DIPARTIMENTO DI SCIENZE GIURIDICHE - CIRSFID
ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA

Corso di Informatica Forense a.a. 2020-2021

Modulo di Fondamenti giuridici dell'Informatica forense

Avv. Antonio GAMMAROTA, Ph.D.,
Professore a contratto, modulo " Fondamenti giuridici dell'informatica forense"
DSG, CIRSFID

Alma Mater Studiorum – Università di Bologna
antonio.gammarota@unibo.it
avvocato@gammarota.it

© 2020 Materiale didattico per uso esclusivamente personale. Ogni diritto resta riservato all'autore

1. I Limiti del diritto in tema di prova digitale

DICHIARAZIONE UNIVERSALE DEI DIRITTI DELL'UOMO (1948)
Articolo 10
CONVENZIONE EUROPEA DIRITTI DELL'UOMO (1950)
Art. 6 Diritto a un equo processo
CARTA DI NIZZA (2000)
CAPO VI – GIUSTIZIA

COSTITUZIONE DELLA REPUBBLICA ITALIANA
Art. 111 (modificato da art. 1 L. cost. 23.11.1999, n. 29)

Codice di procedura penale

Principi generali di informatica e sicurezza dei dati

1. I Limiti del diritto in tema di prova digitale

Dichiarazione Universale dei Diritti dell'uomo (1948)

Articolo 10

Ogni individuo ha diritto, in posizione di piena uguaglianza, ad una equa e pubblica udienza davanti ad un tribunale indipendente e imparziale, al fine della determinazione dei suoi diritti e dei suoi doveri, nonché della fondatezza di ogni accusa penale che gli venga rivolta.

1. I Limiti del diritto in tema di prova digitale

Convenzione Europea Diritti dell'Uomo (1950)

Art. 6 Diritto a un equo processo

1. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia.

2. Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata **legalmente** accertata.

3. In particolare, ogni accusato ha diritto di:

(a) essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della natura e dei motivi dell'accusa formulata a suo carico;

(b) **disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa;**

(c) **difendersi personalmente o avere l'assistenza di un difensore di sua scelta** e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia;

(d) **esaminare o far esaminare i testimoni a carico e ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico;**

(e) farsi assistere gratuitamente da un interprete se non comprende o non parla la lingua usata in udienza

1. I Limiti del diritto in tema di prova digitale

CARTA DI NIZZA (2000)

CAPO VI - GIUSTIZIA

Articolo 47

Diritto a un ricorso effettivo e a un giudice imparziale

Ogni individuo i cui diritti e le cui libertà garantiti dal **diritto** dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo.

Ogni individuo ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni individuo ha la facoltà di farsi consigliare, difendere e rappresentare.

A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.

Articolo 48

Presunzione di innocenza e diritti della difesa

Ogni imputato è considerato innocente fino a quando la sua colpevolezza non sia stata **legalmente** provata.

Il rispetto dei diritti della difesa è garantito ad ogni imputato.

1. I Limiti del diritto in tema di prova digitale

COSTITUZIONE DELLA REPUBBLICA ITALIANA

Articolo 111 (modificato da art. 1 L. cost. 23.11.1999, n. 2)

La giurisdizione si attua mediante il **giusto processo** regolato dalla legge.

Ogni processo si svolge nel **contraddittorio tra le parti, in condizioni di parità, davanti a giudice terzo e imparziale** (...)

Nel processo penale, la legge assicura che la persona accusata di un reato (...)

disponga del tempo e delle condizioni necessari per preparare la sua difesa;

(...) di ottenere (...) l'acquisizione di ogni altro mezzo di prova a suo favore;

Il processo penale è regolato dal **principio del contraddittorio nella formazione della prova** (...)

La legge regola i casi in cui la formazione della prova non ha luogo in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva (...)

1. I Limiti del diritto in tema di prova digitale

Consiglio d'Europa, 2001: Convenzione sul Cybercrime di Budapest

Compiti

- delineare definizioni comuni di reato
- definire poteri comuni di indagine
- predisporre mezzi di cooperazione internazionale

Capitolo II - Diritto procedurale

- scopo delle disposizioni procedurali
- condizioni e tutele
- conservazione rapida di dati informatici immagazzinati
- conservazione rapida e divulgazione parziale di dati relativi al traffico
- ingiunzione a produrre
- perquisizione e sequestro dei dati informatici immagazzinati
- raccolta in tempo reale di dati sul traffico
- intercettazione di dati relativi ai contenuti

Capitolo III – Cooperazione internazionale

Principi generali relativi a:

- cooperazione internazionale
- estradizione
- mutua assistenza
- informazioni spontanee

Disposizioni specifiche:

- Mutua assistenza relativa a misure provvisorie
  - conservazione rapida di dati informatici immagazzinati
  - divulgazione rapida di dati conservati
- Mutua assistenza relativa ai poteri d'indagine
  - assistenza relativa all'accesso a dati informatici immagazzinati
  - accesso transfrontaliero a dati informatici immagazzinati con il consenso o qualora essi siano pubblicamente disponibili
- Mutua assistenza nella conservazione in tempo reale di dati sul traffico
- Mutua assistenza in materia di intercettazione di dati relativi ai contenuti
- 24/7 Rete

1. I Limiti del diritto in tema di prova digitale

Le norme sulla tecno-regolazione del trattamento dei dati a fini processuali penali

- **Legge 23 dicembre 1993 n. 547, (G. U. n. 305 del 30 dicembre 1993)**

Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica

- **Art. 266 bis c.p.p.**

- **Legge 18 marzo 2008, n. 48, (G. U. n. 80 del 4 aprile 2008 S.O. n. 79)**

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

1. I Limiti del diritto in tema di prova digitale

LEGGE 4 APRILE 2008 N. 48

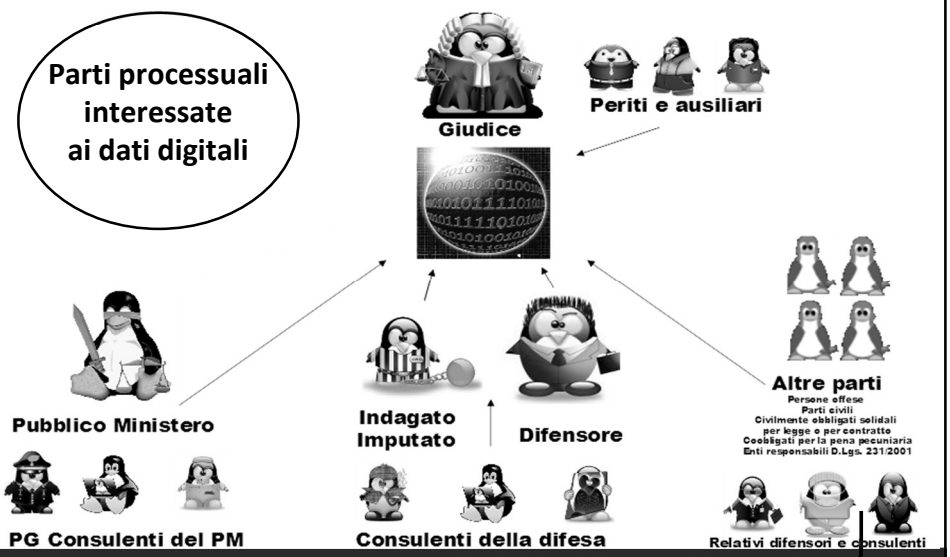
(Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno)

Modifiche al Codice di Procedura Penale

- **Mezzi di ricerca della prova**
  - Ispezioni
  - Perquisizioni
  - Richiesta di consegna
  - Sequestro di corrispondenza telematica
  - Sequestro di dati informatici di traffico
  - Dovere di esibizione
  - Custodia delle cose sequestrate
  - Sigillo elettronico o informatico e copia dei dati
- **Attività a iniziativa della P.G.**
  - Perquisizioni
  - Corrispondenza telematica
  - Accertamenti urgenti e sequestro
- **Conservazione dati di traffico**
- **Competenza**

13

1. I Limiti del diritto in tema di prova digitale



14

1. I Limiti del diritto in tema di prova digitale

Norme che richiamano la tecno-regolazione

- **244 c.p.p. Ispezione** – *… L'autorità giudiziaria può disporre…ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

- **247 c.p.p. Perquisizione** - *1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

- **Sequestro di dati presso l'indagato –** non prevista disciplina particolare

1. I Limiti del diritto in tema di prova digitale

Norme che richiamano la tecno-regolazione

254-bis. – Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. – *1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. (1).*

Sigillo elettronico o informatico e copia dei dati

260 c.p.p. - *L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'art. 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.*

1. I Limiti del diritto in tema di prova digitale

Alcuni problemi di tecno-regolazione

Termini tecnici nelle norme positive senza specificazione (norme opache)

- sistema informatico e telematico
- dati
- informazioni
- programmi

…con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.

- quale tipo di copia ?
- con quali tools ?
- dati originari e originali (hash e time stamping)
- quali tecniche per l'immodificabilità ?
- con quale procedura giuridica ?
- ex art. 359, 360 (117 disp. att. c.p.p.), 392, 233 c.p.p., altro ?
- con quali garanzie difensive per l'indagato-imputato e per le altre parti del procedimento ?

1. I Limiti del diritto in tema di prova digitale

Alcuni problemi di tecno-regolazione

- **"adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" ?**
- obbligo per le persone indicate nell'art. 200 e 201 c.p.p. ?
- obbligo per l'A.G. procedente ?
- obbligo per la P.G. ?

- **…ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione…**
- cracking di P.G. delle misure di sicurezza ?
- l'accesso e la perquisizione modificano ex se i dati (esterni) ? ANTINOMIA
- come impedire l'alterazione, concetto diverso da «immodificabilità» ?
- la verifica postuma dell'alterazione o meno presuppone o impone l'adozione di *tools open source* ?

1. I Limiti del diritto in tema di prova digitale

Alcuni problemi di tecno-regolazione

- … **fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione …**
- metadati, dati di handover, GPS, ecc.

- **… la loro acquisizione avvenga mediante copia di essi** su adeguato supporto…
- con quali procedure e tecniche di acquisizione ?
- con quali garanzie per la difesa ?

- **...su adeguato supporto…**
- quando il supporto può considerarsi "adeguato" ?

1. I Limiti del diritto in tema di prova digitale

Implicazioni:
la tecno-regolazione evoca altre norme giuridiche

Es. trattamento di dati personali e sensibili

- **Se effettuato dal custode nominato**
  - è una forma di trattamento di dati (anche sensibili) che dà luogo a responsabilità ex art. 2050 c.c.
  - obbligo di adozione delle misure di sicurezza ex All. B) D. Lgs. 196/03)
  - …in attesa del Regolamento Generale sulla Protezione dei Dati

- **Se effettuato da PG o AG**
  - è una forma di trattamento di dati (anche sensibili) che dà luogo a responsabilità ex art. 2050 c.c. ?
  - necessità dell'All. C) D. Lgs. 196/03 - Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia (ex artt. 46 e 53 Cod.; termine ex art. 181, 3 c., scaduto il 30 giugno 2004)

1. I Limiti del diritto in tema di prova digitale

2. LA TECNO-REGOLAZIONE DELLA PROVA DIGITALE

2. La tecno-regolazione della prova digitale

Best Practice e Standard di associazioni e enti non UE

- International Organization on Computer Evidence (**IOCE**), http://www.oas.org/juridico/english/ cyber_links.htm
- Best Practices for Computer Forensics, (Ver. 1.0, 15/11/2004; ver. 3.0, Sept. 2013), Scientific Working Group on Digital Evidence (**SWGDE**), https://www.swgde.org/documents/Archived%20Documents
- Best Practices on Imaging, Scientific Working Group on Imaging Technology (**SWGIT**), https://www.swgit.org/documents
- Forensic Science — Digital and Multimedia Evidence, National Institute of Standards and Technology (**NIST**), http://www.cftt.nist.gov/

2. La tecno-regolazione della prova digitale

Best Practice e Standard di associazioni ed enti UE

- International Association of Computer Investigative Specialists (**IACIS**) http://www.iacis.com/
- Good Practice Guide for Digital Evidence, Association of Chief Police Officers – Computer Crime Working Group (**ACPO**)
- Guidelines For Best Practice In The Forensic Examination Of Digital Technology (Ver. 6, 20/4/2009), European Network of Forensics Science Institutes, (**ENFSI**)
- Cloud Computer forensics, European Telecommunications Standards Institute (**ETSI**), http://www.etsi.org/

2. La tecno-regolazione della prova digitale

Best Practice e Standard di associazioni ed enti UE

- International Association of Computer Investigative Specialists (**IACIS**) http://www.iacis.com/
- Good Practice Guide for Digital Evidence, Association of Chief Police Officers – Computer Crime Working Group (**ACPO**)
- Guidelines For Best Practice In The Forensic Examination Of Digital Technology (Ver. 6, 20/4/2009), European Network of Forensics Science Institutes, (**ENFSI**)
- Cloud Computer forensics, European Telecommunications Standards Institute (**ETSI**), http://www.etsi.org/

ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA

2. La tecno-regolazione della prova digitale in Italia

- In Deliberazione 24 maggio 2018, n. 8/2018/G su “L’e-commerce e il sistema fiscale” approvata dalla Sezione centrale di controllo sulla gestione delle Amministrazioni dello Stato.
  - file:///C:/Users/antonio/AppData/Local/Temp/delibera_8_2018.pdf

- La necessità di strumenti per la computer forensics

Con riferimento a quanto sin qui esposto, costituiscono motivo di particolare interesse, i passi della Relazione nei quali la Corte, sottolineando la necessità che l’amministrazione fiscale si doti di nuovi strumenti di intervento per ridurre le entrate sottratte al bilancio pubblico, fa riferimento alla Computer forensics:

[…] Al fine di adeguare i dispositivi di controllo alla crescente digitalizzazione dell’informazione e superare le citate difficoltà operative, il Corpo [della Guardia di Finanza, n.d.s.] ha istituito una specifica figura professionale, attribuendo, all’esito di un apposito percorso di formazione, la qualifica in “computer forensics e data analysis” (CFDA)
https://www.csigbologna.it/referenze/informatica-forense/computer-forensics-indagini-tributarie/

2. La tecno-regolazione della prova digitale in Italia

Circolare 1/2018 - Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali

Protocollo 357600 del 27 novembre 2017

Nuovo “Manuale Operativo in materia di contrasto all’evasione e alle frodi fiscali” – circolare n. 1/2018, con cui sono state aggiornate le direttive operative della Guardia di Finanza concernenti l’esecuzione delle verifiche, dei controlli fiscali e delle indagini di polizia economico-finanziaria finalizzate al contrasto dell’evasione, dell’elusione e delle frodi fiscali. Il Manuale, corredato della presentazione a firma del Comandante Generale, è aggiornato al 1° dicembre 2017 ed entrerà in vigore il 1° gennaio 2018.

Circolare n. 1 2018 Volume I Pubblicato il 4 dicembre 2017	
Circolare n. 1 2018 Volume II Pubblicato il 4 dicembre 2017	
Circolare n. 1 2018 Volume III Pubblicato il 4 dicembre 2017	
Circolare n. 1 2018 Volume IV Pubblicato il 4 dicembre 2017	

https://www.gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca

1. I Limiti del diritto in tema di prova digitale

ISO/IEC

27

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

ISO/IEC

(International Organization for Standardization / International Electrotechnical Commission)

28

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

- Organizzazione indipendente, non-governativa, con membri di 164 organi nazionali di standardizzazione.
- Gli esperti dei suoi membri condividono conoscenze e sviluppano, su base volontaria basata sul consenso, standard internazionali aventi mercato che aiutino l'innovazione e forniscano soluzioni alle sfide globali.
- Nata nel 1947, ha sede a Ginevra, Svizzera.
- Con ISO collabora IEC

INTERNATIONAL ELECTROTECHNICAL COMMISSION

- Organizzazione mondiale che prepara e pubblica gli Standard Internazionali per ogni tecnologia elettrica ed elettronica, altrimenti conosciuta come "electrotechnology".
- Al lavoro di IEC partecipano circa 20.000 esperti dall'industria, commercio, amministrazione, laboratori di prova e ricerca, accademia, gruppi di consumatori.
- Gli Standard IEC si basano sul pieno consenso e rappresentano I bisogni degli operatori di ogni paese partecipante alla sua attività. Ogni paese membro, grande o piccolo, ha un voto ed esprime la propria opinione sull'oggetto dell'attività.
- Nata nel 1906, ha sede a Ginevra, Svizzera.

IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI

29

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

ISO/IEC

- **ISO (l'Organizzazione Internazionale per la Standardizzazione)**
- **IEC (la Commissione Elettrotecnica Internazionale)**

- formano il sistema specializzato per la **standardizzazione a livello mondiale**

- Gli **enti nazionali** che sono membri dell'ISO e dell'IEC partecipano allo sviluppo degli standard internazionali attraverso **commissioni tecniche** istituite dalle rispettive organizzazioni per occuparsi di campi specifici dell'attività tecnica.

- Le commissioni tecniche di ISO ed IEC collaborano in ambiti di mutuo interesse.

- Prendono parte ai lavori anche altre **organizzazioni internazionali**, **governative** e **non governative**, in collaborazione con ISO ed IEC.

30

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

- **ISO (l'Organizzazione Internazionale per la Standardizzazione)**
- **IEC (la Commissione Elettrotecnica Internazionale)**

- Nell'ambito dell'Information Technology, ISO ed IEC hanno istituito una commissione tecnica congiunta ISO/IEC JTC 1.
- Gli standard internazionali sono redatti nel rispetto delle regole stabilite nelle Direttive ISO/IEC Parte 2^.
- Il compito principale della commissione tecnica congiunta è di redigere gli **Standard Internazionali**. I progetti di Standard Internazionali adottati dalla commissione tecnica congiunta vengono fatti circolare fra gli organismi internazionali per il voto. La pubblicazione a livello di Standard Internazionale richiede l'**approvazione di almeno il 75% degli enti nazionali** esprimenti un voto.
- Si richiama l'attenzione sulla possibilità che alcuni elementi di questo documento possano essere soggetti a diritti di brevetto. ISO ed IEC declinano ogni responsabilità in merito all'identificazione di questi diritti.

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

Standard internazionali ISO/IEC sulla digital evidence

(International Organization for Standardization / International Electrotechnical Commission)

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

- **ISO (l'Organizzazione Internazionale per la Standardizzazione)**
- **IEC (la Commissione Elettrotecnica Internazionale)**

- Lo standard ISO /IEC 27037 è stato redatto dalla Commissione Tecnica Congiunta ISO/IEC JTC 1, Information Technology, Sottocommissione **SC 27, IT Security Techniques.**

ISO/IEC JTC 1/SC 27 **Information security, cybersecurity and privacy protection**

33

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

- **ISO/IEC 27037:2012** Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence" pubblicato in versione definitiva il 15 ottobre 2012 (**Linee guida per l'identificazione, raccolta, acquisizione e conservazioni delle prove digitali**)

- **ISO/IEC 27038:2014** Information technology - Security techniques - Specification for digital redaction" pubblicato in versione definitiva il 13 marzo 2014 (**Linee guida per le specifiche di redazione digitale**)

- **ISO/IEC 27041:2015** Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method" pubblicato in versione definitiva il 15 giugno 2015 (**Linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione**)

- **ISO/IEC 27042:2015**, su "Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence" pubblicato in versione definitiva il 19 giugno 2015 (**Linee guida per l'analisi e l'interpretazione di prove digitali**)

- **ISO/IEC 27043:2015** "Information technology - Security techniques - Incident investigation principles and processes" pubblicato in versione definitiva il 1 marzo 2015 (**Principi e processi per l'investigazione di incidenti informatici**)

34

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

- **ISO/IEC 17025:2005** General requirements for the competence of testing and calibration laboratories
- **ISO/TR 15801:2009 -** Document management - Information stored electronically - Recommendations for trustworthiness and reliability
- **ISO/IEC 17020:2012 -** Conformity assessment - Requirements for the operation of various types of bodies performing inspection
- **ISO/IEC 27000:2012** Information technology - Security techniques - Information security management systems - Overview and vocabulary

I RAPPORTI CON ALTRI STANDARD 27037

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

1 Scope

- *This International Standard provides guidelines for specific activities in* ***handling potential digital evidence;***
- *these processes are:* ***identification, collection, acquisition and preservation of potential digital evidence.***
- *These processes are required in an* ***investigation*** *that is designed to maintain the integrity of the digital evidence –* ***an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary*** *actions as well as other required instances.*
- *This International Standard also provides* ***general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence****.*

37

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

- **Fragility** of digital evidence
- An acceptable methodology to ensure the **integrity** and **authenticity of the potential digital evidence**
- ISO does not mandate the use of particular tools or methods
- Credibility in the investigation = **methodology applied** during the process, and **individuals qualified** in performing the tasks specified in the methodology
- ISO does not address the methodology for legal proceedings, disciplinary procedures and other related actions

38

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

• **Presupposto fisico**	**FRAGILITA'** dell'elemento di prova digitale
• **Esigenze**	**METODOLOGIA** di salvaguardia dell'elemento di prova digitale • **INTEGRITA'** • **AUTENTICITA'**
• **ISO non raccomanda**	**METODOLOGIE PARTICOLARI** **STRUMENTI PARTICOLARI**
• **Credibilità dell'investigazione**	**METODOLOGIA da applicarsi alla procedura** e qualificazione degli operatori ad attuare i compiti specificati nella metodologia
• **ISO non indirizza**	**METODOLOGIA PER** • **PROCEDURA GIURIDICA** • **PROCEDIMENTO DISCIPLINARE** • **ALTRE AZIONI CORRELATE**

39

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

ASPETTI TECNICI

- Trattamento dell'elemento di prova digitale
  - tale e
  - potenziale
- Definizione linee guida nelle fasi di
  - Identificazione
  - Raccolta
  - Acquisizione
  - Conservazione
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio
- Per prova informatica si fa riferimento a dati già in formato digitale
- Esclusi quindi dati in formato analogico convertiti in formato digitale

ASPETTI LEGALI

- Acquisizione elemento/mezzo di prova digitale
  - Tale e
  - potenziale
- Definizione linee guida nelle fasi di
  - Ispezione / Perquisizione / Richiesta / Istanza
  - Consegna / Esibizione / Sequestro
  - Acquisizione (immateriale)
  - Assicurazione (paradigma legale)
- Integrità e metodologia degli elementi di prova finalizzati all'ammissibilità come prova in giudizio
- Elemento di prova digitale nativa digitale
- No elementi di prova analogici convertiti in formato digitale

40

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

ISO / IEC

- Application of this International Standard
  - requires compliance with national laws, rules and regulations.
  - It should not replace specific legal requirements of any jurisdiction.

ASPETTI LEGALI

- Applicazione delle norme giuridiche
  - Non impongono l'osservanza di ISO
  - L'inosservanza NON produce
    - inutilizzabilità
    - annullabilità
    - nullità
  - L'inosservanza di ISO incide sulla valutazione dell'elemento di prova
    - Vizio di motivazione

41

RAPPORTI TRA STANDARD ISO/IEC E NORME GIURIDICHE

- Individuazione
- Acquisizione

- 361 cpp
- 359, 360, 392

- Valutazione
- Presentazione

42

RAPPORTI TRA STANDARD ISO/IEC E NORME GIURIDICHE PROCESSULPENALI ITALIANE

Individuazione

Art. 361 Individuazione di persone e di cose

1. Quando è necessario per la immediata prosecuzione delle indagini, il pubblico ministero procede alla individuazione di persone, di cose o di quanto altro può essere oggetto di percezione sensoriale [213-217].

2. Le persone, le cose e gli altri oggetti sono presentati ovvero sottoposti in immagine a chi deve eseguire la individuazione.

3. Se ha fondata ragione di ritenere che la persona chiamata alla individuazione possa subire intimidazione o altra influenza dalla presenza di quella sottoposta a individuazione, il pubblico ministero adotta le cautele previste dall'articolo 214 comma 2(1).

(1) In questo caso non sono previste forme particolari di garanzie difensive.

RAPPORTI TRA STANDARD ISO/IEC E NORME GIURIDICHE PROCESSULPENALI ITALIANE

Acquisizione

Art. 354, 359, 360 (400), 117, 392,

RAPPORTI TRA STANDARD ISO/IEC E NORME GIURIDICHE PROCESSULPENALI ITALIANE

Art. 366 Deposito degli atti cui hanno diritto di assistere i difensori

1. Salvo quanto previsto da specifiche disposizioni [268], i verbali degli atti compiuti dal pubblico ministero e dalla polizia giudiziaria ai quali il difensore ha diritto di assistere [350, 356, 364, 365], sono depositati nella segreteria del pubblico ministero entro il terzo giorno successivo al compimento dell'atto, con facoltà per il difensore di esaminarli ed estrarne copia nei cinque giorni successivi. Quando non è stato dato avviso del compimento dell'atto, al difensore è immediatamente notificato l'avviso di deposito e il termine decorre dal ricevimento della notificazione. Il difensore ha la facoltà di esaminare le cose sequestrate nel luogo in cui esse si trovano e, se si tratta di documenti, di estrarne copia(1).

2. Il pubblico ministero, con decreto motivato, può disporre, per gravi motivi, che il deposito degli atti indicati nel comma 1 e l'esercizio della facoltà indicata nel terzo periodo dello stesso comma siano ritardati, senza pregiudizio di ogni altra attività del difensore, per non oltre trenta giorni. Contro il decreto del pubblico ministero la persona sottoposta ad indagini ed il difensore possono proporre opposizione al giudice, che provvede ai sensi dell'articolo 127.

45

OPERATORI ISO/IEC

DFRS - Digital Evidence First Responder

https://www.fbi.gov/news/stories/online-cyber-training-for-law-enforcement-first-responders

Persona autorizzata, formata e qualificata ad agire per prima sulla scena di un incidente per lo svolgimento di raccolta e acquisizione di elementi prova digitale con la responsabilità per la loro manipolazione

DES - Digital Evidence Specialist

Persona che sa svolgere i compiti di un DEFR e che ha una conoscenza specializzata, competenze e abilità per trattare un'ampia serie di problematiche tecniche.
NOTA Un DES deve avere competenze addizionali di nicchia, per esempio per l'acquisizione da rete, l'acquisizione di RAM, conoscenza di software di sistemi operativi o di server.

IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI

46

STANDARD INTERNAZIONALI ISO/IEC SULLA DIGITAL EVIDENCE

PRO

- diffusione consapevolezza
- tensione al miglioramento
- creazione di un lessico condiviso
- confronto di diverse soluzioni
- verificabilità diffusa (testabilità)
- economie di scala
- scalabilità

CONTRO

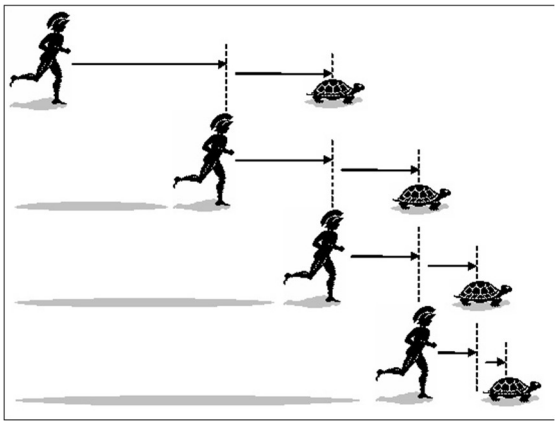
- lobby e procedure di standardizzazione
- brevetti
- trasparenza nella standardizzazione
- provvisorietà rispetto al progresso
- non terrebbe conto di pratiche alternative
- favorirebbe atteggiamenti conservatori
- rallenterebbe l'innovazione
- rallenterebbe il recepimento delle innovazioni

178

1. I RAPPORTI CON ALTRI STANDARD 27037

179

IL PARADOSSO DI ACHILLE E LA TARTARUGA (Zenone di Elea)



http://www.multytheme.com/cultura/multimedia/didattmultitema/scuoladg/filosofia/zenonedielea.html

181

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

GRAZIE PER L'ATTENZIONE

Avv. Antonio Gammarota
Scuola di Giurisprudenza – CIRSFID
Alma Mater Studiorum – Università di Bologna
antonio.gammarota@unibo.it

www.unibo.it

184