GHISLIERI
IL COLLEGIO

Centro per la Comunicazione e la Ricerca
Area 'Diritto e Informatica'

Dipartimento di Giurisprudenza

Corso a.a. 2018-19
di Informatica e logica giuridica

CONVEGNO ANNUALE DI INFORMATICA GIURIDICA

Venerdì 23 novembre 2018 - Aula Magna del Collegio Ghislieri

LA TALPA COL FISCHIETTO

(DAL 'WHISTLEBLOWING' (L.179/2017) AI 'CAPTATORI INFORMATICI' (D.LGS. 216/2017): ASPETTI E PROBLEMI TECNICO-GIURIDICI)

PROGRAMMA DI SALA

---

ore 9:30 Benvenuto del Direttore del Dipartimento di Giurisprudenza prof. Cristina CAMPIGLIO

ore 9:45 Presentazione del Convegno prof. Romano ONEDA

ore 10:00 "DAL FISCHIO ALL'ASCOLTO"

prof. Corrado GIUSTOZZI

(Esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, componente del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), membro del Consiglio direttivo di Clusit. Docente presso varie Università sui temi della cybersecurity e della criminalità informatica, è componente del Comitato Scientifico dell'Area di Diritto e Informatica del Collegio Ghislieri)

Nell'eterna rincorsa tra "buoni" e "cattivi" non è inusuale vedere gli uni adottare metodi degli altri e viceversa. Il problema semmai è identificare chi è il "buono" e chi è il "cattivo", visto che generalmente si considera che la tecnologia sia neutra in sé mentre la differenza, sul piano etico e legale, la facciano il modo in cui essa viene impiegata e gli obiettivi che tramite tale impiego si intende perseguire. Al giorno d'oggi la crittografia può proteggere l'identità e l'incolumità di chi in buona fede vuole denunciare pratiche o azioni illecite, ma viene anche usata da criminali e terroristi per eludere le forze dell'ordine sottraendo loro informazioni o conversazioni essenziali per le indagini; e viceversa, le forze dell'ordine possono utilizzare strumenti informatici d'attacco, tecnicamente indistinguibili dai malware usati da spie e sabotatori, per eludere le misure di protezione messe in atto dai criminali e raccogliere attività o comunicazioni atte a incriminarli.

---

ore 10:00 "PER UN'ETICA PUBBLICA DEL WHISTLEBLOWING: TRA EMERGENZE E BUONE PRATICHE"

prof. Michele BOCCHIOLA

(Assegnista di ricerca presso il Dipartimento di Scienze Politiche e Sociali dell'Università di Pavia. Si

occupa di filosofia politica contemporanea e, in particolare, del fenomeno della corruzione politica e delle politiche anti-corruzione. Tra le più recenti pubblicazioni, è autore, con Emanuela Ceva, di Is Whistleblowing a Duty? per Polity Press)

Il whistleblowing *è «la pratica attraverso cui un membro di un'organizzazione legittima segnala volontariamente alcune azioni illecite, che si presume siano avvenute all'interno di tale organizzazione, con l'intenzione di intraprendere azioni correttive per affrontarle» (Ceva & Bocchiola,* Is Whistleblowing a Duty*?, Polity Press 2018). Lasciato ai margini del dibattito filosofico per molto tempo, dopo il clamore delle intricate vicissitudini di personaggi come Edward Snowden e Chelsea Manning, si è iniziato a riconoscere l'importanza del* whistleblowing*, con particolare riferimento alla sua funzione nella responsabilità sociale di impresa e nella lotta alla corruzione. Questo saggio fornisce un'analisi critica delle principali teorie del* whistleblowing *nella filosofia politica contemporanea.*

---

ore 11: "WHISTLEBLOWINGPA, PIATTAFORMA DI WHISTLEBLOWING PER LA PUBBLICA AMMINISTRAZIONE"

ing. Yvette AGOSTINI

(Consulente indipendente, è cultore di Informatica giuridica presso UniMI, collabora con il Centro Hermes per la trasparenza e i Diritti digitali sin dalla sua fondazione)

La legge n.179/2017 che disciplina il whistleblowing *ha introdotto tra gli obblighi per le PA di utilizzare modalità anche informatiche e il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione. L'adempimento di questi obblighi può essere oneroso per le PA più piccole; per ovviare a questo,* Transparency *International Italia e Hermes Center hanno unito gli sforzi realizzando la piattaforma WhistleblowingPA, basata sul* software *GlobaLeaks e con questionario realizzato da Transparency International Italia, che mette a disposizione per tutte le PA una istanza gratuita del software per la raccolta delle segnalazioni a norma di legge. Razionali del progetto, primissime considerazioni a valle del lancio dell'iniziativa.*

---

ore 11:30 "IL SISTEMA DELL'ATENEO PAVESE: IL RAPPORTO E L'INTEGRAZIONE TRA WHISTLEBLOWING, SURVEY ANTICORRUZIONE, TRASPARENZA E ACCESSO CIVICO"

dott. Loretta BERSANI

(Dirigente Università degli Studi di Pavia, responsabile dell'Area Risorse Umane e Finanziarie, Vice Direttore Generale Vicario e Responsabile per l'Ateneo della prevenzione della corruzione e della trasparenza)

Nella consapevolezza che ogni strategia di prevenzione della corruzione non può non considerare l'istituzione di canali per la comunicazione di eventuali illeciti, il sistema dell'Ateneo Pavese, in aderenza alla legge, ha attivato una piattaforma per il whistleblowing*. Inoltre, si è inteso attivare un ulteriore canale per permettere all'Amministrazione di rilevare le opinioni dei dipendenti e degli studenti, mediante la proposta di una* survey *annuale. Scopo di tale* survey*, che si integra con i processi esistenti relativi alla trasparenza e all'accesso civico, è quello di integrare le criticità di un istituto, come quello del* whistleblowing*, che non è ancora riuscito ad esprimere tutte le sue potenzialità.*

---

ore 12 "IL WHISTLEBLOWING PRIMA DELLA LEGGE 179/2017: GLI OBBLIGHI PER LE BANCHE"

prof. Riccardo COLANGELO

(Cultore di Informatica e logica giuridica e Informatica giuridica presso il Dipartimento di giurisprudenza dell'Università degli Studi di Pavia, è professore a contratto di Elementi di diritto e Sistemi di elaborazione delle informazioni presso il medesimo ateneo. È inoltre iscritto all'albo nazionale delle eccellenze ed attivo quale formatore di dirigenti scolastici, docenti e personale amministrativo, in particolare in materia di amministrazione digitale, protezione dei dati personali, cyberbullismo e uso consapevole della Rete)

L'intervento conclusivo della sessione mattutina dedicata al whistleblowing intende completare lo sguardo d'insieme sulla disciplina ad oggi vigente desumibile da quanto affermato dai precedenti relatori, mettendo in luce quanto il legislatore italiano ha statuito in materia prima della legge 179/2017. Infatti il whistleblowing - così come, mutatis mutandis, la notifica della violazione dei dati ("data breach"), cui fanno riferimento gli artt. 33 e 34 GDPR - non è una novità assoluta per il nostro ordinamento giuridico, che già faceva ad esso espresso riferimento nell'ambito di particolari settori, quali quello bancario.

---

ore 14.30 "TROJAN HORSE: ASPETTI PROCESSUALI PENALI"

prof. Silvia SIGNORATO

(Ph.D., è ricercatore di diritto processuale penale nell'Università degli Studi di Padova. È esperta di indagini penali informatiche)

Il d.lgs. 29 dicembre 2017, n. 216 ha previsto espressamente l'utilizzo del captatore informatico quale mezzo di ricerca della prova in sede di indagine penale. Al riguardo, molto è stato scritto e detto. Per orientarsi in materia occorre però interrogarsi sulla nozione giuridica riferibile al concetto di captatore informatico, sui presupposti che legittimano il ricorso ad esso e sulle regole che presiedono al suo utilizzo.

---

ore 15 "TIMEO DANAOS ET DONA FERENTES. I 'CAVALLI' DI STATO FRA PERVASIVITÀ STRUMENTALE E PERSUASIVITÀ NORMATIVA"

dott. Federica BERTONI

(Informatico Forense, certificata CIFI, collabora con le Cattedre d'Informatica Giuridica delle Università di Brescia e Pavia ed è Affiliate Scholar dell'Information Society Law Center dell'Università degli Studi di Milano diretto dal Prof. Giovanni Ziccardi. È membro del Capitolo italiano di IISFA e socia e docente CLUSIT, l'Associazione Italiana per la Sicurezza informatica. Dal 2003 è autrice e coautrice di diverse pubblicazioni in materia di Sicurezza informatica, Diritto dell'Informatica e delle Nuove Tecnologie, Informatica Forense)

Forse mai prima d'ora, nel nostro Paese, si era realizzato così concretamente quel doppio ordine di effetti, benevoli e malevoli insieme, che solo la legge e la tecnologia sanno fare quando si ritrovano impastate dalle mani del legislatore. E ciò è avvenuto con il d.lgs. 216 del 2017. Tuttavia, come non tutte le ciambelle riescono col buco, così questa riforma non convince: difetta infatti di quegli ingredienti essenziali perché l'uso della potenzialità tecnologica insita nello strumento informatico che s'intende normare non sfoci nell'abuso dello stesso, con conseguente calpestamento dei diritti costituzionalmente garantiti. Perché il rischio è quello di scoprire troppo tardi che il trojan di Stato era, in realtà, la legge e non il captatore informatico.

---

ore 15.30 "POICHÉ NULLA VI È DI NASCOSTO CHE NON SARÀ DISVELATO" (LA SOCIOLOGIA DEI CAPTATORI INFORMATICI)

prof. Antonio BARILI

(Docente di Sicurezza Informatica e responsabile del Laboratorio di Informatica Forense presso il Dipartimento di Ingegneria Industriale e dell'Informazione dell'Università degli Studi di Pavia)

I captatori informatici catalizzano una perfetta sintesi tra tecnologia avanzata, diritto e ansie sociali. Di questi tre elementi, quello tecnologico è forse il meno compreso. Un approfondimento in questo senso, pur non avendo la pretesa di gettare luce sulle questioni di diritto, potrebbe contribuire ad attenuare le ansie sociali che circondano questi strumenti.

---

ore 16 "DA UN GRANDE POTERE DERIVANO GRANDI SECCATURE"

isp. Davide "Rebus" GABRINI

(Davide Gabrini, più noto come Rebus, si occupa di criminalità informatica dal secolo scorso; ha lunghi trascorsi nella Polizia delle Comunicazioni e un futuro nella Polizia Scientifica. Collabora con il Laboratorio di Informatica Forense dell'Università di Pavia)

Le intercettazioni ambientali, consolidato strumento nella pratica di Polizia Giudiziaria, si sono arricchite negli ultimi decenni di nuove interessanti opportunità, legate alla progressiva pervasività delle tecnologie digitali. Tuttavia, la crescente complessità della tecnologia ha aumentato proporzionalmente, insieme al potenziale investigativo, anche la difficoltà di applicare realmente e con successo le soluzioni teoricamente disponibili. Le limitazioni degli spyware e dei dispositivi target in fatto di funzionalità, installazione ed efficienza spingono a ricercare soluzioni alternative, spesso ricorrendo a quella sorta di auto-spionaggio che gli utenti attuano nel circondarsi di dispositivi "intelligenti" e di rassicuranti servizi ubiqui.

---

ore 16:30 Interventi del pubblico e discussione