Table of Contents

Introduzione

Ottuso cercare di rispondere ad ogni domanda nella limitata prospettiva di cio' che ci e' piu' familiare.
E' necessario un **confronto** tra discipline diverse.
Il rapporto tra diritto ed informatica e' oggetto dell'**informatica giuridica**.

- **Informatica del diritto:** informatica applicata al diritto.
- **Diritto dell'informatica:** diritto applicato all'informatica.

Nozioni Base

Common law: origini anglosassoni, sentenze basate sui precedenti simili.
Civil law: evoluzione del diritto romano, codici prestabiliti.
Direttiva: atto legislativo non vincolante che indica un obiettivo per i singoli paesi.
Regolamento: atto legislativo vincolante che deve essere applicato in tutti i paesi.

Informatica del Diritto

Cibernetica (**1948** – **Wiener**). Studio di come umani, animali e macchine comunicano tra loro.

Giurimetria (**1949** – **Loevinger**). Studio della risoluzione dei problemi giuridici attraverso il **metodo scientifico**. Si concentra sull'analisi del comportamento dei giudici e sulla possibilita' di applicare modelli logico matematici al diritto. Realizzazione normative che possano essere analizzate elettronicamente. I risultati di una sentenza non sono piu' opinioni.
Prime sperimentazioni della giurimetria negli anni 70 negli Stati Uniti.

Lawtomation (**1960** – **Hoffman**). Metodotologia per indicizzazione di documenti normativi.

Giuritecnica (**1970** – **Frosini**). Studio delle metodologie risultanti dall'applicazioni tecnologiche al diritto. Tra i primi ad occuparsi del diritto all'informazione, tutela della privacy e brevettabilita' del software.

Nella sua **prima fase** (1950-1975) il rapporto tra diritto ed informatica viene esaminato quasi esclusivamente in termini di applicabilita' dei calcolatori per semplificare il lavoro del giurista.
Consentire ad un giudice di esaminare una questione pratica adeguatamente formalizzata fino a giungere ad una sentenza.

Diritto dell'Informatica

Dal momento che il diritto regola la vita e l'esistenza contemporanea e' caratterizzata dall'impatto pervasivo delle tecnologie informatiche, il diritto e' chiamato ad occuparsi di quest'ultime.

Il **normativamente lecito** e' definito come un sottoinsieme di cio' che e' **tecnicamente possibile**. Si puo' anche arrivare ad affiancare la tutela giuridica con misure tecniche che rendano tecnicamente impossibili alcune azioni illecite (es. crypto).
Creazione di un **equilibrio** che non permetta alla tecnica di prevalere sul diritto, ma neppure al diritto di limitare le potenzialita' della tecnologia.
Si presenta l'esigenza di rinnovare costantemente le discipline giuridiche per adattarsi alle nuove tecnologie ed agli effetti sulla societa'. Se un certo settore non e' regolamentato dal diritto, sara' il settore privato e i limiti tecnici a fare la legge.

Societa' **dell'informazione**. Societa' industriale avanzate basate sulla centralita' dell'informazione e della conoscenza quali risorse essenziali per lo sviluppo economico, sociale e culturale.
Si parla anche di **societa' postindustriale** per evidenziare che la caratteristica predominante non e' la produzione di beni materiali.
Con Internet c'e' una crescita esponenziale delle informazioni e conoscere diventa semplice. Le tecnologie **integrano** e potenziano le **capacita**' umane.
Vengono **abbattuti ostacoli** geografici tipici della realta' fisica e le **interazioni** sono unicamente fondate sugli interessi. Si creano **sinergie inedite** ed emerge il concetto di **intelligenza collettiva** dove il singolo diviene protagonista.

Convergenza tecnologica: contenuti, servizi ed informazioni sono veicolati dallo stesso strumento.

Problematiche inedite. Rischi di esclusione, privacy, sicurezza delle infrastrutture e dei dati.
Fine anni 60 emerge la problematica relativa alla tutela giuridica del software. Fine anni 70 il tema della protezione dei dati personali. In **Italia** solo negli anni 90 vedono la luce numerosi interventi normativi. Esempi:

- 1992 modifica la legge del **diritto d'autore** del 1940;
- 1993 introduzione nel codice penale fattispecie di **diritto penale** dell'informatica;
- 1996 istituzione del garante per la tutela dei **dati personali**;
- 1997 documento informatico e **firma digitale**.

A differenza della rivoluzione industriale, dove gli stati potevano fornire risposte piuttosto autonome, con la rivoluzione digitale c'e' l'esigenza di **soluzioni condivise** a **livello sovranazionale**.

Peculiarita' della materia:
- **intangibilita'** dell'oggetto (le informazioni)
- **identita' digitale** dei soggetti
- **superamento confini** spazio-temporali
- **trasversalita'** delle tematiche

Tematiche:
- **Identita' digitale e privacy** (diritto privato). Trattamento dati personali e tutela.
- **Costituzione e tecnologie** (diritto pubblico). Diritti civili e rapporto tra cittadini e istituzioni.
- **Documento informatico** (diritto privato e pubblico). Garantire certezza e validita' giuridica.
- **Amministrazione digitale** (diritto pubblico). Tecnologie nell'organizzazione pubblica.
- **Contratti e commercio elettronico** (diritto privato). Scambi svolti attraverso la rete.
- **Nomi a dominio** (diritto privato). Protezione della presenza in rete.
- **Tutela dei beni informatici** (diritto privato). Tutela della proprieta' intellettuale del software.
- **Responsabilita' del provider** (diritto civile). Coinvolgimento e responsabilita'.
- **Reati informatici** (diritto penale). Reati commessi tramite strumenti informatici.
- **Informatica forense** (vari ambiti). Raccolta digital evidence per procedimenti giudiziari.
- **Internet Governance**. Gestione di Internet e ruolo degli Stati.

Identita' Digitale e Privacy

Dopo la seconda guerra mondiale quasi ogni ordinamento giuridico, ha sancito l'inviolabilita della **vita privata**, il **domicilio** e la **corrispondenza** degli individui.

1948 - Parigi - **Dichiarazione universale dei diritti umani** da parte dell'ONU. Priva di natura strettamente giuridica, ma di grande significato morale e per lo sviluppo attorno ai temi trattati.

1959 - Roma - **Convenzione europea salvaguardia diritti dell'uomo** (CEDU). Trattato con valenza giuridica che sottolinea l'inviolabilita' della vita privata, domicilio, corrispondenza.

1981 - Strasburgo - **Convenzione 108.** Protezione delle persone rispetto al trattamento automatizzato dei dati personali e stabilisce delle regole per il flusso transfrontaliero.
Dato personale (def). *Informazione concernente una persona fisica identificata o identificabile*.
I dati personali devono essere:
- ottenuti ed elaborati lealmente e legalmente;
- registrati per fini legittimi;
- esatti ed aggiornati;
- non eccessivi in rapporto ai fini;
- conservati per un periodo non superiore a quanto necessario.

Ogni persona ha diritto di:
- conoscere l'esistenza di dati che lo riguardano

- ottenere all'occorrenza la rettifica o cancellazione dei dati

Dati speciali. Dati che rivelano origine razziale, opinioni politiche, religione, salute, vita sessuale, condanne penali. Ne e' proibita l'elaborazione automatica a meno di garanzie appropriate.

1995 – Direttiva UE 95/46. Introduce la figura del **Garante**. E' stato fino ad oggi il principale documento normativo relativo alla privacy dei dati.

2003 - Dlgs 196/2003 (*Codice privacy*). Attuazione della direttiva europea in **Italia**.
Trattamento dati: qualunque operazione effettuata anche senza l'impiego di strumenti elettronici (raccolta, organizzazione, conservazione, consultazione, elaborazione, modifica, diffusione, ...).
Protagonisti trattamento:

- ***Interessato***: persona fisica a cui si riferiscono i dati;
- ***Titolare***: persona fisica o giuridica a cui spettano decisioni sulle finalita' e modalita';
- ***Responsabile***: persona fisica o giuridica responsabile del trattamento (esterna);
- ***Incaricati***: persone fisiche autorizzate al trattamento.

Strumenti per rendere esercitabili i diritti della normativa: **informativa** e il **consenso** al trattamento.
Per l'effettivita' della tutela sono risultati fondamentali i precisi **obblighi** e le puntuali **sanzioni**.

2016 – UE 2016/679 (GDPR). Regolamento che a partire dal 2018 sostituisce la direttiva 46. E' un regolamento, quindi vincolante.

Trasferimento dati verso gli USA
Negli Stati Uniti la protezione dei dati personali non e' un diritto fondamentale. L'accesso ai dati e' ritenuto importante per la lotta al terrorismo (soprattutto dopo l'11 settembre 2001).
Approdo sicuro (2000): autocertificazione delle compagnie USA riguardo la conformita' agli standard europei. Nel 2015, a seguito di vari episodi, la corte ha annullato l'accordo. Significative le rivelazioni di *Snowden* riguado al monitoraggio del NSA (*Datagate* 2013).
Ad oggi le autorita' nazionali UE valutano caso per caso se trasferire i dati e si assiste ad una conseguente modifica delle informative per richiedere il consenso al trattamento dei dati all'estero.

Diritto all'oblio
E' il diritto ad "*essere dimenticati*", una variante del diritto alla riservatezza.
Quando vecchie vicende, un tempo di pubblico dominio, possono essere oggetto di nuova divulgazione e quando invece il trascorrere del tempo ha reso tale divulgazione illecita.
Un tempo l'unico arbitro era lo Stato a cui era affidato il compito di **bilanciare** il diritto alla privacy con il diritto all'informazione. Ad oggi tale ruolo e' lasciato sempre piu' nelle mani di attori privati.
Il problema non e' quello della ripubblicazione della notizia, ma la sua permanenza in rete a causa dell'**indicizzazione** dai motori di ricerca.
Anche se, in pratica, l'obiettivo di essere dimenticati risulta irraggiungibile, l'interessato ha comunque diritto all'aggiornamento delle notizie che lo riguardano.

Diritto alla deindicizzazione.
L'attivita' di un motore di ricerca, qualora coinvolga informazioni contenenti dati personali, deve essere qualificata come **trattameto** di dati personali e il gestore del motore e' il **responsabile** ai sensi della disciplina europea sulla privacy. La presentazione dei dati personali puo' quindi costituire violazione della normativa con l'obbligo del responsabile alla deindicizzazione dei risultati.

Ad oggi, ai risultati di ricerca Google in Europa segue la dicitura: "*alcuni risultati possono essere stati rimossi nell'ambito della normativa europea sulla protezione dei dati*".
Google (per evitare casi come Google Spain) spinge a richiedere, prima di intraprendere qualsiasi azione legale, la rimozione dei risultati direttamente a lui (*judex in causa sua*).
Nessuno deve essere giudice nella propria causa ed e' fondamentale la **terzeita**' del giudice.

Costituzione e Tecnologie Informatiche

Si pone il problema della capacita' delle costituzioni di regolare diritti e liberta' nella societa' tecnologica. C'e' bisogno di soluzioni che superino i confini nazionali.

Domandarsi se necessario intervenire sulle costituzioni meno recenti con nuove norme o se e' sufficiente un interpretazione evolutiva delle norme esistenti.
Alcuni Stati hanno scelto la via della **modifica** altri la via dell **interpretazione**.
Le carte costituzionali piu' recenti hanno potuto assorbire l'impatto delle tecnologie. In alcune vi troviamo riferimento esplicito (es. costituzioni anni 70 come quella spagnola e portoghese).

L'**accesso ad Internet** ad un prezzo ragionevole e' condizione necessaria per l'esercizio della liberta' di espressione ed altre liberta' fondamentali gia' tutelate dalle costituzioni.
Il regolamento europeo **2015/2129** stabilisce le misure riguardanti l'accesso ad un Internet aperta ed il principio di ***neutralita'*** della rete.

In **Italia** la costituzione non contiene riferimenti espliciti alle tecnologie informatiche.
Il diritto di accesso ad Internet puo' essere ancorato al primo comma dell'**articolo 21**: *liberta' di espressione con ogni mezzo di diffusione*, interpretato come liberta' non solo di informare ma anche di informarsi.
Attraverso l'interpretazione evolutiva degli articoli 2 e 3 e' possibile includere molteplici liberta' coinvolte dalle tecnologie informatiche.
Art.2. *Lo Stato garantisce i diritti inviolabili dell'uomo, sia come singolo che nelle formazioni sociali dove si svolge la sua personalita'*.
Art.3. *E' compito dello stato rimuovere gli ostacoli che limitano la liberta' e l'uguaglianza dei cittadini, impediscono il pieno sviluppo della persona e limitano la partecipazione sociopolitica.*
Nell'art.2 e' possibile ritrovare i diritti **all'anonimato**, **data protection**, **oblio**, etc.
Nell'art.3 e' possibile trovare il diritto di **accesso** alla rete ed il principio di **net-neutrality**

Non manca chi richiede un riconoscimento esplicito attraverso un **integrazione** della costituzione stessa. L'interpretazione evolutiva rischia di non cogliere a pieno i diversi aspetti delle nuove liberta', rischiando di favorire l'autoregolamentazione.

Internet Bill of Rights (**dichiarazione dei diritti in Internet**).
In **Italia** nel **2014** la Camera dei Deputati ha nomitato una **commissione** per i diritti ed i doveri relativi ad Internet (coordinata da Rodota') col fine di elaborare una dichiarazione dei diritti in Internet.
La dichiarazione e' priva di forza vincolante giuridica e quindi non mancano critiche sulla sua utilita'.
Indica principi e direzioni per possibili sviluppi normativi.
Articoli divisi in 3 macro aree:

Fruizione della rete

- *Accesso ad Internet*
- *Conoscenza ed educazione*
- *Neutralita' della rete*
- *Governo della rete*

Identita' digitale e privacy

- *Tutela dati personali*
- *Autodeterminazione informativa*: accesso alle infomazini sulla propria persona.
- *Diritto all'identita'*: rappresentazione integrale ed aggiornata dei propri dati.
- *Protezione dell'anonimato*: contrasto con comportamenti illeciti
- *Diritto all'oblio*

Sicurezza

- *Diritto all'inviolabilita' dei sistemi*
- *Trattamenti automatizzati*: nessun atto o provvedimento e' completamente automatizzato
- *Garanzie sulle piattaforme*: l'individuo che vi accede e' il soggetto debole
- *Sicurezza in rete*: tutela da attacchi ma anche da fenomeni come hate speech e cyberbullismo.

Digital divide.

Divario tra chi accede ed utilizza le tecnologie informatiche e chi ne e' escluso.
Cause principali: culturali, geografiche, anagrafiche, economiche, disabilita'.
Dal digital divide scaturisce il nuovo **analfabetismo digitale**.
Legge Stanca (2004). Disposizioni per favorire l'accesso ai soggetti disabili agli strumenti informatici.
Il **CAD** (dlgs **82/2005**) approfondisce il diritto di accesso non soltanto sotto il profilo tecnico ma anche sotto l'aspetto culturale, rileva la necessita' di competenze al fine di poter utilizzare l'accesso messo a disposizione e *coglierne il valore, le opportunita' e i rischi*.
Lo Stato e' tenuto a promuovere iniziative volte a favorire la diffusione della cultura digitale.

E-Democracy.

Utilizzo delle tecnologie nelle diverse fasi del processo democratico al fine di promuovere il **coinvolgimento** nella sfera pubblica e la **partecipazione** ai processi decisionali.
Si va dalle newsletters, sondaggi e forum fino ad arrivare al **voto elettronico**, potenziale strumento per combattere l'astensionismo. Terminali posizionati nei seggi elettorali o in luoghi pubblici.
L'**home voting** ad oggi non e' abbastanza sicuro sia da attacchi cyber che da attacchi fisici. I problemi afferiscono all'art. 48 della costituzione: "*il voto e' personale, libero e segreto*".

Dichiarazione di indipendenza del cyberspazio (***Barlow*** **1996**). La rete vista come uno spazio spontaneo e libertario con una propria regolazione giuridica retta dalla self-regulation degli utenti.
Utopia dell'***agora'*** **digitale**, di una nuova democrazia *dal basso* caratterizzata da un ampia liberta'.
In realta' pero' la rete ha fatto emergere **nuovi poteri**, esercitati da soggetti privati a livello globale e guidati da interessi economici.
Per sfruttare a pieno le potenzialita' di Internet devi passare da loro. Trading di informazioni personali in cambio di servizi con il rischio di scivolare in una societa' del controllo e della sorveglianza.
Le "condizioni generali del servizio" dei tech giants generano norme la cui violazione produce conseguenze. Tali regole sono accettate piu' o meno consapevolmente dagli utenti.

Documenti Informatici e Firme Eletroniche

Documento elettronico: qualsiasi contenuto digitale contenente **atti** e **fatti** giuridicamente rilevanti.
La **firma elettronica** e' lo strumento di identificazione e imputazione del documento elettronico.
Tipo firme

- **autografa**: segno apposto sul documento cartaceo
- **elettronica**: sequenza binaria riconducibile al soggetto

eIDAS (Electronic IDentification, Authentication and trust Services): regolamento europeo del 2014 per le firme elettroniche, transazioni elettroniche e tutela delle parti coinvolte per aumentare la sicurezza del business online.
Definisce tre tipologie di firma elettronica:

- **Semplice**: strumento che consente di associare dei dati ad un identificativo unico, la firma (es. password). Sul piano probatorio ha lo stesso valore del doc informatico non sottoscritto e la valutazione e' rimandata a posteriori al giudice.
- **Avanzata**: creata mediante dati che il firmatario puo' usare sotto il proprio esclusivo controllo e collegata ai dati sottostanti in modo da consentire l'identificazione di eventuali modifiche (es. firma grafometrica). In sede probatoria fa piena prova fino a querela del falso.
- **Qualificata**: firma avanzata creata da un dispositivo supportato da un certificato qualificato.
  In sede probatoria fa piena prova a meno di prova del falso.
  Digitale: firma qualificata basata su un sitema di chiavi crittografiche asimmetrico.

Il **certificato** di firma elettronica e' un attestato elettronico che collega i dati di convalida di una firma elettronica ad una persona fisica. Il certificato qualificato e' un certificato rilasciato da un prestatore di servizi fiduciari qualificato (**terzo garante**).
La **firma autenticata** e' una firma sottoscritta in presenza di un notaio o un pubblico ufficiale. Ha maggiore valore probatorio.

In **Italia** il dlgs **179**/**2016** e' intervenuto per adeguare la normativa ad eIDAS, applicando le dovute modifiche al CAD (dlgs 82/2005) introducendovi le principali norme relative al documento informatico e le firme elettroniche.

Posta elettronica certificata

La **PEC** nasce per rimediare alle debolezze della email classica tramite ricevute opponibili a terzi. Paragonabile alla raccomandata con ricevuta di ritorno. Caratteristiche:

- verifica del mittente
- verifica di integrita'
- certezza dei momenti di invio e ricezione

La credenziali del servizio sono rilasciate dal provider previa **verifica dell'identita**'. Il provider garantisce la qualita' del servizio, l'integrita' del messaggio e le ricevute di presa in carico e consegna.
I log sono conservati dal provider per almeno 30 mesi.
Il messaggio si intende consegnato se reso disponibile all'indirizzo dichiarato.
Entrambe le parti devono usare un indirizzo PEC, questo lo rende un **sistema chiuso**.
Inoltre al momento e' un sistema applicabile solo all'interno del territorio nazionale italiano.

Permette la valida presentazione di istanze e dichiarazioni per via telematica alla pubblica amministrazione.
Al fine di incentivarne l'utilizzo e' previsto l'obbligo di un indirizzo PEC a carico di pubbliche amministrazioni, imprese e liberi professionisti.
Fra i diritti digitali previsti dal CAD il cittadino ha la possibilita' di indicare al comune di residenza il proprio domicilio digitale (PEC).
Elenchi PEC pubblici tenuti dall'Agenzia per l'Italia Digitale (**AgID**): IPA (amministrazioni), INI-PEC (imprese e professionisti) e ANPR (anagrafica nazionale popolazione residente).

Contratti

Contratti **digitali**: conclusi tramite l'uso delle tecnologie
Contratti **telematici**: contratti digitali conclusi a distanza.

Commercio **diretto**: le transazioni si svolgono interamente online
Commercio **indiretto**: alcune fasi si svolgono online, mentre altre, come la consegna, si svolgono in modo tradizionale.

Tipologie per **soggetti** coinvolti: *B2B* (business to business), *B2C* (business to consumer), *C2C* (consumer to consumer), *C2A* (consumer to administration), *B2A* (business to administration).

Internet consente di instaurare rapporti tra soggetti che fanno parte di ordinamenti giuridici diversi. La decentralizzazione e delocazione provoca la **spersonalizzazione** del contratto.
La spersonalizzazione offre vantaggi agli operatori professionali, ma nuovi pericoli per gli utenti.
La materia e' articolata e complessa, composizione di norme nazionali e internazionali.

Per l'individuazione dei **contraenti**, con la conseguente imputabilita' delle manifestazioni di volonta' e degli effetti del contratto, vengono in aiuto le firme elettroniche.
Molto spesso, al fine di favorire la rapidita' nei rapporti contrattuali, si assiste ad un "aformalismo negoziale" e si usa una firma debole.
Sul **luogo** di conclusione, le norme non forniscono particolari indicazioni. Solitamente il criterio e' scelto dalle parti e in assenza si applica la legge del paese con cui il contratto presenta un collegamento piu' stretto, ed eccezione del *B2C*, dove si applicano le normative del paese del consumatore.
Sul **tempo** di conclusione, il contratto si ritiene concluso al momento in cui e' eseguito il pagamento.

Le tecnologie possono essere usate anche solo come mezzo di comunicazione (es. contratto via mail).
Il valore giuridico del contratto variera' a seconda della tecnologia impiegata (es. PEC vs mail).
Laddove l'accettazione non sia conforme alla proposta varra' come nuova proposta.

Nel caso di contratti perfezionati via web per mezzo dell'accesso alla **vetrina virtuale** del sito, questo puo' riportare tutti gli elementi necessari del contratto ed in tal caso il sito proporra' un *offerta al pubblico*. In caso contrario, si trattera' di un *invito ad offrire* e la risposta all'invito non sara' in tal caso un accettazione, ma varra' come proposta.

Amministrazione Digitale

Nella pubblica amministrazione si pongono esigenze piu' stringenti per garantire la validita' giuridica delle attivita' espletate e dei documenti digitali generati, trasmessi e conservati.

Amministrazione digitale (e-government): l'organizzazione delle attivita' dell'amministrazione pubblica fondata sull'adozione delle tecnologie informatiche.
Non solo automatizzazione dei processi ma anche riorganizzazione della struttura interna, reingegnerizzazione dei processi e un nuovo rapporto con l'utenza.
Obiettivi: qualita' dei servizi ed efficienza e quindi maggiore soddisfazione degli utenti.

Il **CAD** (**dlgs 82/2005**) e' la norma di riferimento in materia, oggetto di ripetute modifiche ed integrazioni nel corso degli anni.
Dal 2012 CAD delega all'**AgID** le funzioni di programmazione, monitoraggio, coordinamento, emanzione di regole e vigilanza.
Per incentivare l'attuazione delle disposizioni il CAD ricorre ad **obblighi** e **sanzioni** a carico delle amministrazioni.

Open government
Seguendo il principio di *openness* l'e-government e' maturato negli anni verso l'**open-government**, modello secondo cui i governi e le amministrazioni devono essere **trasparenti** a tutti i livelli.
Approccio orizzontale **multistakeholder**, orientato a favorire i processi decisionali per mezzo del dialogo con la collettivita', raccolta di proposte, osservazioni e feedback.
La trasparenza favorisce l'**accountability** delle amministrazioni.
Esempi:

- partecipa.gov.it : consultazione e partecipazione pubblica in Italia.
- decidim.org : consultazione e partecipazione pubblica in Spagna.

L'**Italia** ha aderito all'iniziativa internazionale **Open Government Partnership** (OGP) promossa nel **2011** e tesa a favorire l'apertura dei governi.
In Italia lo Stato, le Regioni e le autonomie locali sono tenute, ai sensi del **CAD** ad assicurare la gestione, l'accesso e la conservazione dell'informazione in modalita' digitale organizzandosi autonomamente nella scelta degli strumenti specifici secondo il principio di **neutralita**' **tecnologica**.
Il CAD si applica a tutte le pubbliche amministrazioni (nazionali, regionali e locali), alle societa' a controllo pubblico (escluse societa' quotate) e ai privati (per attivita' documentale e comunicazioni).
Sono esclusi dall'applicazione della normativa istituzioni di controllo fiscale, sicurezza pubblica, sicurezza nazionale e polizia giudiziaria.

Cittadinanza digitale
La configurazione dei **diritti** dei cittadini nei confronti delle istituzioni, resa possibile dalle tecnologie.
Questi diritti hanno come presupposti necessari il diritto di accesso ad Internet e il diritto di alfabetizzazione informatica dei cittadini.
L'AgID e' tenuta a pubblicare sul proprio sito una guida di riepilogo dei diritti di cittadinanza digitale previsti dal CAD. Alcuni esempi:

- domicilio digitale delle persone fisiche.
- comunicazioni telematiche delle imprese con le istituzioni (via PEC).
- effettuazione dei pagamenti online.

- qualita' dei servizi e misura della soddisfazione.
- partecipazione democratica elettronica (e-democracy).

Alla provisione di diritti corrisponde il **dovere** di renderli effettivi da parte dell'amministrazione pubblica, chiamata a rispondere in caso di mancato rispetto delle disposizioni.
La performance organizzativa dei dirigenti e' cosi' misurata tenendo conto dell'attuazione delle disposizioni del CAD.
Un **responsabile transazione digitale** (RTD) deve essere individuato in ogni amministrazione e deve essere in posseso di adeguati requisiti di imparzialita', autonomia e competenza. Tale soggetto deve eventualmente inviare segnalazioni e reclami per violazioni all'ufficio per le segnalazioni disciplinari.
Caso di studio. Nel 2011 TAR Basilicata contro la Regione Basilicata per il disservizio. Assenza di almeno un indirizzo PEC sul sito e mancata attuazione del diritto degli utenti di comunicare telematicamente con le amministrazioni.

Attivita' documentale
CAD vuole garantire ai cittadini il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalita' digitale.
Le amministrazioni sono tenute a formare gli originali dei propri documenti e gestire i procedimenti con mezzi informatici.
Previste comunicazioni telematiche nei rapporti tra le pubbliche amministrazioni.
Nei rapporti con i privati l'obbligo del canale digitale varia a seconda del soggetto privato. Nei rapporti con le imprese e' prevista espressamente l'esclusiva modalita' digitale.

Identita' digitale e servizi online
SPID (Sistema Pubblico per la gestione dell'Identita' Digitale). E' un sistema di autenticazione che permette a cittadini ed imprese di accedere con un unica identita' digitale ai servizi di pubbliche amministrazioni e imprese aderenti.
SPID e' rilasciata a domanda dell'interessato da identity providers accreditati da AgID.
Per garantire una certa qualita' dei servizi ai soggetti cui si applica il CAD, le piattaforme devono consentire agli utenti di esprimere la soddisfazione rispetto alla qualita' del servizio, pubblicando sui propri siti i risultati. In caso di violazione gli interessati possono agire in giudizio (class action).
Devono essere rilevati strumenti idonei alla rilevazione continua e sicura del giudizio degli utenti.

Open data

Strumento necessario ai modelli di open government. Restituire dati alla collettivita' e lasciare che l'intelligenza collettiva ne faccia uso (dati geografici, ambientali, sanitari, etc.)

Secondo ***Open Knowledge Foundation***, un dato si definisce **aperto** se chiunque e' in grado di riutilizzarlo e ridistribuirlo, con l'eventuale limitazioni della richiesta di attribuzione e condivisione nello stesso modo.

Secondo il CAD un dato e' aperto se presenta le seguenti **caratteristiche**:
- disponibile secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque;
- disponibile gratuitamente o a costi marginali (sostenuti per la loro riproduzione o divulgazione).
- accessibile e processabile tramite le tecnologie informatiche;

Open data e' anche strumento di prevenzione e lotta alla corruzione. Generando maggiore fiducia nelle istituzioni, garantisce partecipazione e coinvolgimento. Miglioramento delle politiche pubbliche in quanto di supporto alle decisioni.

Principio ***open data by default***, i dati pubblicati dalle amministrazioni e senza l'esplicita adozione di una licenza per il riutilizzo si intendono rilasciati come open data (eccetto dati personali),
Nel caso di dati personali, l'obbligo di pubblicare i dati in *formato aperto* non implica che siano anche dati aperti, cioe' liberamente utilizzabili da chiunque.
Open data deve scontrarsi con la tutela di altri interessi protetti dall'ordinamento quali il segreto di stato, segreto statistico, diritto d'autore, privacy e sicurezza pubblica.

Nel 2011 il governo ha lanciato il portale www.dati.gov.it, un catalogo aperto di dati pubblicati dalle varie amministrazioni locali.

Big data

Enormi volumi di dati detenuti da grandi organizzazioni, quali governi e multinazionali, provenienti da diverse fonti e analizzati da tecnologie specifiche e tecniche di **data mining** (pattern discovery in large data sets).

Vi si possono trovare tracce digitali provenienti da diverse fonti: forniti sui social networks su base volontaria, dati scambiati o comprati, dati forniti in modo meno consapevole (es. GPS del telefono), dati ricavati da altri dati, dati raccolti dallo Stato, etc.
Il fenomeno e' destinato a crescere con l'IoT.
Capacita' **predittiva** dei big data: consentono di interpretare bisogni ed esigenze, profilare gli utenti, monitorare i consumi e suportare le istituzioni nelle scelte.
Istat ha istituito nel 2016 il **Big Data Committee** con il compito entro il 2020 di definire policy a supporto dell'uso dei big data per la statistica ufficiale.

Non c'e' nessuna definizione nell'ordinamento giurdico. Neanche il GDPR ne parla esplicitamente.
Come per gli open-data, puo' crearsi una certa frizione fra big data e protezione della privacy.
Le grandi aziende si atteggiano a "proprietari" dei nuovi dati prodotti dalla combinazione di dati di cui sono titolari i soggetti terzi.
I soggetti pubblici possono servirsi delle banche dati dei soggetti privati per attivita' di sorveglianza.
Il quadro giuridico non risulta del tutto idoneo per la regolamentazione dei big data.
Per riequilibrare l'asimmetria informativa tra i pochi big players e gli altri, e' possibile pensare ad una sanatoria, rilasciare i dati come "**open big data**" anche se comporterebbe una notevole perdita di potere per le grandi aziende e probabili problemi di privacy.

Diritto dei Privati

Nomi a dominio

Segni distintivi identificanti un nome di un soggetto (privato, impresa, etc).

Il valore distintivo deriva dalla riconduciblita' del nome a dominio ad un'attivita', un prodotto, un servizio. Questo valore ha provocato la conseguente attenzione del diritto ai nomi di dominio.
Si leggono da destra verso sinistra. Il primo livello e' il **TLD** (top-level domain), seguito dal SLD (second level domain), seguito da eventuali sottodomini.
Il TLD puo' indicare la nazionalita' (country code – **ccTLD**) o la categoria (generic – **gTLD**).
DNS: sistema che traduce i nomi in indirizzi IP.
ICANN (Internet Corporation of Assigned Names and Numbers) – societa' internazionale non-profit con in carico la gestione delle assegnazioni e risoluzione delle controversie per i nomi di dominio. Delega i compiti ad autorita' territoriali, le **Registration Authorities**.

Oggi e' tutelato dal codice della proprieta' industriale (2005). La normativa pone aspetti determinanti per la risoluzione di eventuali controversie. Esempi:

- *Divieto di adottare insegna o nome a dominio uguale o simile all'altrui marchio se puo' causare confusione per il pubblico nel caso di attivita' affini.*
- *Il divieto si estende anche nel caso di attivita' non affini, se l'uso del marchio possa trarre indebitamente vantaggio per la fama del marchio*.

Passive domain holding: registrazione di un nome a dominio identico al marchio altrui senza utilizzarlo
Cybersquatting: passive domain holding con finalita' di profitto.
Typosquatting: registrare nomi a dominio monto simili a marchi o nomi altrui (e.s rnicorosoft.com).
E' proibito l'uso del marchio di un altro soggetto anche nei *metatag* per sfruttarne in modo parassitario i vantaggi.

Diritto d'autore

Le tecnologie permettono una facile diffusione dei contenuti digitali e quindi aumentano in modo esponenziale le modalita' di circolazione e fruizione dei contenuti, incidendo in modo significativo sulla **proprieta' intellettuale**.

Il diritto d'autore e' disciplinato in Italia dalla legge **633/1941** del codice civile e protegge le opere dell'ingegno di carattere creativo (scienze, letteratura, musica, etc). La 633 e' stata successivamente estesa per la tutela del software.
La **creazione** dell'opera e' condizione sufficiente all'acquisto del diritto d'autore e comporta l'acquisizione automatica dei diritti collegati e la connessa tutela, non e' richiesta alcuna formalita'.

L'autore ha il diritto esclusivo di pubblicare l'opera e di utilizzarla economicamente in ogni forma e modo. L'utilizzo puo' essere precluso a soggetti diversi dal titolare.
Il diritto d'autore e' pero' adatto ad una realta' analogica basata sul controllo fisico della circolazione delle opere. Il software e' intangibile ed e' quindi piu' difficile controllarne l'artefice e la diffuzione.
Nella rete spesso i contenuti digitali sono "*di seconda mano*", ossia distribuiti da terzi. Diviene difficile risalire all'autore originario per ottenere l'autorizzazione.
Da un punto di vista legale, per la 633, l'autore concede l'utilizzo tramite una **licenza**.
La tutela tradizionale consiste nel riservare tutti i diritti all'autore, anche se tali indicazioni sono superflue in quanto come gia' detto, si acquisiscono i diritti semplicemente con la creazione dell'opera.
Le licenze si dividono in: **proprietarie** ed **aperte**.

Creative Commons: licenze aperte che consentono all'autore di rendere liberamente accessibili i propri contenuti. Di sei sottotipi, frutto della combinazione di quattro diverse clausule:

- *Attribution* (**BY**) : riconoscimento paternita' dell'opera.
- *ShareAlike* (**SA**): ridistribuzione con le stesse modalita'.
- *NoDerivatives* (**ND**): non si autorizzano opere derivate.
- *NonCommercial* (**NC**): no scopi commerciali.

Le CC vietano l'apposizione di misure tecnologiche per la protezione dei diritti concessi (no DRM).

Materiale trovato in rete

- Licenza aperta: basta attenersi alla licenza.
- Nessuna licenza: necessario ottenere l'autorizzazione da parte dell'autore.

In alcuni siti il "*deep-linking*" e' proibito ed infrange la copyright policy dell'autore.

AgCom (Autorita' amministrativa per le garanzie delle Comunicazioni). Nel **2013** ha approvato il regolamento in materia di tutela del diritto d'autore online e che mira a promuovere l'offerta legale di opere digitali e l'educazione alla corretta fruizione delle stesse.
Per il regolamento AgCom, il titolare, qualora ritenga che una sua opera digitale sia stata resa disponibile in violazione della legge puo' presentare un istanza all'Autorita', chiedendone la rimozione. Entro 7 giorni l'Autorita', individuata l'istanza e il provider, avvia il procedimento istruttorio. Se il contenuto e' rimosso, allora l'istanza e' archiviata, altrimenti viene coercitivamente disabilitato l'accesso all'opera, applicando le sanzioni amministrative previste.

Per il software, dopo un dibattito che ipotizzava anche la **tutela brevettuale**, il diritto ha scelto la disciplina del **diritto d'autore**. Con esso si tutela l'implementazione di un idea e non l'idea stessa.
Per il software la **SIAE** offre, iscrivendosi ad un registro pubblico speciale, un'ulteriore tutela tramite una prova documentale.

Caratteristiche uso del software:

- **non-rivale**: piu' individui possono usare lo stesso software contemporaneamente;
- **non-escludibile**: una volta che l'utente ne e' in possesso, non possiamo impedirne l'uso.

Per rendere escludibile il suo uso occorrono misure tecnologiche e giuridiche aggiuntive.

Diritti inderogabili: copia di riserva, riprodurre, tradurre, studiare e testare allo scopo di determinare idee e principi (*reverse engineering*).

Open source. Possibile alterare il codice sorgente del programma. Nessun obbligo per il soggetto concedente. Caratteristiche **free software** per *Stallman*: liberta' di riprodurre, studiare, ridistribuire e migliorare. **Copyleft**: obbligo di ridistribuire il software modificato con la stessa licenza (*viral license*).
Closed source. Software distribuito senza codice sorgente, impedendone quindi tecnicamente la modifica e la ridistribuzione. Conseguente perdita della conoscenza e utilita' sociale.
Freeware. Distribuito gratuitamente in formato eseguibile.
Shareware. Come freeware ma per un periodo limitato (evaluation).
Double license. Open source e proprietaria per un prodotto piu' ricco.

Banche dati

Informazioni metodicamene archiviate ed accessibili tramite strumenti elettronici.

Tipologie banche dati per la proprieta' intellettuale:

- **selettive**: contenuti selezionati in modo originale;
- **dispositive**: e' originale l'organizzazione del materiale.

Per la scelta o la disposizione delle informazioni, queste costituiscono proprieta' intellettuale.
La tutela non si estende al contenuto.
Diritto del **costituitore** (autonomo rispetto al diritto d'autore). A prescindere dall'originalita' dei dati, tutela il costituitore assegnandogli il diritto di vietare l'estrazione o il reimpiego dei dati (dura 15 anni).
Casi in cui non e' richiesta l'autorizzazione del titolare: didattica, ricerca, sicurezza pubblica, procedure amministrative o giuridiche.

Responsabilita' del provider

Nelle telecomunicazioni, il **provider** e' il soggetto che esercita un attivita' imprenditoriale di prestatore di servizi:

- **connessione e trasporto**: es. mail o Internet service provider (**ISP**);
- **memorizzazione temporanea** (caching): es. proxy o search engines;
- **memorizzazione** (hosting): es. web server o storage.

Per la direttiva EU **2000/31** il provider non ha l'obbligo di sorveglianza sulle informazioni trasmesse o memorizzate dall'utente. Ne di ricercare fatti o circostanze che indichino attivita' illecite.
Il provider si limita ad un attivita di ordine meramente tecnico, automatico e passivo.
La responsabilita' insorge solo nel caso di conoscenza dell'illecita' dei contenuti. In tal caso deve informare immediatamente l'autorita' giudiziaria.

Nel caso di hosting, il provider **attivo** e' l'autore dei contenuti, il provider **passivo** e' chi presta la piattaforma. La responsabilita' e' del provider attivo.
Caso di studio: **ViviDown**. Piattaforme di video hosting come YouTube effettuano la selezione dei contenuti in base alla descrizione e non all'effettivo contenuto dei video.

Diritto Penale e Reati Informatici

Gli strumenti informatici offrono grandi possibilita' per chi voglia impiegarli per finalita' criminose.
Approccio normativo ai **Cybercrimes**:

- **evolutivo**: i nuovi reati sono inseriti in atti normativi autonomi (es. US);
- **organico**: i nuovi reati sono inseriti in un corpus gia' esistente (es. IT).

I primi attacchi hacker (80s) erano prevalentemente volti a mettere alla prova le proprie capacita'.
Oggi si assistono ad attacchi ad opera di cyber criminali di vario tipo a scopo di spionaggio o di lucro.
La raccomandazione **EU 89/9** riporta un elenco delle fattispecie criminose bisognose di un (al tempo) urgente riconoscimento giuridico.
La raccomandazione e' stata accolta in **Italia** con la legge **547/93** (modifiche al codice penale in tema di criminalita' informatica) e la legge 48/2008 (estensioni 547).

Fattispecie introdotte dalla 547.

- **Accesso abusivo** (3-8 anni). Vale anche in caso di accesso a risorse in modo non autorizzato all'interno di un sistema di cui abbiamo l'autorizzazione ad accedere.

- **Diffusione o uso di apparecchiature o software diretti a danneggiare** il funzionamento di un sistema informativo.
- **Falsificazione o alterazione** delle comunicazioni (1-4 anni).
- **Intercettazione o interruzione** illecita delle comunicazioni.
- **Installazione di apparecchiature di intercettazione o interruzione** delle comunicazioni. Pene leggermente piu' lievi rispetto all'utilizzo.
- **Danneggiamento dati o programmi** (6 mesi-3 anni).
- **Danneggiamento sistemi informatici** (1-5 anni).
- **Frode telematica** (6 mesi-3 anni). Rispetto alla *truffa*, nella frode informatica non si trae in inganno la vittima ma si altera un sistema informatico a proprio vantaggio.

Le pene per ciascuna delle fattispecie enumerate sono piu' gravi nel caso in cui a compierle sia un pubblico ufficiale o nel caso in cui siano coinvolti sistemi di interesse militare o pubblica sicurezza.

Il legislatore non poteva pero' prevedere l'emersione di nuovi fenomeni resi possibili dal successivo sviluppo tecnologico. In alcuni casi e' comunque possibile ricondursi a comportamenti illeciti gia' presenti nel nostro ordinamento. Negli altri casi gli strumenti di tutela risultano evanescenti.
Sono state inserite nel codice penale alcune norme che, se da un punto di vista formale non rientrano nei reati informatici, da un punto di vista sostanziale si: distribuzione materiale pedopornografico, cyberstalking, favoreggiamento attraverso fornitura di strumentazione, cyberterrorismo, cyberbullying (sfortunatamente quest'ultimo non ancora punito con un reato specifico).
Caso di studio: **Phishing**.

Procedimenti Giudiziari

Molti i tentativi di interpretare le norme come se fossero equazioni. Nell'ordinamento italiano sono state recentemente introdotte procedure automatizzate (in senso funzionale e non decisionale).

Processo Civile Telematico (PCT). Dpr **123/2001** "misure urgenti per digitalizzazione giustizia". Disciplina l'uso degli strumenti informatici nel processo civile, amministrativo e dinanzi alle sezioni giurisdizionali. Sopprerire all'annoso problema della lentezza che affligge cronicamente il contenzioso civile. Con specifico riferimento all'amministrazione della giustizia viene chiamato e-justice.
Nel **2014** il PCT ha esaurito la sua fase sperimentale, ponendo l'obbligo di **deposito telematico** dei ricorsi per decreto ingiuntivo e di tutti gli altri atti civili depositati dal legale successivamente alla costituzione in giudizio.
Consente la consultazione online di documenti, dati e fascicoli dei procedimenti in svolgimento.
Le attivita' sono svolte solo dai soggetti autorizzati che si autenticano attraverso **punti di accesso** gestiti da enti appositamente individuati.

Informatica Forense

Digital evidence. Qualunque informazione generata, memorizzata o trasmessa in formato digitale dotata di valore probatorio in un procedimento giudiziario.
Elementi probatori non soltanto di un reato informatico, ma di una qualunque tipologia di reato.
Classificazione: *human to human* (es. mail), *human to machine* (es. file di testo), *machine to machine* (es. file di log); dati volatili o persistenti.

Caratteristica principale e' l'**intangibilita'**, materialita' diversa costruita comunque di elementi fisici.
Ha una natura particolarmente modificabile, puo' essere facilmente (anche involontariamente) corrotta o manipolata. Solo tramite la corretta catena di custodia le prove digitali possono rimanere integre in tutti i loro passaggi, dal sistema di origine fino alla disponibilita' del giudice durante il dibattito.

La **convenzione di Budapest** (**2001**) e' il primo accordo internazionale sui temi di raccolta e conservazione della prova digitale. Alle parti aderenti (soprattutto providers) si pone l'obbligo di prevedere il **quick freeze** dei dati per un loro eventuale uso come prova forense.

Acquisizione **post-mortem**: quando il sistema e' trovato spento e l'acquisizione avviene dai dati persistenti. Se il sistema e' trovato attivo ogni operazione potrebbe compromettere l'integrita' dei dati (volatili e non volatili) e si deve procedere ad un'attenta analisi forense **live**.
L'attivita' di perquisizione deve essere effettuata con sistemi e tecniche idonee (es. accensione o spegnimento del pc puo' alterare il timestamp di alcuni files).
Tecniche: write blocker, image cloning, crypto hash per la verifica di integrita' dei dati clonati, etc.
Caso di studio: delitto di Garlasco.

Sfide Attuali e Future

Internet governance. Un server e' geograficamente situato in uno Stato. La vecchia sovranita' nazionale ha dunque ancora un ruolo ancora decisivo sulle nuove tecnologie.

ARPA (Advanced Research Projects Agency) nasce nel 58 (guerra fredda) con lo scopo di sviluppare una rete telematica che fosse meno centralizzata e quindi piu' resiliente ad eventuali attacchi fisici alle strutture.
ARPANET (68) collega 4 nodi: Uni di Los Angeles, Santa Barbara, Utah e lo Stanford Research institute.
Negli anni 70 viene adottato TCP/IP che consente la creazione di una rete di reti (Internet).

Inizialmente il **DNS** era gestito dalla stessa ARPA attraverso **IANA**. In seguito nasce **ICANN** un associazione non profit che pero' e' assoggettata al diritto californiano e legata da un contratto di consulenza al Dipartimento del Commercio degli USA. Quindi, nonostante si ponga come una associazione indipendente e sovrannazionale, in realta' e' un ente privato che svolge una funzione pubblica globale.
L'attuale gestione e' contestata da organizzazioni indipendenti per la tutela della liberta' e da attori statuali che non brillano in fatto di liberta' (es. Cina, Russia, Iran). Si sente l'esigenza generale di attribuire tale competenza ad un organizzazione veramente indipendente come l'ITU.

Cyberwarfare. Rispetto alla guerra tradizionale, c'e' l'illusione di una guerra non violenta e quindi se ne sottovalutano gli effetti. Non viene *dichiarata* e generalmente gli attacchi non sono *rivendicati*, rendendo difficile capire anche le motivazioni.
L'Estonia nel 2007 subisce 3 settimane di attacchi ricordati come ***Web War One***. A seguito dell'evento a Tallin e' istituito il **CCDCOE** (Cooperative Cyber Defence Center of Excellence). Il CCDCOE individua 95 regole applicabili alla cyberwarfare nel **Tallinn Manual** (**2013**).

Il manuale offre linee guida e parametri (e.g. severity, directness, invasiveness, etc).
Riconoscere un attacco cyber alla stregua di un attacco militare classico ha conseguenze giuridiche precise. Riconosciuto allo stato aggredito il diritto di reagire con la forza (quando raggiunge il livello di attacco armato).
Il manuale non ha forza giuridica vincolante, e' "*NATO centric*" ed e' praticamente ignorato da potenze come Russia e Cina.

Pirateria. Maggiore e' l'ostilita' del criminale nei confronti di chi afferma di detenere legittimamente il potere, maggiore sara' l'esigenza di repressione e quindi la pena. Il punto massimo di inimicizia e' stato costantemente assegnato a chi con le proprie azioni o pensiero minacciava il potere alle sue fondamenta. Alla massima figura di inimicizia e' sempre stata associata la figura del pirata.
La pirateria marittima colpisce in acque internazionali, e' quindi un crimine universale ed e' compito di tutti reprimerla.
La parola pirateria fu coniata nel 600 dal Vescovo di Oxford per indicare la riproduzione non autorizzata di libri.
Nessuno Stato del mondo crede che la violazione del copyright sia un fenomeno realisticamente sanzionabile. L'obiettivo della repressione non e' tanto quello di neutralizzare le infrazioni del diritto d'autore, piuttosto quello di neutralizzare i soggetti piu' pericolosi, quelli che predicano il vangelo del copyleft mossi da un insofferenza assoluta verso l'assetto attuale della diffusione della conoscenza.
Emerge non soltanto il movimento open source e del copyleft, ma anche il sabotaggio digitale e la diffusione dei documenti riservati (vedi wikileaks).