19-20 maggio 2006
Palazzo Vecchio - Firenze

Trusted Computing, traitor tracing, ERM e privacy

Avv. Giovanni Battista Gallus – Dott. Francesco Paolo Micozzi

Indice

- Nozioni: TC, traitor tracing ed ERM
- Il TC alla luce della normativa comunitaria e nazionale
- Il controllo a distanza dei lavoratori con i nuovi strumenti

Sciogliamo alcuni acronimi...

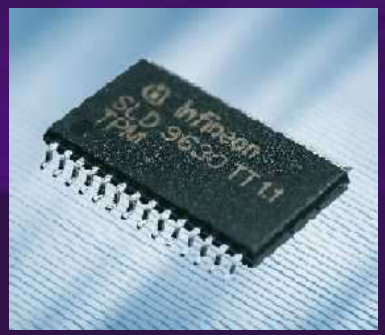
- TCG = Trusted Computing Group
- TPM = Trusted Platform Module
- CAs = Certification Authorities
- NGSCB = Next Generation Secure Computing Base (prima noto come Palladium) è il sistema composto da Nexus (kernel del SO deputato alla sicurezza) e dagli NCA.
- NCA = Nexus Computing Agents, sono i sw capaci di sfruttare le caratteristiche del kernel Nexus
- LT = Intel LaGrande Tecnology (Progetto che cerca di inglobare il TPM in una particolare CPU al fine di aumentarne le potenzialità in termini di sicurezza)

Sciogliamo alcuni acronimi...

- SEM (Presidio) = Security Execution Mode (progetto della AMD analogo a quello di LaGrande)
- EK = Endorsement Key - is a 2048-bit RSA key pair of which the private portion (PRIVEK) is stored in a shielded location inside the TPM, and the public portion (PUBEK) is available to the user and applications on the trusted computer.
- AIK = Attestation Identity Keys - Anonymous (do not contain information about the EK)
- DAA = Direct Anonymous Autentication

Alcuni cenni di natura tecnica: il Trusted Computing

- Il TCG (Trusted Computing Group) è un'alleanza tra Microsoft, IBM, Intel, HP, AMD e tanti altri, che si propone di creare una piattaforma che sia più sicura per l'utente finale.
  - Ogni singola applicazione di un sistema TC dovrebbe essere in grado di comunicare in tempo reale, in rete, lo stato del sistema, dei software in esso contenuti ed i documenti custoditi.



- Elemento centrale in un sistema NGSBC di TC è il Chip "Fritz". Questo, applicato alla MB, conserva le Endorsement Key una serie di chiavi private per la cifratura asimmetrica dei dati.

Alcuni cenni di natura tecnica: il Trusted Computing

L'ambiguità di una parola semplice: trusted.

- Per il TCG trusted significa fidato... ma non fidato per l'utente.
- Tale termine, sarebbe da intendersi come “fiducia tecnica”: uno strumento è fidato solo se si ha la certezza che si comporterà sempre nelle modalità richieste dagli scopi per il quale è stato ideato.
- Gli oppositori al TC invitano a diffidare da un sistema di cui sia oscuro ed indecifrabile il funzionamento: in questo caso non si dovrebbe concedere alcuna fiducia.

Alcuni cenni di natura tecnica: il Trusted Computing

- Le Endorsement Key sono una combinazione di chiavi RSA a 2048 bit che vengono impiantate in modo indelebile al momento della produzione del chip Fritz (o TPM).
- Questa coppia di chiavi identifica in modo univoco il sistema sul quale il chip è installato e, di conseguenza, anche il sw che "gira" in quel sistema.
- Il Fritz chip è stato pensato per scavalcare il problema dei sistemi di autenticazione basati solamente su software

Alcuni cenni di natura tecnica: il Trusted Computing

- Il Fritz chip, insomma, ha delle funzionalità crittografiche che permettono:
  - 1) di cifrare e decifrare al volo documenti e flussi di dati
  - 2) di firmare digitalmente, ed automaticamente, i documenti prodotti o modificati con quel sistema TC
- Se si riuscisse a disattivare il Fritz chip non si potrebbe, di conseguenza, avere accesso ai files precedentemente cifrati con esso.

Alcuni cenni di natura tecnica: il Trusted Computing

- Vi sono, inoltre, delle caratteristiche ulteriori che possiamo rinvenire in sistemi di tipo TC:
  - Una memoria a camere stagne (*Curtained Memory*) – (LaGrande)
  - Input/Output blindato (LaGrande)
  - Cifratura delle unità di memorizzazione legata al sistema (hw+sw) (*Sealed Storage*) – vedi sistemi di ERM
  - Attestazione remota – Un certificato digitale creato dall'hw comunica la fotografia del sistema (hw+sw) a chi ne faccia richiesta.

Alcuni cenni di natura tecnica: il Trusted Computing

- Principali funzionalità dell'architettura Trusted Computing

- 1. Memory curtaining
- 2. Secure input and output
- 3. Sealed storage
- 4. Remote attestation

Alcuni cenni di natura tecnica: il Trusted Computing

- Come sarà composto un sistema di tipo TC?
  - Da un BIOS in grado di gestire il chip TPM
  - Da un kernel di sicurezza (Nexus)
  - Da driver appositamente pensati per lavorare in ambiente TC
  - Da software capaci di sfruttare le funzionalità di un sistema TC (i cosiddetti NCA – Nexus Computing Agents)
- Con il TC si può fare in modo che solo la combinazione hw-sw certificata possa "girare" su una determinata macchina.

Alcuni cenni di natura tecnica: il Trusted Computing

- A questo punto:
  - "Chi produce il sistema operativo, si trova in una posizione superiore a chi crea il software applicativo;
  - Chi produce il BIOS, si trova in una posizione ancora più alta e può decidere quale sistema operativo può essere caricato.
  - Chi produce l'hardware si trova in una posizione ancora più alta e può decidere che BIOS può essere caricato.
  - Chi fa le leggi che vigono nel paese in cui viene prodotto l'hardware può controllare tutta questa catena di poteri."

(Alessandro Bottoni)

Alcuni cenni di natura tecnica: il Trusted Computing

- Ma allora perchè il singolo utente dovrebbe utilizzare i sistemi TC?
  - Chiave di forza per l'espansione delle tecnologie TC sarà, per il singolo utente, l'incremento delle barriere a difesa dei singoli dati. Una difesa... a tutti i costi.
- Scarsa pubblicizzazione degli altri aspetti legati al TC.

Alcuni cenni di natura tecnica: il Trusted Computing

- E' possibile disattivare il Fritz chip? e quali sono le conseguenze? (take ownership)
- E' possibile violare il Fritz chip?
- Quali conseguenze sulla interoperabilità dei software con il TC?
- Quale futuro per il software libero dopo l'introduzione dei sistemi TC?
  - E' in fase di studio il progetto OpenTC. Con questo sistema tutto il controllo (decisione sulle chiavi, firma di sw e driver, certificazione dell'hw) è preso dall'utente e non dal produttore. In questo caso il termine “trusted” assume un altro significato.

Alcuni cenni di natura tecnica: il Trusted Computing

- L'**Endorsement key** contenuta nel Fritz chip consente di associare ad un determinato sistema un determinato utente attivo.
- La **Remote attestation** è una funzionalità del TPM che permette ad un utente remoto, o ad un software gestito da remoto, di capire se il sistema è stato modificato rispetto al momento (solitamente al boot) in cui il sistema è stato identificato da un apposito hash.
- Con questi strumenti l'utente è costretto a "farsi riconoscere", perdendo così in parte il controllo sulla propria macchina.

Alcuni cenni di natura tecnica: il Trusted Computing

- La funzione di remote attestation, come tutte le altre è già implementabile via sw, ma con il TC diventa (o sembra diventare) pressoché inespugnabile
- The trusted computing architecture will not only protect data against intruders and viruses, but also against you.
- In effect, you, the computer owner, are treated as an adversary (Set Shoen)
- La prevalenza dell'UTONTO

Alcuni cenni di natura tecnica: il Trusted Computing

- L'Owner Override è un sistema che è stato pensato per far fronte alla perdita di controllo della macchina da parte dell'utente (Seth Schoen di EFF). *"L'owner override permette al proprietario del PC, quando fisicamente presente alla tastiera, di generare deliberatamente un attestato che non riflette la situazione corrente del PC, in modo da poter presentare all'interlocutore remoto una immagine di sua scelta riguardo al sistema operativo, ai driver ed al software applicativo in uso."*

Alcuni cenni di natura tecnica: il Trusted Computing

- L'owner override, tuttavia, non sarà applicato ai sistemi TC. A tal proposito una ricercatrice australiana, Catherine Flick, ritiene che l'owner override potrebbe comportare problemi maggiori di quelli che si propone di risolvere:
  - Perdita di sicurezza nel sistema;
  - Falso senso di sicurezza dell'utente sul sistema;
  - Perdita di efficacia per i sistemi DRM.

Alcuni cenni di natura tecnica: il Trusted Computing

- I sistemi di TC, apparentemente perfetti sotto il profilo della sicurezza, suscitano dei dubbi – quantomeno - sul rispetto delle norme sulla privacy, soprattutto se considerati in accoppiata con altri sistemi DRM (come l'ERM).
- Ross Anderson evidenzia la possibilità che i sistemi di tipo TC possano essere utilizzati per operazioni di censura da remoto.

Alcuni cenni di natura tecnica: il Trusted Computing

- Tali sistemi, inoltre, sono stati qualificati come "**double edged sword**" poichè si prestano ad espletare in tutta sicurezza anche attività antisociali ed illegali in genere.
- Gli stessi strumenti posti a tutela del sistema contro il malware possono essere utilizzati anche per impedire che un determinato sw (solo perchè, ad esempio, non è di gradimento della casa produttrice del chip) possa essere utilizzato su quello stesso sistema. Allo stesso modo potrebbe impedire all'utente di fruire di file multimediali non originali.

Alcuni cenni di natura tecnica: il Trusted Computing

- Considerato che il sistema di TC è un sistema "chiuso", quali problemi potrebbero sorgere in caso di elezioni politiche online, gambling online, transazioni finanziarie, VPN aziendali... ?
- Vale davvero la pena di rinunciare a diritti fondamentali, come può essere considerato quello alla riservatezza, per avere in cambio un sistema informatico esente (forse) da virus?
  - Ed, inoltre, siamo sicuri che il TC sia posto a tutela dei diritti dell'utente e non dei "digital rights" di alcune aziende?

TC e opt-in

- I sistemi TC dovrebbero prevedere la possibilità di disattivare i meccanismi di controllo
- Il loro utilizzo sembrerebbe quindi rimesso alla libera scelta dell'utente (i TC pc sarebbero comunque retrocompatibile)
  - In realtà, qualora il TC si diffondesse massicciamente, la possibilità di scelta diverrebbe illusoria. Con il TC disattivato, sarebbe impossibile accedere ai file criptati, oppure autenticarsi ai servers che richiedano appunto l'identificazione mediante TC
- Impossibilità di accedere ai file
- Impossibilità di lavorare, o anche solo di compiere, per esempio, operazioni di home banking

TC, anonimizzazione e controllo

Trusted Computing offers much in its arsenal for keeping data secure from tampering and unwanted viewing by third parties.

As well as being attractive to honest applications, its capabilities could be used by those wishing to keep their information secure due to the anti-social nature of that information. (Double Edged Sword... o triple?) - (C. Flick).

- Qual'è la risposta a questi problemi?

- Una backdoor per usi governativi, finalizzata al controllo delle attività illegali

TC, anonimizzazione e controllo

- Microsoft nel 2003 ha dichiarato che non inserirà mai volontariamente una back door in alcuno dei suoi prodotti, e si batterà attivamente per opporsi ad ogni obbligo di inserzione di una backdoor
- Il problema è proprio dato dalla "volontarietà"

Alcune opinioni sul TC

- Il Tc potrà avere successo soltanto a spese della privacy e della libertà di scelta del consumatore (Catherine Flick)
- Togliere il controllo del pc al suo proprietario è l'esatto opposto dell'originale “sogno” del personal computer, sogno sul quale la stessa Microsoft è stata fondata. Il rimuovere il controllo dell'utente riporta il “personal” computer ad essere un semplice terminale connesso al network di qualcun altro (Karl-Friedrich Lenz)
- Il TC dovrebbe essere ribattezzato “Treacherous Computing”, perchè è progettato per essere sicuri che il tuo computer ti disobbedisca sistematicamente” (Richard Stallman)

Alcuni cenni di natura tecnica: il Traitor Tracing

- Strumento già in uso da alcuni anni, ma che fa sorgere dei dubbi sul suo "privacy compliant" è il sistema di **traitor tracing**.
  - Ci si è forse ispirati alla figura di Emmanuel "primal traitor" Goldstein di 1984?
- Il traitor tracing è una forma di DRM che tende a legare indissolubilmente ed univocamente la creazione (o il download) o la modifica di ogni file protetto ad un soggetto determinato

Alcuni cenni di natura tecnica: il Traitor Tracing

Come si lega un soggetto ad una determinata copia di un file?
Pensiamo al caso dell'azienda che metta in commercio via internet un software X. E', certamente, possibile compiere queste operazioni interamente online. L'acquirente inserirà i suoi dati personali in apposito form sul sito del venditore e, quest'ultimo, invierà il codice di attivazione del prodotto scaricato.

Ovviamente l'azienda venditrice rilascia un solo codice per ogni utente... se la chiave di attivazione venisse, ad esempio, pubblicata su internet, l'azienda saprebbe facilmente a chi rivolgersi...

Alcuni cenni di natura tecnica: Enterprise Rights Management

- I software ERM vengono creati per rafforzare le protezioni all'accesso, utilizzo, stampa, etc di documenti interni ad un'impresa. Le possibili applicazioni sono svariate: dalle e-mail, ai manuali, dai documenti di ricerca ai progetti aziendali.
- Già oggi, con la sola cifratura di un documento aziendale, con il sistema a chiave pubblica, a chiave, cioè asimmetrica, è possibile mettere in campo un sistema di ERM a protezione dei dati.

Alcuni cenni di natura tecnica: Enterprise Rights Management

Con l'avvento del Trusted Computing anche i sistemi ed i sw di ERM saranno rafforzati. Si potranno imporre maggiori limiti sui files protetti con tali tecniche. Si potrà, ad esempio, fare in modo che una email inviata ad un dipendente si autodistrugga dopo un intervallo prefissato; si potrà impedire la stampa di un documento; si potrà impedire il semplice accesso al documento da parte di un soggetto estraneo all'azienda...

Alcuni cenni di natura tecnica: Enterprise Rights Management

- Ancora: si potrà impedire che un documento creato con un determinato software possa essere aperto con un sw diverso. Questo potrebbe costituire, in sostanza, un pericolo per tutta una serie di swhouse, o per il software libero.
- La caratteristica principale del sw di ERM è quella di creare differenti livelli di autorizzazione su un singolo file proprio per impedire a soggetti diversi dall'autore tutta una vasta serie di operazioni: dalla presa di visione alla stampa.

Privacy

Poste queste semplici premesse di tipo nozionistico sul TC, vediamo quale può essere l'impatto tra un siffatto sistema e la normativa comunitaria e nazionale sulla protezione della riservatezza.

Privacy

- Quali problemi giuridici può comportare un sistema di tipo TC?

1) Deve essere fornita un'informativa all'atto dell'acquisto di un sistema TC?
   E all'atto della registrazione dell'acquisto di un sw (per gli usi legati al sistema di traitor tracing)?
2) Quali diritti può esercitare l'utente? e nei confronti di chi? Chi è il rappresentante del titolare di cui all'art. 5 comma 2 d.lgs. 196/03?
3) Un italiano che si connetta ad un sito internet straniero può esercitare i diritti riconosciutigli dalla normativa italiana?

Privacy

- Art. 5 (D.lgs. 196/03) - Oggetto ed ambito di applicazione

- *1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.*
- *2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.*
- *3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.*

Privacy

- Quali problemi giuridici può comportare un sistema di tipo TC?

  4) Cosa accadrebbe nell'ipotesi in cui il sistema TC venisse inserito nell'all. B del d.lgs. 196/03, e quindi considerato una misura minima di sicurezza?

  5) Cosa accadrebbe, sul versante della responsabilità civile, a tutti quei soggetti che non utilizzassero una tecnologia TC una volta che questa fosse considerata misura idonea?

Privacy

- Quali problemi giuridici può comportare un sistema di tipo TC?

  6) In che rapporto si trova il limite di cui all'art. 4 L. 300/70 con un sistema di tipo TC?

  7) Se i controlli sui lavoratori sono eseguiti per conto del datore di lavoro da parte di terzi estranei all'azienda si avrebbe una violazione dell'art. 4 L. 300/70?
  Ed il datore di lavoro, in che posizione si trova rispetto alla normativa sulla privacy?

ERM e TPM: un connubio fatale?

- While DRM is not the only application for trusted computing, it certainly is one that could work much better in a trusted computing environment (Karl-Friedrich Lenz)
- La stessa affermazione è valida, senza dubbio, anche per i sistemi di ERM, o per il traitor tracing

Tracing e Data protection working party

- The tagging of a document should not be linked to an individual except if this link is necessary for the performance of the service or if the individual has been informed and has consented to it
- The Working Party is concerned about the fact that the legitimate use of technologies to protect works could be detrimental to the protection of personal data of individuals.
  - Working document on data protection issues related to intellectual property rights, January 18, 2005

TC, who is the owner?

- In addition, the concept of property is clearly part of the specifications for the Trusted Computing Platform Alliance (TCPA) and the Trusted Computing Group (TCG group) where the roles of users and administrators are clearly differentiated.
- It is administrators who are responsible for defining and limiting both the technical and practical rights of the users.
  - Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group) - ARTICLE 29 Data Protection Working Party

ERM, TC e lavoratori

- The TPM specifications make a distinction between the role of the owner and the role of the user.
- This distinction ... can raise some issues in corporate environments.
- In the corporate environment an individual worker would be the user while the employer would be the owner. He may take a number of decisions that affect the individual employee and the amount of data concerning the individual that is processed.

- The owner still has ultimate control and can decide whether to delegate certain key functions or not.
  - Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group) - ARTICLE 29 Data Protection Working Party

ERM e soppressione della corrispondenza

- Come sottolineato un sistema di ERM (soprattutto se implementato in un'architettura TC) consente il controllo totale e assoluto dei documenti
- La eventuale soppressione (o comunque il controllo) potrebbe configurare una violazione della corrispondenza?
- G.I.P. Milano, 10/5/2002
  - *L'uso dell'e-mail costituisce un semplice strumento aziendale a disposizione dell'utente lavoratore al solo fine di consentire al medesimo di svolgere la propria funzione aziendale e che, come tutti gli altri strumenti di lavoro forniti dal datore di lavoro, rimane nella completa disponibilità del medesimo senza alcuna limitazione*

Il controllo totale dei lavoratori

- Lavoro su sistemi TC
- Badge RFID che consentono anche l'identificazione della posizione del lavoratore
- Controllo nell'utilizzo del PC
- Controllo degli spostamenti
- Controllo delle telefonate
  - Incrocio dei dati
- Controllo totale e globale delle attività dei dipendenti

TC e Statuto dei Lavoratori

- art.4 L. 20.5.70, n.300 (Statuto dei Lavoratori)
  - Divieto di installazione di sistemi di controllo a distanza dell'attività dei lavoratori (art. 114 Codice privacy)
- art.8
  - Divieto di ogni indagine sui dipendenti che non sia strettamente attinente all'attività lavorativa (art. 113 Codice Privacy)

TC e Statuto dei Lavoratori

- ART. 4 - Impianti audiovisivi.
  - È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
  - Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna

TC e Statuto dei Lavoratori

- ART. 8. - Divieto di indagini sulle opinioni.
  - E' fatto divieto al datore di lavoro, al fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoro
  - Espressamente fatto salvo dall'art. 113 Codice Privacy
- Garante dati personali - Decisione 2 febbraio 2006
  - Proporzionalità nei controlli effettuati dal datore di lavoro
  - Artt. 3 - 11 Cod. Privacy

TC e Statuto dei Lavoratori

- Un controllo volontario e sistematico dell'attività dei dipendenti è sicuramente vietato
- Quali controlli sono ammissibili?
  - Quelli giustificati (o giustificabili...) sulla base di concrete esigenze produttive, organizzative e di sicurezza
- Il problema dell'uso degli strumenti aziendali
  - Non una forma di controllo, ma di disponibilità dei mezzi, che rimane nel controllo del datore di lavoro (who is the owner of TPM?)

Quali sono i controlli ammissibili?

- I controlli "difensivi"
  - *devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd.controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate*
  - *Cass. Sez. lavoro Sent. n. 4746/02*

    http://www.ictlex.net/index.php/2002/04/03/cass-sez-lavoro-sent-n-474602/
- TC come strumento di "controllo difensivo"?
- TC come misura di sicurezza?

TC e Statuto dei Lavoratori

- Tribunale di Milano 12 aprile 2005
  - dichiara antisindacale l'uso di un software che permetteva indirettamente il controllo a distanza dei lavoratori, senza che fosse stata concordata preventivamente con le rappresentanze sindacali la sua installazione
  - vieta l'utilizzo dei dati fino a quel momento raccolti mediante il suddetto sistema di controllo

TC e obbligo di notificazione al Garante

- Art. 37, lett. D Codice della Privacy
- Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
  - d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

TC e divieto di monitoraggio

- Art. 122 Codice Privacy
  - Informazioni raccolte nei riguardi dell'abbonato o dell'utente
  - Riguarda il trattamento di dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni
  - *Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.*

Dichiarazione di Montreux

- "La protezione dei dati personali e della privacy in un mondo globalizzato: un diritto universale che rispetta le diversità"
  - Le Autorità fanno appello ... ai produttori di hardware e software affinché sviluppino prodotti e sistemi che incorporino tecnologie per il potenziamento della privacy
  - L'appello sarà ascoltato?

In conclusione

- *«Nella vita di tutti giorni non siamo tenuti a portare un cartello con il nostro nome o a registrarci all'edicola quando comperiamo il giornale.*
- *Dovremmo pertanto poter decidere noi stessi quando vogliamo essere riconosciuti e quando no»*
  - Jürgen Bäumler
- Users should have the option to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service
  - Art. 29 Data Protection Working Party
- E se non fossimo più noi a poter decidere?

In conclusione

- *Solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*
  - Warren and Brandeis - "The Right to Privacy" - Harvard Law Review, Vol. IV December 15, 1890

    http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html

Domande?

Suggerimenti?

Obiezioni?

Critiche?

Insulti?

Avv. Giovanni Battista Gallus, LL.M.
Dottore di Ricerca
Studio Legale Gallus Cardia
g.gallus@studiogallus.it

Dr. Francesco Paolo Micozzi
Studio Legale Nati
f.micozzi@studionati.it