# I Cybercrimes dal Deep web al Dark web

OPPORTUNITÀ E LIMITI DELLA DIGITAL FORENSICS – vincenzocalabro.it

# *infosfera onlife*

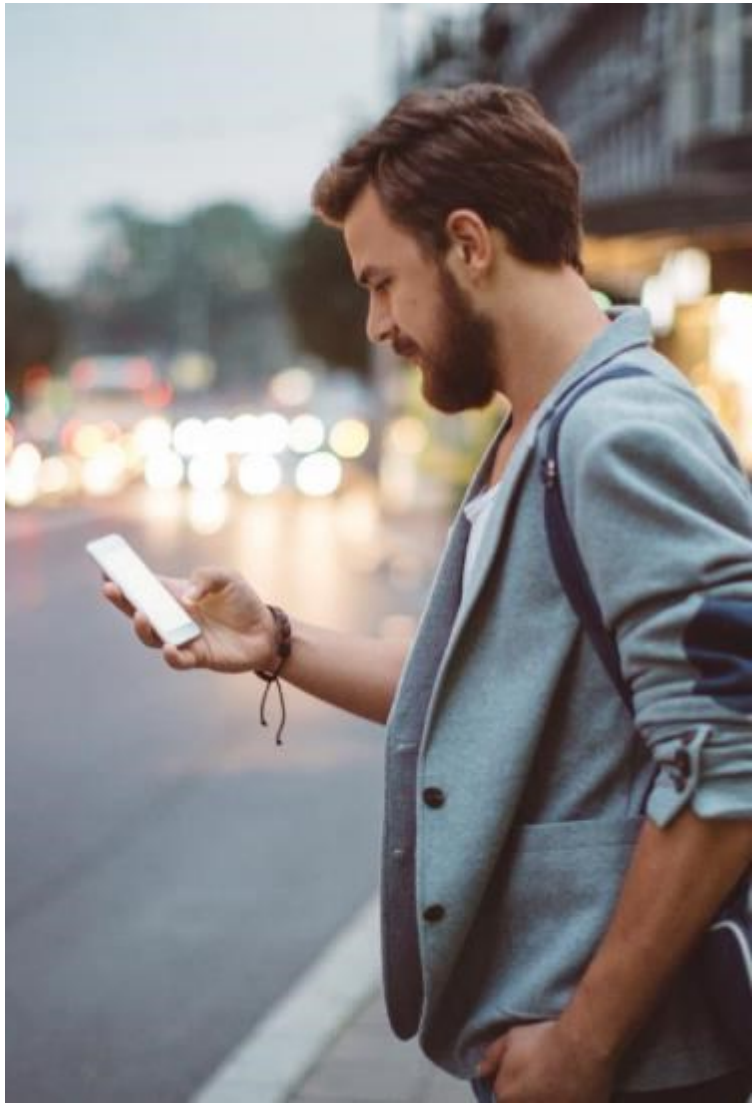
La maggior parte degli individui vive immerso in un mondo digitale, un mondo in cui i confini tra la vita online e quella offline si dissolvono all'ombra della iper-connettività.

Floridi* parla di una quarta rivoluzione epocale, dopo quelle di Copernico, Darwin e Freud, che ci sta portando dritti verso una "***infosfera***" globale.

Siamo compenetrati dalla realtà informatica e l'essere connessi è diventato parte integrante della nostra quotidianità tanto che si parla di vite condotte «**onlife**».

Questa trasformazione antropologica-digitale, che riguarda l'agire quotidiano di ogni individuo, ha ricadute giuridiche in tutti gli ambiti sociali:

- Democrazia e Libertà di espressione
- Comunicazione e Informazione
- Economico-Finanziaria e Produttiva
- Sfera Pubblica e Privata



Luciano Floridi, professore di filosofia ed etica dell'informazione all'Università di Oxford

# Peculiarità dell'*onlife*

La vita iperconnessa impone la consapevolezza di alcune criticità:

- Il problema dell'Identità digitale o Anonimato
- La Comunicazione mediata / Distanza tra interlocutori
- Raggiri o Ricatti basati sulla fiducia o i sentimenti dell'interlocutore
- L'Utilizzo dei Deep fake (image / audio / video)
- La violazione del diritto all'Oblio e alla Privacy
- La Volatilità e l'Alterabilità del dato digitale
- Gli Algoritmi di Intelligenza Artificiale che posso orientare il Libero Arbitrio
- La Facilità di reperimento di Informazioni, Beni e Servizi (Globalizzazione reale)
- Gli Usi, i Linguaggi e le Legislazioni differenti / Assenza di Tutele (in alcuni contesti)
- I Confini e le Competenze Territoriali / Assenza di Regole (in alcuni contesti)
- Il fenomeno del Crime-as-a-service

**Computer as a tool:**
Con questo termine ci si riferisce ai reati informatici impropri (o atipici), ossia ai reati comuni previsti dal codice penale o dalla legislazione speciale, che solo incidentalmente vengono commessi mediante l'uso di un computer e della rete: esempi comuni sono i reati di ingiuria e di diffamazione (che possono perfezionarsi anche attraverso la posta elettronica, le chat o un sito Internet), le molestie (perpetrate attraverso lo spamming, o sui social network) e altri reati più gravi come l'istigazione a delinquere, l'istigazione all'odio razziale, il riciclaggio (*cyberlaundering*) o la pedopornografia, il cyberbullismo, il grooming (addescamento del minore), il revenge porn, il sextortion, il furto d'identità, le frodi online, le fake news, ecc .

# Cybercrime o Reato informatico

**definizione**

- Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema (**computer as a tool**) o colpendolo (**computer as a target**).

**Computer as a target:**
In genere è un reato perpetrato per colpire un sistema informatico.
Si tratta di reati informatici propri (o tipici), la maggior parte dei quali sono stati introdotti nell'ordinamento italiano dalla legge 547/1993 e dalla legge 48/2008, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica di Budapest del 23 novembre 2001.
Ad esempio: il danneggiamento di dati, programmi e sistemi, la frode informatica, l'accesso abusivo, la detenzione e la diffusione abusiva di codici d'accesso e la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, la falsificazione di documenti informatici, l'interferenza illecita nelle comunicazioni informatiche o telematiche e alcuni di quelli previsti dalla legge sul diritto d'autore.

# Digital Evidences

Le **peculiarità** che contraddistinguono la fonte di prova digitale, che non possono essere ignorate, consistono in:

- **Immaterialità**: la prova digitale è il contenuto e non il supporto su cui è memorizzata,
- **Dispersione**: la prova digitale può essere dislocata su più dispositivi molto distanti tra loro,
- **Promiscuità**: la prova digitale può trovarsi all'interno di dispositivi che contengono altre informazioni non attinenti all'indagine,
- **Congenita modificabilità**: la prova digitale è estremamente alterabile.

## Definizione

La **fonte di prova digitale** o *digital evidence* è «*qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale*»

Distinguiamo:

- La prova creata dall'uomo
- La prova creata autonomamente dal computer
- La prova creata sia dall'essere umano che dal computer

# Digital Forensics

La giurisprudenza, pertanto, incoraggia l'utilizzo delle **tecniche di informatica forense**, affinché siano estratti contenuti in copia dei dati presenti, cristallizzati in **copie forensi** consentendo la produzione di **elementi giudiziali certi**, in relazione ad **integrità dei dati**, **non manipolazione**, **riconducibilità all'autore e certezza temporale**, rendendo la copia forense prodotta **immodificabile** e tendenzialmente vincolante per il giudicante.

## Perché la digital forensics

Il tema della prova è centrale all'interno del processo, costituendo il campo più critico entro il quale si dispiega l'attività degli operatori del diritto e che oggi non può prescindere dall'informatica, dalla **volatilità** e **fragilità** del **dato informatico**, dall'importanza della corretta acquisizione e gestione dei bit, dalla fonte di prova digitale.

# Digital Forensics

**L'ordinamento Italiano**, dopo l'approvazione della Legge 48 del 2008 di ratifica della Convenzione sul Cybercrime di Budapest, **ha stabilito che**, nel processo penale, **tutte le attività probatorie che hanno ad oggetto le prove digitali devono essere disposte attraverso tecniche idonee ad assicurare la conservazione dei dati originali ed impedirne l'alterazione.**
Pertanto, è necessario che anche **le metodologie utilizzate per il trattamento delle evidenze digitali abbiano la capacità di resistenza ad eventuali contestazioni e capacità di convincimento del giudice e delle parti processuali in ordine alla loro verificabilità, ripetibilità, riproducibilità e giustificabilità.**
Per tale motivo è fortemente consigliato impiegare tecniche e standard ispirati al metodo scientifico.

Lo **scopo dell'informatica forense** si esplicita nelle seguenti prerogative:

- identificare
- conservare
- acquisire
- documentare
- interpretare i dati

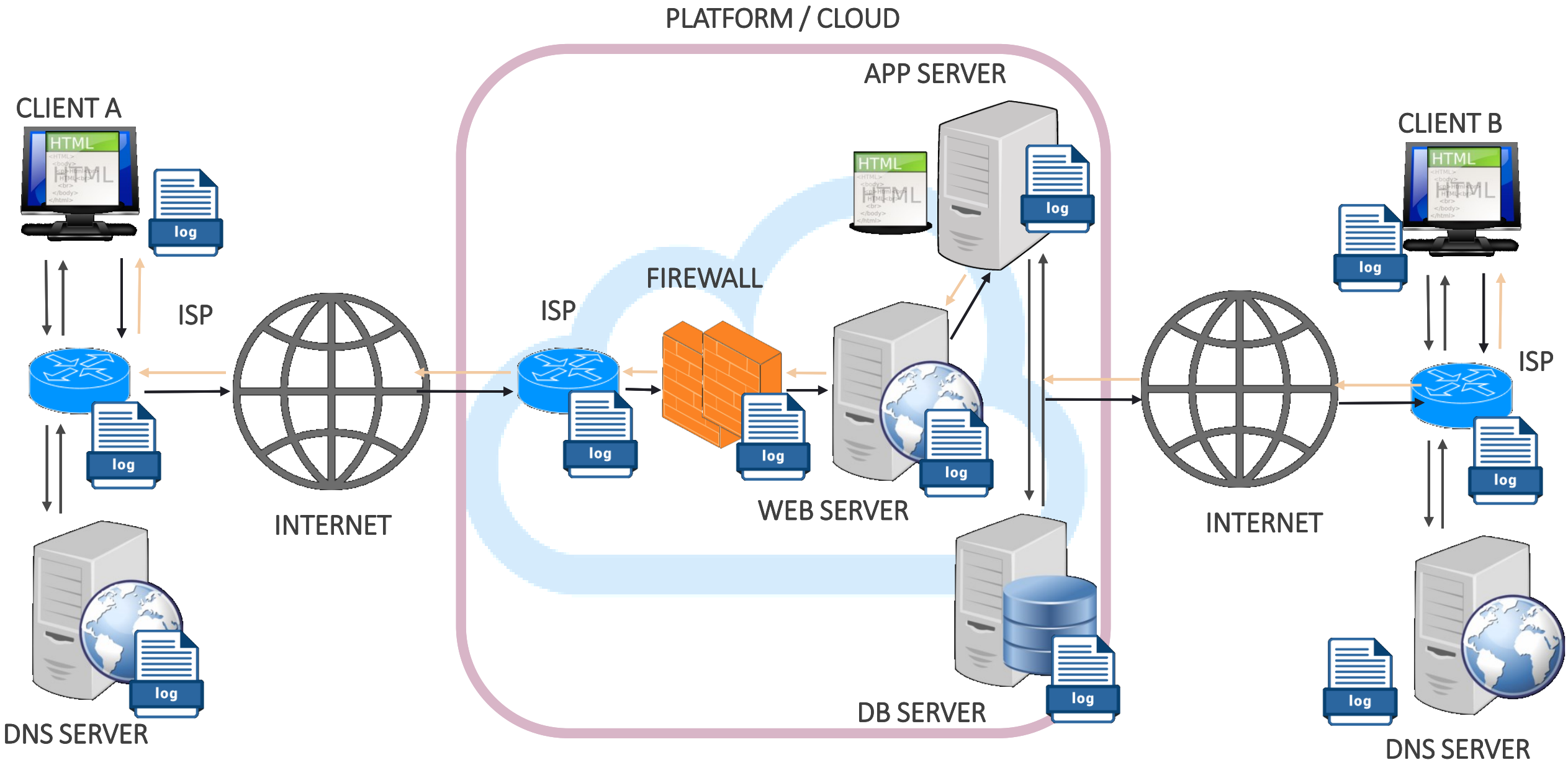
presenti su una memoria digitale.

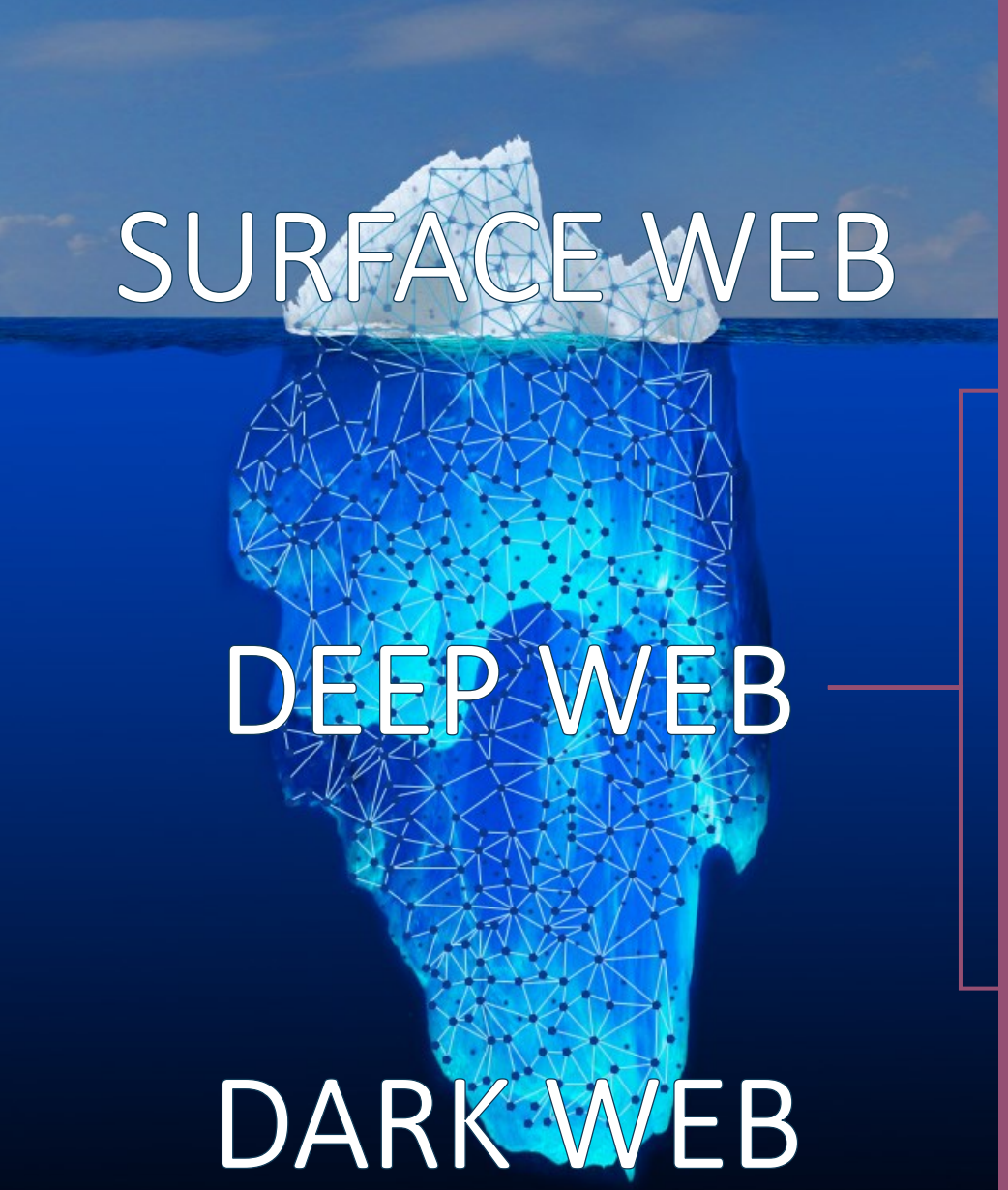

## IL PROCESSO DI DIGITAL FORENSICS

Lo standard ISO/IEC 27037:2012 "*Guidelines for identification, collection, acquisition, and preservation of digital evidence*" fornisce delle linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione, raccolta, acquisizione e preservazione.
Lo standard ISO/IEC 27042:2015 «*Guidelines for the analysis and interpretation of digital evidence*" fornisce una guida sull'analisi e l'interpretazione delle prove digitali in grado di affrontare le questioni di continuità, validità, riproducibilità e ripetibilità.

# Opportunità e Limiti della Digital Forensics sul Web

# Web architecture: *dove cercare le evidenze*






Public

## Contenuti/Servizi pubblici e legali

*siti web, motori di ricerca, social media, news, …*

## Contenuti/Servizi riservati e legali

*banche dati riservate (sanità, finanza, copyright, …*

## Contenuti/Servizi privati e legali

*email, comunicazioni private, dati personali, …*

## Contenuti/Servizi anonimi e legali

*chat anonime, TOR encrypted sites, I2P,*
*cripto valute, peer-to-peer, dark-room, …*

## Contenuti/Servizi anonimi e illegali

*pedoporno, drugs, arms e cyber-arms, false-id, credit card, …*

Anonymous

# Obiettivo

acquisire in maniera certa e sicura le evidenze presenti online da diversi fonti e servizi diversi

## Criticità

- La nascita del c.d. Web 2.0 e la crescente pervasività delle tecnologie ha favorito la proliferazione di diversi servizi Internet (Newsgroup, Blog, Chat, Social network), utilizzati per la diffusione delle informazioni
- Spesso questi servizi non sono ben regolamentati e coperti dall'anonimato.
- Inoltre, in base alle caratteristiche di alcuni dei predetti servizi, le informazioni oggetto di reato possono essere volatili e, quindi, facilmente manipolabili o rimovibili.
- Infine, i dati di interesse possono essere memorizzati in località con legislazione diversa dalla nostra, possono non essere direttamente raggiungibili (deep web) e il provider si rifiuta di collaborare.

## Conseguenza

- Ciò ha incrementato il numero di determinati reati quali: la diffamazione, lo stalking (cyber-stalking), l'hate-speech, l'adescamento telematico (grooming), la pedopornografia, il reverge porn, il sextortion, il furto d'identità digitale, la sostituzione di persona, la violazione di copyright e l'utilizzo illecito di marchi, il furto dei dati, il phishing, le truffe online, l'accesso abusivo ad una banca dati, la violazione della privacy, il controllo a distanza illecito, l'assenza di tutela legale, l'intercettazione abusiva, gli attacchi denial of service, il danneggiamento degli apparati di telecomunicazione, ecc.

# Soluzione

realizzare una acquisizione forense e certificata del contenuto che si contesta così come è consultabile, che diventerà evidenza, prima che possa scomparire

## Acquisizione on-premise

La modalità on-premise (in sede) consente di prelevare le evidenze direttamente dalla fonte e può prevedere la raccolta dei seguenti elementi:

- La copia forense della memoria dei servers (**anche parziale**)
- **I logs dei servers** (WEB, APP, DB)
- **I logs del traffico dell'ISP** che ospita i server
- **I logs del traffico dell'ISP** da cui è stata effettuata la connessione
- **I logs dei DNS server**
- **I logs del traffico telefonico** (per risalire all'utenza telefonica)
- **La copia forense del client** da cui è stato eseguito il reato

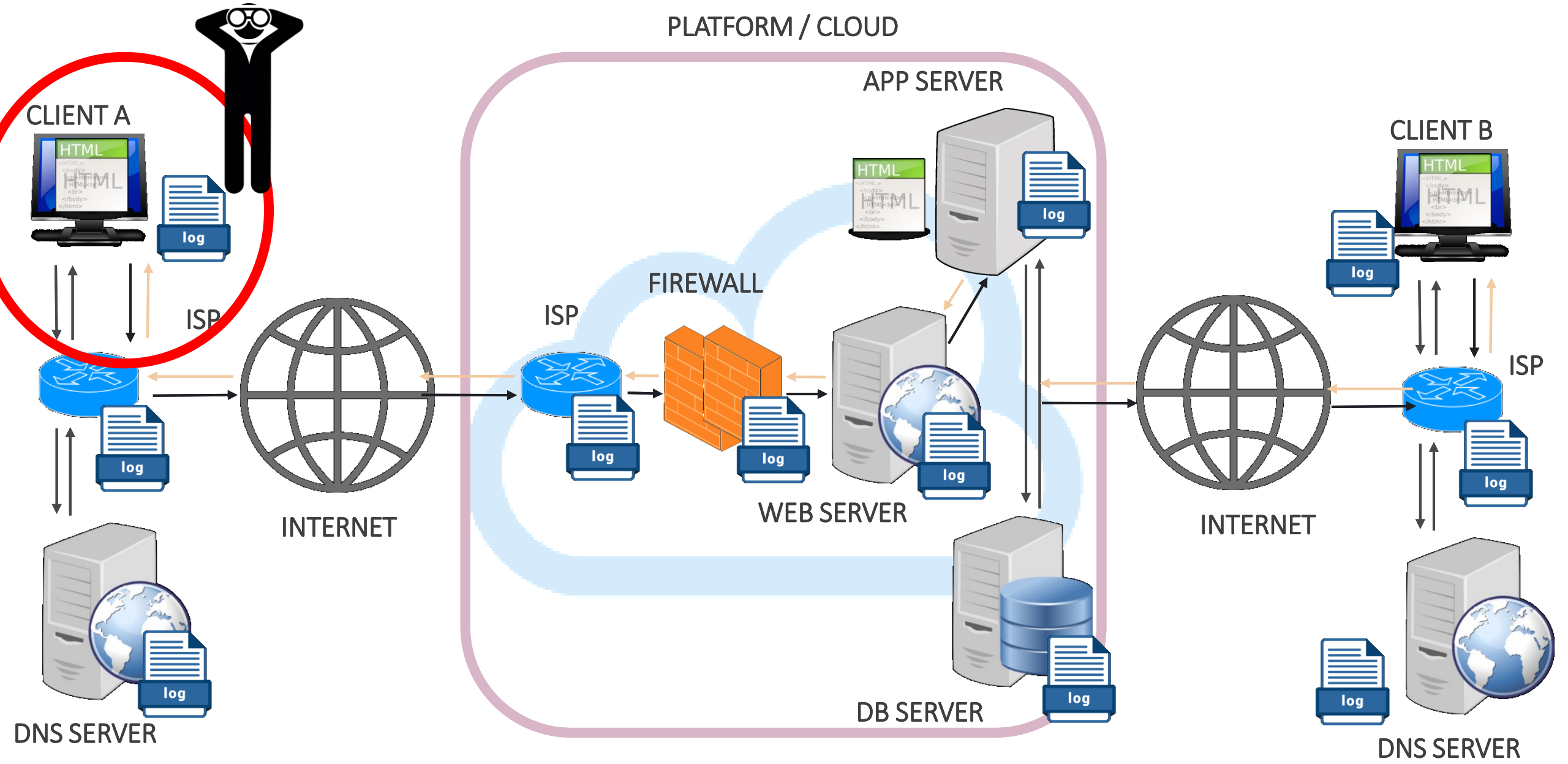
## Acquisizione off-premise

**È la tecnica utilizzata per realizzare una «preview» del dato e nei casi in cui non è possibile intervenire in presenza sui dispositivi su cui sono memorizzate le evidenze di interesse.**

L'acquisizione forense a distanza può essere eseguita quando si verifica una della seguenti ipotesi:

- il nodo/server non è agevolmente identificabile e raggiungibile. Si pensi, ad esempio, alle infrastrutture dei grandi Social Media o degli Operatori OTT - Over-The-Top ,
- non siamo nelle condizioni giuridiche per chiedere ad un terzo la copia forense di un dato, anche se è pubblico, perché siamo in una fase di precontenzioso;
- il server si trova in uno stato estero per cui è necessaria una rogatoria internazionale di difficile attuazione;
- il dato d'interesse ha un alto grado di volatilità, si pensi ad un post pubblicato su un portale social, e pertanto si rischia di non trovarlo più disponibile;
- il tempo concesso per svolgere l'indagine non è compatibile con le tempistiche scandite da questa modalità di acquisizione.

# Web architecture: *come estrarre le evidenze*



# Fonti di prova alternative

1. Ricostruire le fasi preliminare di attacco
   - falsa identità
   - seduzione
   - raccolta informazioni
   - manipolazione
2. Carving sul web per tracce orfane
3. Cloud storage forensics
4. Mobile App forensics
5. Log forensics
6. Crypto-currency forensics
7. Captatore Informatico
8. Informazioni a latere per rendere un’indagine più robusta

# Il Perito Digitale deve assicurare che siano rispettate 6 garanzie fondamentali

il dovere di conservare inalterato il dato informatico originale nella sua genuinità

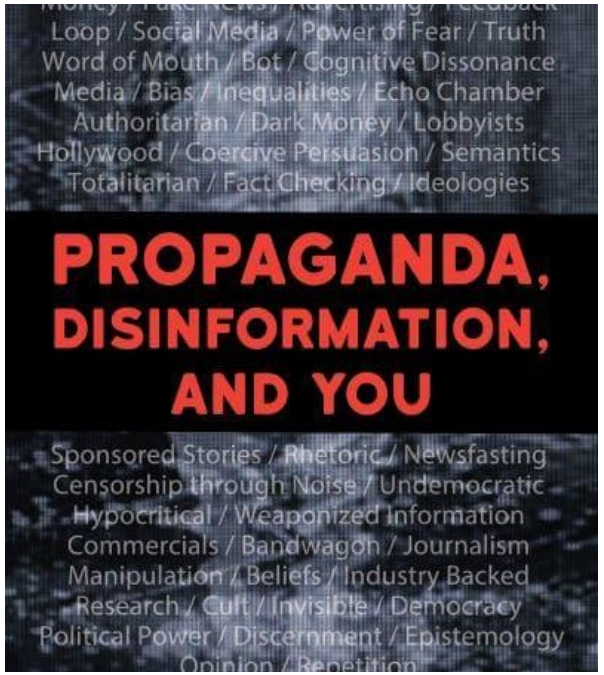
il dovere di impedire l'alterazione successiva del dato originale

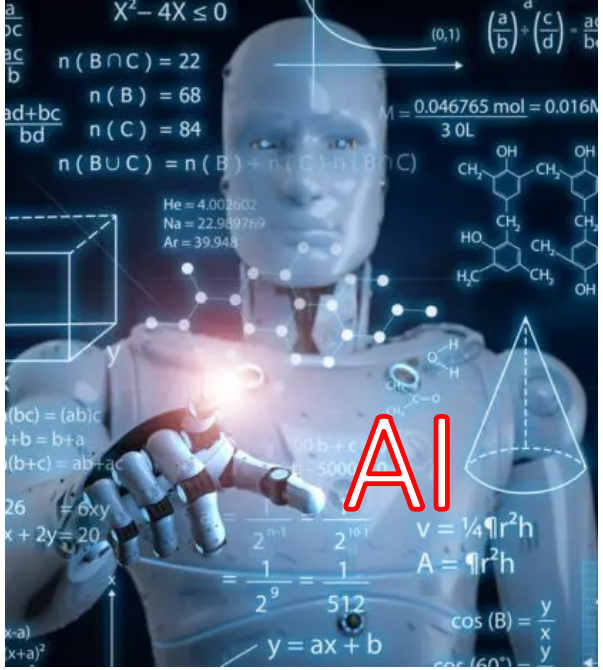
il dovere di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale

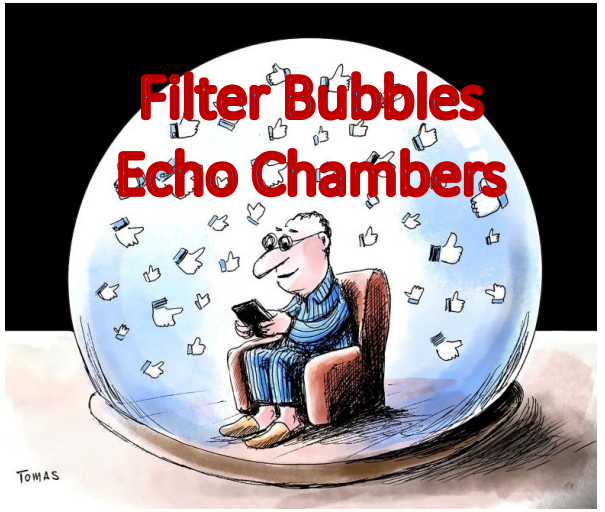
il dovere di assicurare l'immodificabilità della copia del documento informatico

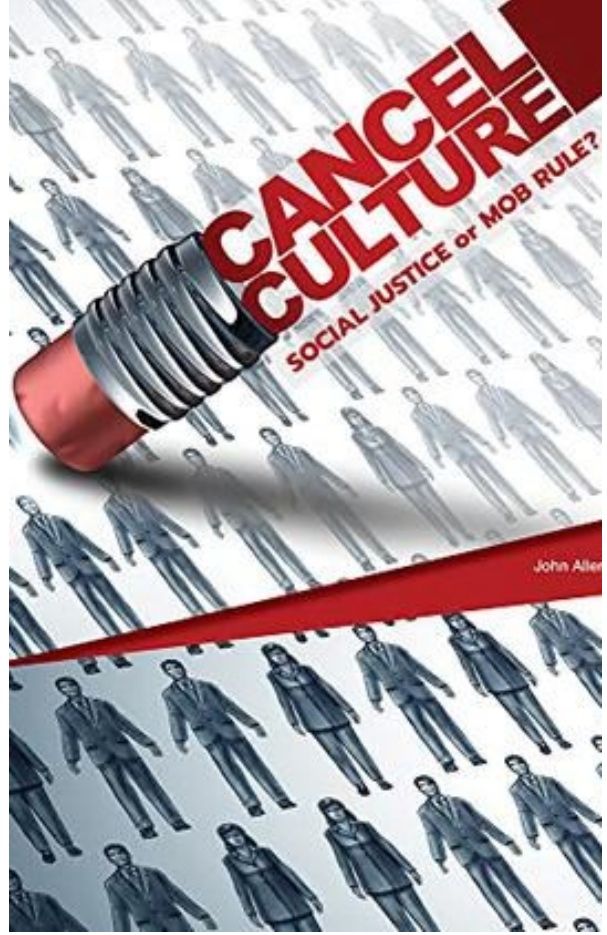
la garanzia delle installazioni di sigilli informatici sui documenti acquisiti

la riproducibilità e la verificabilità del proprio operato


Loop / Social Media / Power of Fear / Truth
Word of Mouth / Bot / Cognitive Dissonance
Media / Bias / Inequalities / Echo Chamber
Authoritarian / Dark Money / Lobbyists
Hollywood / Coercive Persuasion / Semantics
Totalitarian / Fact Checking / Ideologies
PROPAGANDA, DISINFORMATION, AND YOU
Sponsored Stories / Rhetoric / Newsfasting
Censorship through Noise / Undemocratic
Hypocritical / Weaponized Information
Commercials / Bandwagon / Journalism
Manipulation / Beliefs / Industry Backed
Research / Cult / Invisible / Democracy
Political Power / Discernment / Epistemology
Opinion / Repetition


AI


Filter Bubbles
Echo Chambers
TOMAS


CANCEL CULTURE
SOCIAL JUSTICE or MOB RULE?


FAKE NEWS


social media
BANNED
BLOCKED
DELETED
CENSORED