale dell'agente. Se non sorgono dubbi circa l'identità il comportamento non si pone contro la pubblica fede e come tale non perseguibile ex art- 494 c.p.

- È del tutto evidente che **sostituirsi il nome con altro di fantasia non è di per se reato**, deve esistere il **dolo specifico** quale fine; deve esserci la **coscienza e la volontà** di ingannare altri. Il vantaggio può ravvisarsi nel compiere un crimine o più semplicemente nel cercare nuovi contatti sulla rete. Azione che alla maggior parte dei cybernauti appare lecita o forse scorretta ma raramente conosciuta come reato. La Cassazione con la sentenza 1570/06 ha ritenuto che:
- ***"il dolo richiesto dall'art. 494 c.p. ricorre quando l'agente si attribuisce un falso nome con lo scopo di entrare in relazione con persone che, altrimenti, non concederebbero a lui la loro amicizia o confidenza."***

Sostituzione di persona, danno altrui.

- Elemento oggettivo del reato e l'induzione in errore al fine di ottenere un vantaggio o danno altrui. Non è necessario l'effettivo vantaggio o il concreto danno altrui.

- **Danno altrui** si verifica quasi sempre nel momento in cui la parte offesa denuncia il fatto illecito (es. diffamazione) che anche in caso di ritiro della querela, laddove si trattasse di reato perseguibile a querela, prosegue in quanto la sostituzione di persona, essendo un reato contro la pubblica fede, è perseguibile d'ufficio. Infatti la Corte Suprema con la sentenza 2335/07 cassa il ricorso e riconosce il reato anche nel caso in cui vi sia la remissione della querela che in origine ha attivato l'azione penale:

- ***"il fine di recare, con la sostituzione di persona, un danno al soggetto leso: danno poi in effetti, in tutta evidenza concretizzato, …. (relativo al reato di diffamazione, peraltro poi estinto per remissione di querela) nitidamente delinea nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l'immagine e la dignità."***

Stalking.

- Col temine *stalking* si indicano una serie di comportamenti e/o atteggiamenti posti in essere da un soggetto al fine di affliggere altra persona.
- Questi atteggiamenti sono di tipo persecutorio ed hanno lo scopo di affliggere il destinatario generando in lui paura ed ansia.
- Questa condotta è penalmente rilevante dal 2009 quando il reato è stato introdotto dall'art. 7 del D.L. 11/2009.
- ***612-bis.*** *Atti persecutori.*
- *Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita. La pena è aumentata se il fatto è commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa. La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.*

Cyberstalking.

- Con il termine *Cyberstalking* si indica lo stesso comportamento previsto dal 612 bis utilizzando la rete quale mezzo per raggiungere il destinatario del comportamento persecutorio.
- In questo caso gli atti persecutori sono molto più dannosi:
- Avvengono in una piazza virtuale dove non è possibile valutare il numero di persone presenti,
- Non è possibile cancellare i documenti trasmessi in rete,
- Non è possibile sapere per quanto tempo potrà viaggiare sulla rete ciò che è stato pubblicato con fini persecutori, con i socialnetworks il documento pubblicato sfugge al controllo di chi lo ha pubblicato.

- La Corte di Cassazione ha ritenuto che le molestie su facebook rientrino nel reato di stalking confermando la pena per coloro che attuano una condotta persecutoria e assillante tramite il socialnetwork.

- V sezione penale, 12 aprile 2012 n. 13878, Pres. Oldi, Rel. Zaza

Cyberbullismo.

- Bullismo on line o nella vita reale comporta spesso la violazione del codice penale, del codice civile e il codice della privacy (D.L.vo 196/2003).

- Alcune statistiche dicono che oggi il 34% del 'bullismo' avviene on line.
- Si presenta in diversi modi:
- Sui socialnetworks, con la posta elettronica o con SMS, lo scopo è quello di minacciare ripetutamente e senza motivo la vittima di turno.

- Nel cyberbullismo gli atti di bullismo sono spesso nascosti alla vittima di turno che a volte scopre tramite terzi i danni subiti con la pubblicazione di foto o documenti che hanno il solo scopo di denigrare la vittima di turno.

- **Tutti i danni del cyberbullismo -** (5 luglio 2009) - Corriere della Sera -
- Messaggi offensivi, foto o video indesiderati, minacce via cellulare: così il bullismo è diventato cyberbullismo, un fenomeno nuovo, come dimostra una ricerca fatta su 700 studenti dall' Università di Chieti. Le vittime soffrono di depressione nel 35% dei casi mentre l' 8% dei cyberbulli è a rischio di sviluppare comportamenti antisociali.

Phishing – truffa realizzata attraverso internet

- *Phishing*, (pescare) è un tipo di truffa ormai tra le più comuni ma ancora di grande diffusione.

- Il malcapitato riceve un mail con la quale gli si chiede, per motivi di sicurezza, di modificare i dati personali del suo conto corrente cliccando su un link che si trova sulla stessa mail.
- Il Mittente *(phisher)* spedisce una mail simulando l'identità di una banca. Se il destinatario ha un conto on line con quella banca è indotto a credere che si tratta di una richiesta lecita.
- Il link contenuto nella mail indirizza la vittima su un falso sito dove vengono registrati i dati che vengono abitualmente usati per accedere al proprio conto corrente.

- È necessario fare molta attenzione e ricordare che le informazioni riguardanti dati personali e/o password devono essere utilizzate solo sulle pagine preposte a tale scopo dal gestore del nostro conto corrente on line.

Frode informatica.

- Previsto dall'art. 10 della legge 547/93 che ha aggiunto l'art. 640 ter nel capo II del codice penale. 'Delitti contro il patrimonio'.
- "*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad essi pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 a 1549 euro se ricorre una delle circostanze previste dal secondo comma numero 1 dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore di sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante*"

- Questo reato si consuma con l'introduzione abusiva all'interno di un computer per ottenere un profitto illegale.

- Due casi tipici sono:

- Far confluire gli arrotondamenti degli interessi bancari sul conto del truffatore.
- Alterare il programma di una slot machine per ridurre la possibilità di vincita.

Accesso abusivo ad un sistema informatico.

- Previsto dall'art. 615 ter ed anch'esso introdotto dalla legge 547/93.
- *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
- *La pena è della reclusione da uno a cinque anni:*
- *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
- *se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*
- *se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*
- *Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque d'interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».*
- È compreso tra i reati contro l'inviolabilità del domicilio al capo III del titolo XII del codice penale, in quanto il sistema informatico viene considerato come il domicilio e pertanto tutelato dagli accessi non autorizzati o dal permanere in un sistema contro la volontà di chi ha il diritto di escluderlo.

Prevenzione e contrasto dei reati commessi sul web.

- È importante sapere che un **costante controllo** di ciò che viene pubblicato avviene da parte degli stessi **utenti della rete** i quali possono segnalare ai diversi gestori ciò che possa essere interpretato come reato.
- Inoltre la rete è continuamente monitorata dalla **polizia postale** per prevenire la quantità di reati che sempre più facilmente si pongono in essere in internet.
- A seguito della segnalazione e dell'accertamento di un reato da parte della Polizia postale viene trasmessa la **notizia di reato alla Procura della Repubblica** che dispone la richiesta di oscuramento della pubblicazione e/o l'acquisizione di maggiori informazioni utili per la prosecuzione delle indagini.

- Trattandosi di reati che viaggiano in rete in tempo reale anche la polizia di stato si è adeguata con la realizzazione del sito www.commissariatops.it dove è stato riprodotto un commissariato virtuale.

- Il sito presenta un ufficio virtuale che opera su 7 differenti aree tematiche:
- **sicurezza telematica, immigrazione, polizia amministrativa e sociale, concorsi, passaporti, minori e denunce.**

Prevenzione e contrasto dei reati commessi sul web.

- Trattando di reati informatici l'interesse cade su due aree tematiche, la **sicurezza telematica** e le **denunce.**

- **Sicurezza telematica**: dedicata a chi vuole approfondire argomenti attinenti a Internet e al mondo on line, o che si vuole tutelare dalle frodi informatiche. La Polizia di Stato dà consigli concreti su argomenti che vanno dall'hacking al phishing, dal commercio elettronico alle carte di credito e ai bancomat, dallo spamming (la posta "spazzatura" non richiesta) ai reati di pedofilia on line, dalla tutela del diritto d'autore alla telefonia in generale. A completare quest'area gli approfondimenti generali, il forum tematico, i moduli per la richiesta di informazioni su questi temi, per le segnalazioni e per la denuncia di reati telematici. Infine, le risposte aggiornate alle domande più frequenti e le news.

- **Denunce**: niente più code e tempi di percorrenza per arrivare al commissariato della vostra città perché la denuncia (per smarrimento o furto e per **i reati telematici**) la potrete fare **via web!** Sarà sufficiente collegarsi al sito della Polizia di Stato e seguire le istruzioni.

Denunce via web.

Solo successivamente, muniti del vostro numero di protocollo che vi fornirà il commissariato on line, andrete in un commissariato reale a formalizzare la denuncia, anche qui senza fare la fila: avrete diritto a una **"corsia preferenziale".**

- Con questo servizio viene dato ai cittadini uno strumento utilissimo per ricevere informazioni e difendersi dai reati informatici che viaggiando in rete possono creare danni in tempi molto brevi e quindi il commissariato virtuale diventa una risposta altrettanto veloce.