http://e-privacy.winstonsmith.org

eprivacy@winstonsmith.org

Il convegno è ad accesso libero e gratuito, ma i posti sono limitati. Si consiglia di effettuare un'iscrizione nominativa inviando una mail a segreteria@winstonsmith.org

PROGETTO WINSTON SMITH

e-privacy 2012

Privacy + Trasparenza

=

Libertà

PROGRAMMA

Milano, 21-22 GIUGNO 2012

Università degli Studi di Milano
Via Festa del Perdono, 3
20122 - Milano

Aula 400
III Piano
Facoltà
di Giurisprudenza

9:30 – 11:00

La privacy nella gestione delle fonti d'informazione critiche: whistleblowing, anonimato, Tor, GlobaLeaks

Chairman Marco Calamari

Claudio Agosti
Il whistleblowing non e' un fenomeno nuovo. In passato si lasciava una lettera dentro ad una cassetta delle lettere con su scritta la "soffiata". Negli anni questa pratica è cambiata, taluni nazioni la incentivano in quanto meccanismo di contrasto alle malversazioni, altre nazioni non hanno neppure una traduzione adeguata nella loro lingua: è il nostro caso. GlobaLeaks e' una tecnologia che permette di fare la cosiddetta "technologically driven whistleblowing", poiché garantisce la sicurezza di chi ha dati da segnalare, proteggendolo da eventuali ripercussioni. Questa tecnologia, che ha già raggiunto la fase di prototipo avanzato, ha suscitato interesse nel giornalismo investigativo, nelle aziende che si promuovono come trasparenti, nella vita cittadina e nella politica locale. L'intervento consiste in una panoramica del fenomeno, nella spiegazione del progetto software, nelle garanzie tecnologiche che mette a disposizione

Arturo Filastò
Tor e' un progetto che nasce con lo scopo di garantire comunicazioni anonime. Il diritto all'anonimato, però, e' qualcosa che spaventa molto i regimi, per questa ragioni molti hanno deciso di bloccarlo. A quel punto il progetto Tor ha iniziato a cercare di trovare modi per evitare di essere bloccato da un lato (i bridge) e altri per aggirare i sistemi di censura (obfsproxy). Verrà raccontata la storia di Tor ed il rapporto con il mondo della censura dal 2005 ad oggi. La presentazione si concluderà con una spiegazione di OONI, un progetto nato con l'intento di disegnare una mappa mondiale della censura di internet.

Fabio Pietrosanti
I Tor hidden service sono una tecnologia molto flessibile e con un grande potenziale, ma purtroppo non sono usati quanti dovrebbero. Danno la possibilità ad una persona di offrire un servizio TCP (HTTP, FTP, etc.) senza rivelare la sua identità o posizione fisica. Questo significa, in pratica, che posso mettere su un sito web senza dover registrare un dominio, un indirizzo IP o acquistare un virtual machine. Può persino funzionare su una DSL di casa perché non richiede che l'IP sia statico. La comunicazione tra client e server e' cifrata end-to-end e l'indirizzo che inserisco nel browser funge da autenticazione per la chiave pubblica dell'HS. Con servizi quali tor2web un HS può persino essere raggiungibile da persone che non utilizzano un client Tor. Tor2web sacrifica sicurezza e anonimato del client in cambio di usabilità.

Stefano Mele
La penetrazione sempre maggiore degli strumenti informatici all'interno del tessuto sociale, nonché la crescente delocalizzazione e concentrazione delle informazioni attraverso tecnologie distribuite e virtualizzate in Rete, rischiano di concedere inedite opportunità di controllo e spionaggio ben oltre i limiti imposti dalle normative nazionali e internazionali. La tutela dei diritti fondamentali e della privacy nelle attività investigative e di difesa nazionale nel cyber-spazio è divenuta pertanto un'esigenza imprescindibile, chiesta oggi a gran voce anche nei documenti strategici dei principali Paesi occidentali

Leonardo Maccari
La prossima "arab spring" verrà streammata su reti wireless mesh distribuite, finanziata in Bitcoin e condivisa su Diaspora. O forse no. E' possibile rendere distribuito qualsiasi servizio? ed è veramente più sicuro e più democratico? Partiamo dal sogno di una rete di accesso wireless distribuita per capire se è possibile "distribuire" tutto!

11:30 – 13:00

La privacy nelle città e nelle amministrazioni del futuro: smart cities, smart grids

Chairman Valerio E. Vertua

Yvette Agostini
La sinergia tra tecnologie dell'energia e quelle dell'informazione ha dato impulso al movimento smart: Smart cities, smart grid, smart appliance. Attraverso la disamina degli schemi tecnologici salienti attuali e prevedibili, si individuano i possibili rischi per la privacy connessi con la progressiva adozione a livello globale di queste tecnologie.

Valerio E. Vertua
Smart grid e smart appliance pongono delle problematiche per la privacy e per il trattamento dei dati di tutte le parti in causa: cittadini e fornitori di servizi. L'intervento ha quindi l'obiettivo di fare il punto della situazione sulla disciplina normativa vigente in Italia con uno sguardo a quella europea, cercando di individuare, se possibile, anche le possibili prospettive legislative future.

Roberto Leone
La rete di distribuzione elettrica del 21° secolo sta migrando verso il modello denominato Smart Grid. Queste nuove infrastrutture sono progettate per gestire in modo dinamico differenti tipi di centrali, fra cui quelle ad energie rinnovabili, che richiedono alla rete capacità di adattamento impossibili ai sistemi di distribuzione odierni.

Giulio Beltrami, Andrea Rudelli
Con la sperimentazione di un innovativo centro-contatti digitale, multimedia e multicanale, per l'ecosistema lombardo di Informatici Senza Frontiere, stiamo concependo un nuovo approccio "condominiale" alla e-privacy, in grado di prevenire gli abusi nelle telecomunicazioni, favorendo la collaborazione intra e inter associativa

14:00- 15:30

Privacy, e-government, open data e trasparenza

Chairman Nicola Lopane

Nicola Lopane, Pasquale Lopriore

L'importanza di utilizzare sistemi telematici per gestire gare d'appalto "e-procurement" è stata riconosciuta nel Piano d'Azione europeo di eGovernment 2011-2015 e nell'Agenda digitale italiana, in quanto l'e-procurement garantisce segretezza, trasparenza e affidabilità del procedimento, comportando un evidente risparmio di risorse sia economiche che umane. Per ottenere questi vantaggi occorre creare una piattaforma telematica che tenga conto di più aspetti di natura legale e informatica oltre a seguire i rigidi dettami propri delle procedure di gara d'appalto. Uno degli aspetti più delicati da curare è la gestione dei dati personali, poiché la piattaforma deve garantire alla stazione appaltante e alle ditte partecipanti adeguati livelli di segretezza e inviolabilità delle offerte. A tal proposito, per la gestione dei dati personali, il legislatore ha individuato come Responsabile del trattamento dei dati la figura "Gestore del sistema informatico" incaricata dalla stazione appaltante di gestire il funzionamento delle procedure telematiche assumendone la relativa responsabilità. Il Gestore del sistema, pertanto, deve adottare una apposita policy sulla privacy che analizzi tutti gli aspetti tipici di una procedura di gara, prevedendo piani di disaster recovery. Per la realizzazione della piattaforma di e-procurement della Regione Puglia "EmPULIA" sono state prese in considerazione tutte queste problematiche redigendo una apposita disciplina di utilizzo, approvata dagli utenti, nella quale si regolamenta le procedure telematiche utilizzate e il ruolo dei soggetti coinvolti.

Morena Ragone

Quali sono gli strumenti che le amministrazioni possono utilizzare per favorire la costruzione del governo aperto? L'esame si sofferma sulla 'rivoluzione open data', nonché sull'uso e funzione dei social network nel rapporto tra amministrazione e cittadino. Non si mancherà di evidenziare alcuni profili di criticità della trasparenza in rapporto alla privacy, ma, anche e soprattutto, della necessaria alfabetizzazione da cui nessuno può prescindere.

Alessandro Rodolfi

Partendo da un interessante studio di Barbara Coccagna, dottore di ricerca presso Università degli Studi di Teramo, dal titolo "Monitoraggio collaborativo e democratizzazione dell'informazione di fonte pubblica" saranno approfonditi gli aspetti relativi alla riservatezza dei soggetti che segnalano brogli elettorali, corruzione, reati e illeciti a qualsiasi livello (locale, nazionale, sovranazionale) evidenziando inoltre le possibili connessioni con l'Open Data e l'Open Government.

16:00 – 19:00

Privacy, Computer Forensics e Crimini Informatici

Chairman Marco Calamari

Corrado Giustozzi

I recenti casi di attacchi alle Certification Authorities hanno messo in luce la fragilità della catena di fiducia in Rete. Le infrastrutture critiche non sono solo quelle da cui dipende il funzionamento della Rete: il vero punto debole sono i servizi da cui dipende la Rete stessa.

Roberto Flor, Stefano Marcolini, Eleonora Colombo

Dall'evoluzione della giurisprudenza costituzionale di molti Stati europei, della Corte di Giustizia dell'Unione europea e, seppur in modo minore, della giurisprudenza italiana, in casi aventi ad oggetto misure di contrasto, anche tecnologiche, alla criminalità, si può ricavare la nascita di nuove forme di manifestazione del diritto generale della personalità in Internet: il diritto all'autodeterminazione informativa ed il diritto alla riservatezza, all'integrità ed alla sicurezza di dati e sistemi informatici. L'esigenza di tutela di questi "nuovi" diritti fondamentali deve confrontarsi con la necessità di contrastare forme gravi e transnazionali di fenomeni criminosi. Il bilanciamento di questi interessi contrapposti deve avvenire tenendo conto nelle nuove competenze penali dell'Unione europea dopo l'entrata in vigore del Trattato di Lisbona.

Mattia Epifani

Il costante aumento nell'utilizzo dei sistemi di cloud computing ha introdotto nuove questioni e problemi in relazione all'analisi forense dei dati. Le tradizionali tecniche di acquisizione non sono più utilizzabili in questi contesti ed è quindi necessario definire metodi alternativi e dedicati. Tra i servizi di Cloud Computing particolare diffusione e successo sta riscuotendo iCloud di Apple, per la possibilità di condividere le informazioni in automatico su strumenti di diverso tipo (Mac o PC, iPhone, iPod, ecc.).

Ulrico Bardari

Premessi i principali reati commessi in Internet e l'inadeguatezza degli strumenti messi a disposizione degli organi preposti al contrasto del cibercrimine, si intende argomentare l'importanza di un data retention adeguatamente disciplinato al fine di tutelare la proprietà del dato trattato e allo stesso tempo consentire un margine d'intervento puntuale all'autorità giudiziaria in caso di incidente informatico. Si prendono in considerazione le divergenze che scaturiscono tra la necessità di tutelare la riservatezza delle comunicazioni e l'obbligo dell'azione penale per la tutela delle vittime di reati informatici o perpetrati a mezzo informatico.

Nicla Diomede, Donato la Muscatella, Marco Spada

L'intervento analizza gli aspetti tecnici della raccolta dei dati sul traffico e le implicazioni giuridiche relative alle protezione dei dati personali di utenti e lavoratori che utilizzano l'infrastruttura dei poli Universitari, anche in relazione alle richieste investigative provenienti dall'Autorità Giudiziaria

Federica Mingotti

Nel 2008 gli adempimenti nell'ambito della compliance aziendale sono stati estesi all'area dei reati informatici. All'art. 24 bis del D.lgs. 231/01 sono previsti quali reati presupposto, inter alia, il falso in documenti informatici, l'accesso abusivo al sistema informatico, l'intercettazione, impedimento, interruzione di comunicazioni informatiche, il danneggiamento di informazioni, dati e programmi informatici, la frode informatica del soggetto che presta servizi di certificazione di firma elettronica. L' inserimento del pacchetto "reati informatici" richiede la creazione di sistemi di controllo di prevenzione in tutte le aree di rischio, dalla direzione, alle HR passando per il marketing, le vendite, gli acquisti e la sicurezza informatica. Si tratterà quindi innanzitutto di procedere all'esecuzione di mappature delle aree a rischio e, in secondo luogo, sarà necessario stendere dei protocolli di prevenzione quali la definizione di deleghe responsabilità e poteri connessi, rendere procedurali le attività informatiche e ancora identificare l'Organismo di Vigilanza a cui è demandato il compito di rapportarsi periodicamente per i test di verifica e controllo. In terza analisi tra le best practice si annovera l'opportunità di prevedere un codice etico ove dichiarare i valori e principi per l'uso dell'informatica aziendale, la gestione delle credenziali d'accesso, l'accessibilità stessa ai sistemi clienti, fornitori, oltre alla gestione dei dati riservati e sensibili. Si tratta di interventi che per altro richiedono uno stretto coordinamento con la compliance relativa alla privacy (D.lgs. 196/2003), con la quale collimano e si intersecano. Non a caso si registra spesso la richiesta ai professionisti lato privacy di curare anche l'aspetto della 231/ 01 inerente ai reati informatici. Richiesta che testimonia ancora una volta il peso specifico e il ruolo centrale riconosciuto al diritto acclamato a gran voce da ogni angolo nell'epoca dell'informatizzazione: il diritto alla privacy. Tanto invocato nella sua immanenza quanto sfuggente nell'elefantiasi procedurale che gli fa da strascico e che sembra volerci tutti quanti più di ogni altra cosa ... "proceduristi"!!!

09:30 – 11:00

Privacy, poteri di controllo e nuove frontiere

Chairman Giovanni Ziccardi

Italo Cerno

Le informazioni attinenti la propria sfera privata vengono sempre più frequentemente barattate con le "utilità" fornite dai prestatori dei «servizi della società dell'informazione». I dati attinenti il comportamento tenuto in Rete vengono da questi ultimi raccolti ed elaborati non solo e non tanto al fine di migliorare i servizi offerti, ma anche per proporre pubblicità "mirata" ovvero vicina ai gusti, alle preferenze ed alle necessità degli utenti (c.d. on-line behavioural advertising). A partire dal marzo di quest'anno, la società Google ha reso unica la propria informativa privacy ed integrato i propri servizi: questi sono strettamente collegati tra loro in ragione dell'uso che l'utente fa anche solo di uno di essi. L'obiettivo dichiarato è quello di "personalizzare" i risultati, ma i profili degli utenti vengono adoperati anche allo scopo di propinare pubblicità mirata. Emergono, pertanto, criticità in ordine alla trasparenza dell'attività di raccolta dati, alla consapevolezza del soggetto interessato ed alle modalità con cui viene espresso il consenso. Il sistema adoperato è quello dell'opt-out, ovvero, è il singolo utente a dover manifestare la propria volontà di non essere monitorato e non il contrario come, invece, imporrebbe la normativa, europea ed italiana, in materia di protezione dei dati personali. Scopo dell'intervento è quello di evidenziare le principali problematicità dell'attività posta in essere dalla società Google alla luce delle norme applicabili alla pubblicità "comportamentale" e dei pareri espressi al riguardo dal Gruppo di lavoro ex art. 29 sulla protezione dei dati personali.

Alessio Pennasilico

Cercheremo di affrontare il tema della sicurezza del cloud computing partendo da alcuni casi di cronaca recente. Analizzeremo in particolare il caso delle chiusura di MegaUpload e di tutti i fatti correlati, per raccontare cosa =E8 accaduto davvero la notte del 19 gennaio 2012, partendo dal Governo degli Stati Uniti D'America, per arrivare in Europa, passando da Anonymous, 2600, il CCC, l'FBI e la sicurezza dei nostri dati.

Alberto Cammozzo

Il riconoscimento facciale automatico è una tecnologia matura e in ampia diffusione. La faccia è qualcosa che non possiamo cambiare e che difficilmente si nasconde in pubblico: perciò l'impiego di queste tecnologie solleva molti problemi etici legati alla privacy e ai diritti umani. Nel 2011 si è parlato delle tecnologie di Face Recognition nei social networks, ma il 2012 ne vede il silenzioso ed ubiquitario consolidamento: come tecnologie di sicurezza (autenticazione utenti, borders processing, identificazione di sospetti, lotta alle frodi, sorveglianza "face in the crowd", controllo presenze ed accessi), in ambito commerciale (digital out-of-home advertising, fidelizzazione,controllo dell'età), fino ai motivi più frivoli (smile-activated vending machines, identificazione dei personaggi ritratti in quadri antichi) ma anche militari (target identification, anche nei droni). Nei prossimi anni le migliori implementazioni di queste tecnologie si consolideranno e diverranno interoperabili: dalla webcam, al videocitofono, al televisore fino alla telecamera di sorveglianza. In aggiunta recenti ricerche hanno messo in evidenza la fattibilità delle re-identificazione massiccia attraverso i volti (Accorsi 2011). Quali sono le risposte pubbliche, tecnologiche e sociali al dilagare di queste tecnologie invasive e potenzialmente pericolose? Il dibattito pubblico sull'eticità dell'impiego di queste tecnologie, sulla loro responsabilità alle dittature e sul rispetto della privacy è quasi assente. Le istituzioni appena cominciano a prendere in considerazione il problema: in UE il WP Art29 (opinione 2/2012) e la FTC in USA (Dec 2011). La ricerca tecnologica su implementazioni di riconoscimento facciale che rispondano a criteri di privacy-by-design non abbonda, tuttavia vi sono risposte "dal basso" che propongono svariate Privacy Enhancing Techniques (di efficacia non sempre testata) per ripristinare la visual privacy

11.30-12.00

Premiazione Big Brother Award

http://bba.winstonsmith.org

12:00 – 13:00

Il delicato rapporto tra privacy e diritto

Chairman Simone Onofri

Simone Bonavita

Conoscere a che fine sono destinati i propri dati è fulcro della libertà di autodeterminazione informativa, in un'ottima di totale trasparenza e tutela delle libertà digitali. A tal riguardo il Codice della Privacy ha previsto che, prima della prestazione del consenso, debba essere resa una informativa contenente informazioni idonee a fondare la consapevolezza del consenso stesso. Detta disposizione trova tuttavia limiti nel territorio delle nuove tecnologie. Nel Web accade così, nella migliore delle ipotesi, di impattare in lunghe e dettagliate informative conformi alla Legge, ma non alle regole non codificate della Rete, che stabiliscono immediatezza nella trasmissione dell'informazione. Ma, ancora prima, i titolari del trattamento sono effettivamente edotti dei dati che trattano nel Web, anche mediante l'utilizzo di cookie e di nuove tecnologie? E le informative che questi rendono, prevedono indicazioni in merito? In quest'ottica diviene
interessante procedere ad una analisi di questi aspetti, anche alla luce della direttiva 2009/136/CE e delle modifiche recentemente proposte in tema di cookie ed altre analoghe tecnologie.

Giovanni Battista Gallus, Ernesto Belisario, Francesco Paolo Micozzi

Il right to be forgotten ha assunto una dimensione nuova e centrale nel corretto trattamento dei dati personali. Le problematiche connesse al diritto all'oblio hanno già avuto modo di essere più volte affrontate nelle aule giudiziarie e nella "giurisprudenza" del Garante: la tensione tra le pretese dell'individuo e la ricostruzione storica e la libertà d'informazione dovrà trovare un nuovo equilibrio, anche alla luce del Regolamento comunitario di prossima approvazione. In questo quadro, già complesso, sono intervenute le plurime novità legislative che hanno reso obbligatoria la pubblicazione di atti online da parte delle Pubbliche Amministrazioni, con una non sempre facile fare sintesi tra esigenze di trasparenza e diritti dei singoli. L'intervento cercherà di affrontare l'argomento nella triplice chiave di lettura, civilistica (e delle libertà costituzionali), penalistica e amministrativistica.

14.30-15.00

Corso "Cittadinanza digitale e Tecnocivismo"

Andrea Trentini

Quest'anno per la prima volta abbiamo provato a somministrare contenuti di "awareness digitale" nel contesto "essere cittadini". Abbiamo trattato tutte le implicazioni (a volte positive e a volte negative) della tecnologia informatica nella relazione cittadino-istituzioni. A fine corso gli studenti hanno approfondito alcuni temi come prova d'esame.

15:00 – 19:00

Privacy, diritti umani e diritto all'oblio

Chairman Pierluigi Perri

Marco Bettoni

Le imprese tecnologiche americane ed europee riforniscono i regimi autoritari di tutto il mondo degli strumenti e delle tecnologie utilizzate per attività di controllo, sorveglianza e repressione dei diritti umani nei propri paesi. Criticità del fenomeno, in continua espansione, dal punto di vista del diritto e della politica.

Cesare Maioli, Elisa Sanguedolce

Partendo da alcune problematiche della governance di Internet, si evidenzia la opportunità di includere nel tema gli aspetti etici che valorizzano la ricostruzione dei diritti civili con riferimento alla privacy. Si considerano le raccomandazione internazionali e si fornisce un contributo alla definizione di un nuovo quadro di riferimento.

Monica Senor, Carlo Blengino

Dove si colloca il diritto all'oblio, tra diritto alla privacy, diritto alla protezione dei dati e diritto all'identità?
Esiste un diritto di sequela sui dati personali, una specie di copyright, o meglio di diritto morale d'autore sulle informazioni che ci riguardano?

Alessandro Mantelero

Il tema dei dati aperti, ove concerna informazioni di carattere personale, implica il necessario contemperamento delle esigenze di divulgazione e ri-uso dei dati con quelle di autodeterminazione informativa dei singoli. Il tale prospettiva si sono orientati tanto il legislatore comunitario che quello nazionale. Alla luce della recente proposta di riforma della disciplina europea sui dati personali occorre dunque valutare quali spazi siano lasciati dalle nuove norme alla divulgazione dei dati ed al ri-uso degli stessi. Con riguardo al primo profilo (accessibilità e divulgazione dei dati) bisogna porre attenzione alle modalità di rilascio, onde evitare che si traducano nella pubblicazione di grandi quantità di dati personali in maniera non conforme alle finalità che autorizzano le amministrazioni pubbliche al trattamento. In merito al ri-uso bisogna invece focalizzare l'attenzione sulla compatibilità fra le finalità iniziali della raccolta e le eventuali modalità di ri-uso, valutando sia i profili inerenti la pertinenza, che l'informativa, che la gestione del ri-uso mediante le licenze.

Nicola Gargano

L'avvento del processo telematico ha sicuramente rivoluzionato il rapporto tra gli operatori del mondo giustizia, tanto nell'approvvigionamento di informazioni quanto nella comunicazione tra avvocato e ufficio. Tuttavia, solo in alcuni casi, la quantità di informazioni disponibili nella rete giustizia veniva resa accessibile al cittadino che, fino ad oggi, non può prescindere dall'interfacciarsi con il proprio legale per conoscere, ad esempio, lo stato di un procedimento. Dal 18 maggio 2012, invece, l'enorme quantità di dati giudiziari finora accessibili tramite i punti di accesso solo alle parti del processo regolarmente costituite e dotate di sistemi di autenticazione forte, diviene disponibile in forma anonima per tutti grazie al portale dei servizi telematici di cui all'art. 6 del DM 44/2011. Il processo telematico dunque, non sarà più riservato agli addetti ai lavori ma sarà una realtà con la quale dovrà fare i conti anche il cittadino che, provvisto di un indirizzo PEC, potrà ricevere notifiche di atti giudiziari in forma elettronica e, prima di rivolgersi al proprio legale potrà acquisire informazioni mediante un portale accessibile non solo agli addetti ai lavori. Una rivoluzione tuttavia non esente da problematiche. Quanto è tutelata la privacy del cittadino? L'avvocato sarà costantemente sottoposto al controllo da parte del cliente che potrà controllare da solo le vicende della causa di cui è parte e non?

Monica Gobbato

L'intervento avrà ad oggetto le dinamiche dei principali social network come Facebook, Twitter, Badoo e Foursquare con particolare riferimento al fenomeno della geolocalizzazione, evidenziandone le possibili insidie. Verranno esaminate le modalità con cui i Titolari di questi siti (?) informano l'interessato riguardo ai propri servizi e se e in che modo gli stessi adempiono o meno agli obblighi privacy in tema di geolocalizzazione. Si esamineranno anche i recenti casi portati innanzi all'Autorità Garante della Protezione dei dati Personali. Si descriveranno poi i rischi effettivi che un interessato corre nel momento in cui si affida a tali tecnologie, soprattutto quando utilizza smartphone, tablet o PC di ultima generazione. Si tenterà infine di offrire qualche spunto di riflessione a quei titolari che comprendono l'importanza di mettersi in regola alla luce dei Pareri e degli Studi forniti sull'argomento dai Garanti europei in tema di geolocalizzazione. Potrà il riconoscimento del diritto all'oblio ostacolare l'era dei big data?