Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali

Jacopo Fortuna

Il rapporto tra diritto e nuove tecnologie

- Evoluzione del rapporto tra diritto e tecnologie digitali nella prospettiva comparatistica.
- Comunicazione della Commissione europea «Plasmare il futuro digitale dell'Europa», febbraio 2020.
- Decisione UE 2022/2481 del Parlamento Europeo e del Consiglio del dicembre 2022 che istituisce il «Programma Strategico per il decennio digitale 2030».
- La «trasformazione digitale» comprende: la sovranità digitale, l'inclusione, l'uguaglianza, la sostenibilità, la resilienza, la sicurezza e il rispetto dei diritti fondamentali, dello Stato di diritto, e della democrazia.

La trasformazione digitale ha un rapporto stretto col diritto:

1- Il diritto crea la cornice normativa che consente detta trasformazione;
2- Il diritto assicura che la trasformazione avvenga nel modo desiderato, ad esempio nel rispetto dei diritti fondamentai degli individui;

Diritto e tecnologia: esiste un rapporto simbiotico tra diritto e attività umane che, sfruttando le acquisizioni della scienza, creano nuovi strumenti atti a migliorare la vita dell'uomo.

- Il rapporto tra diritto e nuove tecnologie non è tipico solo delle epoche più recenti.

- Il diritto si è sempre posto in relazione con le tecnologie.

- La scrittura è, ad esempio, una tecnologia ed è stata inventata dall'uomo per perseguire obiettivi fondamentali per il diritto, come la documentazione, ed è stata importate anche per fondare e far rispettare istituti giuridici come la proprietà.

- Oggi al centro del dibattito ci sono le tecnologie digitali, ma esse non sono più tecnologia di quanto non lo siano la carta, la penna o lo stesso linguaggio, che è una forma di tecnologia del pensiero.

Tecnologie che hanno permesso all'uomo di affrancarsi dalla preistoria:

Parole: rappresentazione del pensiero;
Scrittura: permette la descrizione del mondo;
Carta: consente alla scrittura di mantenersi stabile nel tempo e di poter circolare nello spazio;

In assenza di scrittura, carta e alfabetizzazione diffusa, i testimoni rappresentavano lo strumento per dare certezza e stabilità ai traffici e alle relazione giuridiche. Pertanto, tali tecnologie hanno inciso profondamente sul diritto e sulle sue caratteristiche.

Emersione di nuove tecnologie:

- usate dal diritto per perseguire propri obiettivi;
- possono portare alla creazione di nuove regole giuridiche;

- Evoluzione del diritto in chiave diacronica: step evolutivi del diritto si sono verificati quando l'uomo ha avuto accesso a nuove tecnologie.

- L'evoluzione del diritto coincide con l'evoluzione dei mezzi espressivi e delle tecnologie ad essi relative.

- Diritto c.d. muto (quando l'uomo si esprimeva solo a gesti): assenza di ogni forma di concettualizzazione.

- Prima innovazione tecnologica: disponibilità del linguaggio articolato (tecnologia del pensiero); conseguentemente cambia il diritto.

- Nelle società senza scrittura:
- il patrimonio giuridico viene consegnato alle generazioni successive in forma orale;
- Nella cultura orale la legge è custodita in massime formulaiche e in proverbi.
- La forma orale del patrimonio giuridico esclude l'astrazione e la generalizzazione e implica l'uso di formule brevi e ripetitive (antica Roma).

Avvento della scrittura (tecnologia della parola): il diritto evolve ulteriormente poiché la redazione delle leggi provoca un distacco del precetto giuridico dai fatti del caso e lo rende più generale e astratto.

Nasce l'interpretazione e il diritto diventa più tecnico, poiché il testo che riproduce la regola diviene fisso e può essere conservato inalterato.

Ulteriore progresso si ha con i caratteri a stampa:
- diffusione spaziale dello scritto;
- stabilizzazione e standardizzazione dei testi e del linguaggio;
- ulteriore premessa per concettualizzazioni e astrazioni;
- formazione di una classe di esperti: nasce la tradizione giuridica colta;

L’analisi diacronica dimostra che ogni stadio evolutivo del diritto deve alcune sue peculiarità dalle tecnologie utilizzate:

- Diritto c.d. muto diverso da quello delle società orali;
- Diritto delle società orali diverso dal diritto scritto;
- Diritto in contesti con ampio uso della stampa diverso dal diritto che si sviluppa dove sono presenti solo rari manoscritti;

In che modo il diritto disciplina fenomeni legati all’informatica e alla telematica? In che modo le nuove tecnologie digitali modificano il diritto?

- Le nuove regole giuridiche nate dall'emersione delle tecnologie informatiche presentano tratti caratteristici che possono portare a parlare di diritto dell'era digitale.

- Il termine «digitale» è un anglicismo, anche se l'origine è comunque latina, da «*digitus*» («dito»), che serve appunto per numerare. Infatti il termine digitale deriva da *digit*, che in inglese vuol dire «cifra», «numero».

- Il termine «digitale» richiama dunque la rappresentazione di un fenomeno attraverso i numeri.

- È la rappresentazione di un fenomeno in elementi c.d. discreti, cioè di un fenomeno di cui è possibile individuare le parti.

- Il termine «digitale» si contrappone infatti al termine «analogico», cioè non discreto.

- «Sono analogici i dispositivi che trattano grandezze rappresentate da altre grandezze legate alle prime da una relazione analogica».

- Rappresentazione del fenomeno attraverso i numeri: esistono vari sistemi di numerazione; il più familiare è il sistema decimale.

- La scrittura di numeri in base 2, in cui esistono solo le cifre 0 e 1, è la notazione posizionale più semplice ed essenziale e viene definita «sistema binario».

- La locuzione «carattere binario» rimanda all'inglese *binary digit* (cifra binaria) e dalla crasi di questi due termini è nato il termine *bit*.

- Per *bit* si intende un'unità di informazione che può essere rappresentata da zero a uno.

- Nella notazione in base 2 è implicita la logica binaria (c'è - non c'è; acceso - spento; vero – falso).
- Attraverso la logica binaria vengono registrati tutti i dati all'interno del calcolatore.
- Ogni informazione, anche la più elaborata, può essere ridotta a una sequenza di 0 e di 1.

La logica binaria innerva l'era digitale, che include in sé operazioni come:

- Rappresentazione: rappresentazione di tutte le forme espressive (testi, suoni, immagini) in notazione binaria;

- Elaborazione: il codice binario può essere trattato ed elaborato mediante strumenti automatici come i computer (il termine informatica nasce dalla crasi dei termini francesi «*information*» e «*automatique*»);

- Comunicazione: convergenza tra le tecnologie informatiche e le tecnologie della comunicazione (il termine «telematica» deriva dall'unione di «telecomunicazione» e «informatica»).

COMPARAZIONE GIURIDICA E NUOVE TECNOLOGIE

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali

Jacopo Fortuna

Lezione 2

La relazione tra diritto e società

- Che cos'è il diritto?
  - *Diritto = legge?*
- Le diverse relazioni tra diritto ed altri fenomeni del sociale
  - Il diritto religioso
  - Il diritto consuetudinario
  - Il diritto laico

Caratteristiche principali del diritto laico

Il soggetto giuridico al centro del sistema dei diritti

La territorialità

Il principio dello Stato di diritto

Giuristi professionisti

Diversi contenuti e diversi stili del diritto sulla base dell’area geografica in cui si sviluppa

L’esposizione universale del 1900 a Parigi e la nascita degli studi comparatistici.

- *Problema della diversità nazionale delle legislazioni.*

Diritto ≠ ***legge***

Il concetto di paragiuridico:

il sistema giuridico è costituito non solo dall’insieme delle norme ma da una serie di elementi durevoli del diritto

- *il ruolo della dottrina*
- *Il valore della giurisprudenza*
- *Le professioni legali*
- *La storia di un sistema*
- *Lo stile delle sentenze*

La comparazione come scienza che guarda al contesto delle norme giuridiche

La tradizione giuridica occidentale e il dialogo common law-civil law

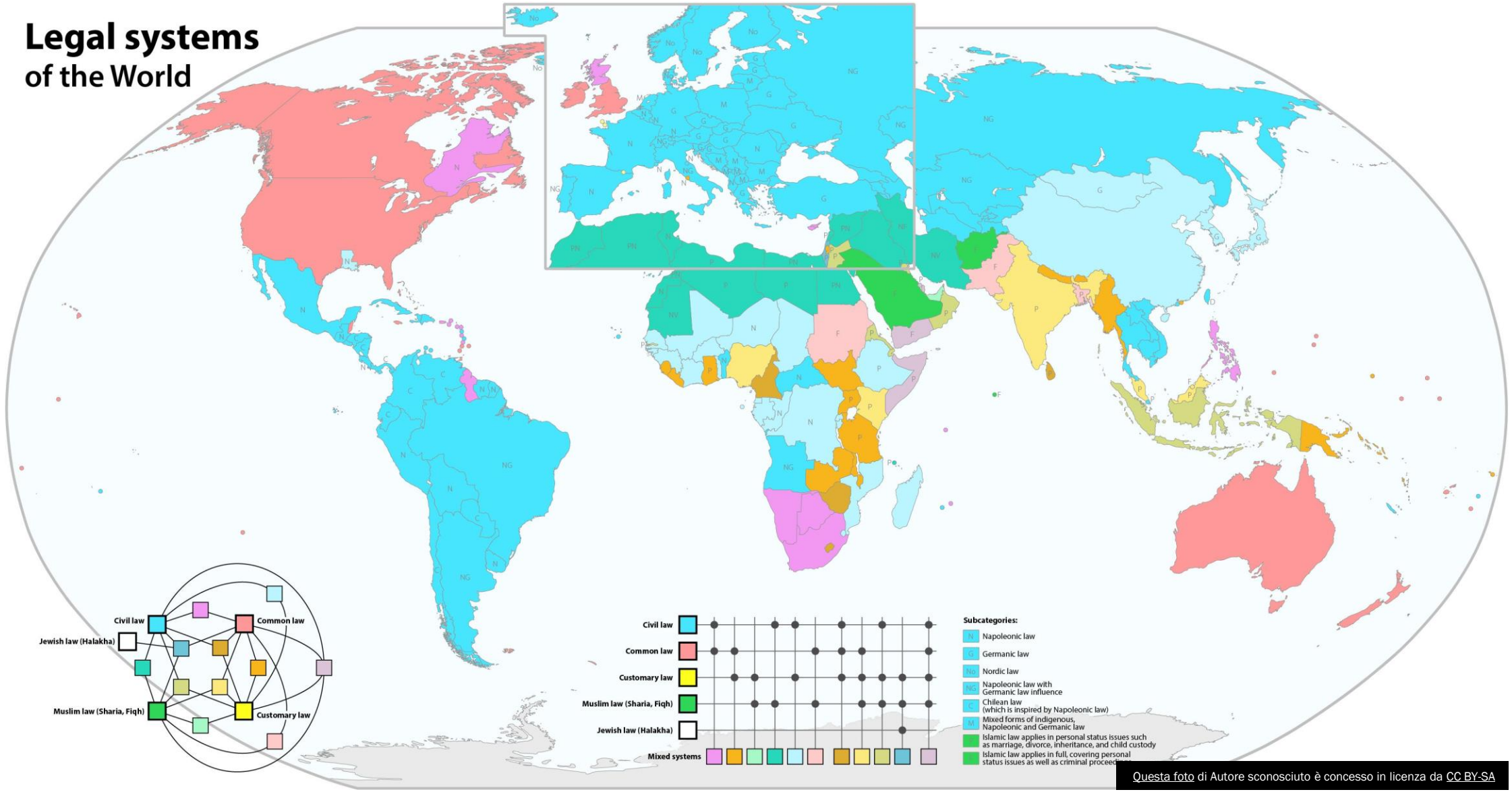
Common law

- Diritto non scritto
- L'idea di diritto come prassi-importanza della giurisprudenza
- La formazione pratica dei giuristi
- La continuità storica

Civil law

- Diritto scritto
- L'importanza del diritto come legge-le codificazioni
- La formazione accademica dei giuristi
- L'abbandono della tradizione dello ius commune

Legal systems
of the World



La comparazione come studio delle differenze: *common law* **vs.** *civil law*

I diversi significati di *common law*

- tradizione giuridica di matrice inglese
- Diritto patrio (diritto comune)
- Diritto giurisprudenziale (*common law= case law*)
- Sistema delle fonti (diritto scritto e non – precedente)
- Sistema giuridico anglo-americano

I diversi significati di *civil law*

- *Civil law* come famiglia giuridica romano-germanica
- *Civil law* come diritto dotto
- *Civil law* come diritto codificato

Rule of law ⟺ Stato di diritto

Common law

Il diritto viene prima dello Stato: l'idea della extra-statualità del diritto.

- *l'assenza di una costituzione scritta*
- *Il principio del due process*
- *L'unicità della giurisdizione*

Civil law

Il diritto è formato dallo Stato: l'idea della autolimitazione dello Stato.

- *La costituzione come legge fondamentale dello stato*
- *La divisione dei poteri*

Comparazione giuridica come studio delle somiglianze: common law ***and*** civil law

La graduale armonizzazione delle tradizioni giuridiche

Il contesto europeo e lo sviluppo del diritto privato europeo

L’armonizzazione del diritto nella tradizione giuridica occidentale

Il diritto dell’Unione Europea

- Il diritto comunitario come diritto comune agli Stati membri dell’UE, ma settoriale

I progetti di armonizzazione del diritto privato europeo

- Principi di Diritto Europeo dei Contratti
- Quadro comune di riferimento e le difficoltà di adozione da parte dell’UE

L’armonizzazione del diritto a livello internazionale: *common law* **and** *civil law*

- lo strumento legislativo per l’unificazione del diritto
- Il ruolo della giurisprudenza per l’uniformazione del diritto
- Il ruolo dei progetti della dottrina e l’idea di soft law

Il diritto tecnologico: *code is law*

- L’idea di una regolazione senza diritto
- La presunta affidabilità delle regole tecnologiche
- L’idea dell’ubiquità del diritto: diritto senza territorio
- Un diritto dematerializzato: dai beni ai bit

L’avvento di internet

29 novembre 2019 Internet Global Forum

> *«I progressi tecnologici si stanno sviluppando ad una velocità senza paralleli nella storia umana. L’impatto della tecnologia digitale è talvolta paragonato a quello dell’invenzione della stampa da parte di Gutenberg nell’Europa del 1439. Entrambi hanno democratizzato la conoscenza, ma a velocità molto diverse […] La tecnologia digitale sta plasmando la storia. Ma c’è anche la sensazione che ci stia scappando di mano. Dove ci porterà? [Antonio Guterres]*

Internet come opportunità ma anche come fonte di problemi giuridici posti dalla tecnologia digitale

ESISTE UN DIRITTO A INTERNET?

Qual è la natura di questo diritto?

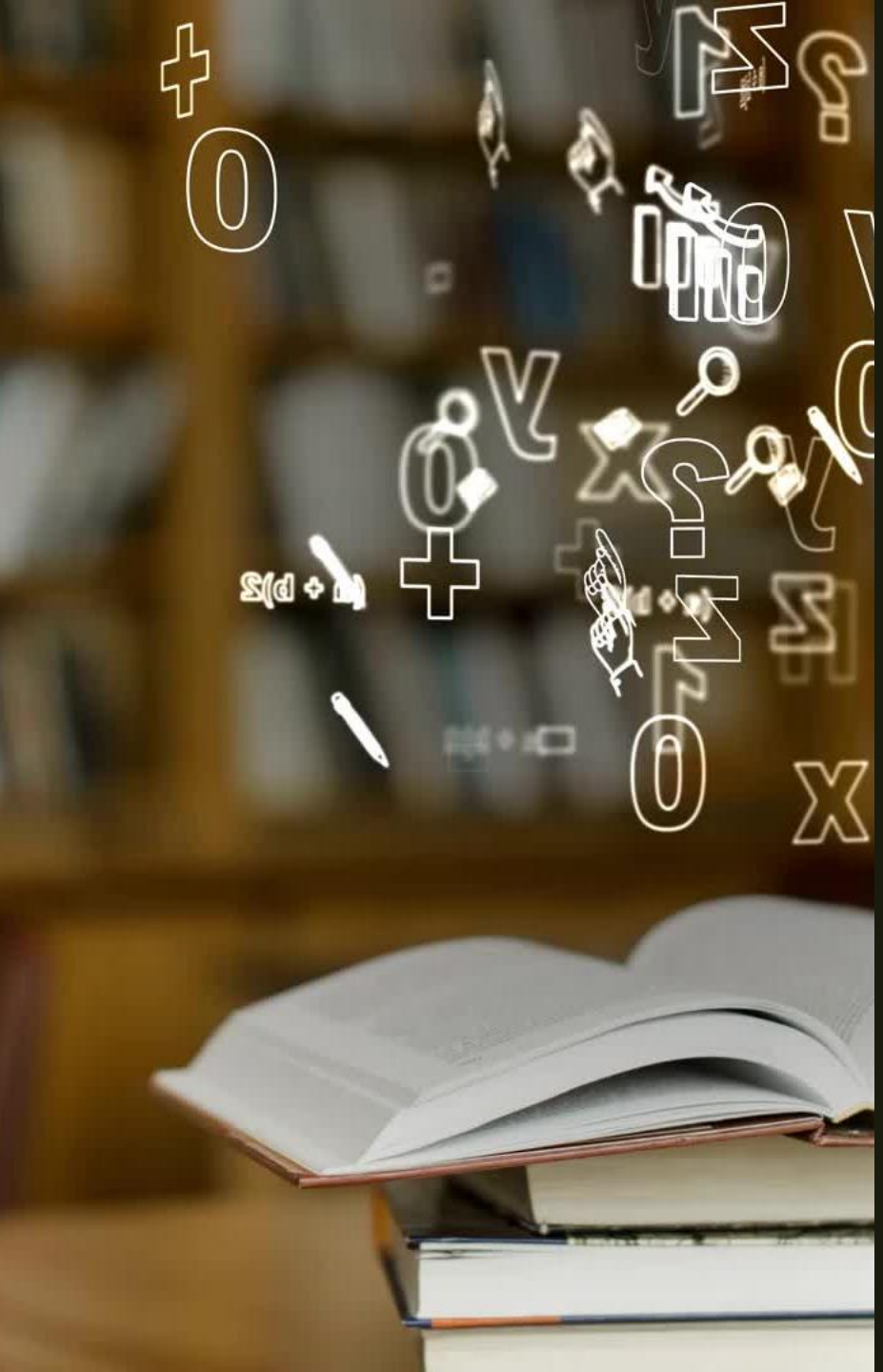
È un diritto fondamentale, tutelato dale Carte dei diritti ?

È tutelato dalla nostra costituzione?

Il diritto a internet come presupposto per la libertà nella rete - il contesto internazionale e europeo

La Corte di Giustizia non ha mai riconosciuto espressamente un diritto a internet come diritto fondamentale.

A livello internazionale, la Corte Europea dei diritti dell'Uomo non ha mai riconosciuto un diritto a internet



Diritto a internet e Costituzione italiana

Il diritto a internet non è riconosciuto espressamente dalla Costituzione italiana

- *Art. 21: libertà di espressione*
- *Proposte di riforma costituzionale per il riconoscimento del diritto a internet mai approvate*

Il 1 emendamento della Costituzione degli Stati Uniti d'America e il diritto di accesso a internet

1 Amendement: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peace- ably to assemble, and to petition the Government for a redress of grievances".

Caso *Packingham v. North Carolina* 2017

Giudice Kennedy: «Questi siti web probabilmente mettono a disposizione del cittadino i mezzi più potenti per far sentire la sua voce. Essi consentono a chiunque abbia una connessione internet di diventare un banditore, con una voce che risuona più lontano di quanto si potrebbe fare urlando da un pulpito».

Nel caso concreto la Corte equiparava pertanto lo spazio digitale al foro pubblico e risolveva il caso applicando le regole giurisprudenziali sulla tutela del diritto di accesso allo spazio pubblico al ciberspazio.

TUTELA DELLA LIBERTÀ DI ESPRESSIONE E HATE SPEECH: UNA QUESTIONE DI CONTRATTO

Moderazione dei contenuti on line e contrasto delle fake news

Tribunale Varese, Sez. I civile, 2 agosto 2022, n. 1181/2022 (ordinanza)

Il fatto:

Una cittadina pubblica sul profilo di un social network un post riportante il link a un video contenente dichiarazioni rese da un parlamentare che, nel corso di una audizione, definiva i vaccini anti-Covid come **inefficaci, sperimentali e dannosi, se non letali**.

Il post viola gli standard della Community, stabiliti attraverso condizioni generali di contratto, accettate dall'utente, che proibiscono le seguenti affermazioni:

i) "Affermazioni secondo cui i vaccini anti COVID-19 sono sperimentali, se il contesto dell'affermazione suggerisce che le persone vaccinate stanno partecipando a un esperimento sanitario";

ii) "Affermazioni secondo cui i vaccini anti COVID-19 uccidono o danneggiano gravemente le persone, conducendo a uno dei seguenti effetti collaterali dannosi: – Morte ...".

Qual è l’autonomia contrattuale della piattaforma nella regolazione dell’accesso e dei contenuti dei post degli utenti?

Il contratto di erogazione di servizi di social networking

Secondo il tribunale si tratta di un contratto **atipico tra utente consumatore e piattaforma** che è caratterizzato dal seguente contenuto:

- La Piattaforma si impegna a prestare un servizio a favore degli utenti e a mettere a disposizione gli strumenti per connettersi ad altri utenti, creare community, condividere esperienze.
- L’utente concede alla piattaforme la facoltà di utilizzare i propri dati personali, consentendo alla piattaforma un ritorno economico.

La qualificazione giuridica del rapporto utente piattaforma nella decisione del Tribunale di Varese

Il contratto di erogazione di servizi di social networking è meritevole di tutela ex art. 1322 c.c.:

- *(Autonomia contrattuale). Le parti possono liberamente determinare il contenuto del contratto nei limiti imposti dalla legge e dalle norme corporative.*

Il contratto deve essere valido e deve rispettare le norme imperative dell'ordinamento

- *Art. 1418:*
- *(Cause di nullità del contratto). Il contratto è nullo quando è contrario a norme imperative, salvo che la legge disponga diversamente.*

La soluzione del tribunale di Varese

Il tribunale esclude la vessatorietà, e dunque la nullità delle clausole degli ‘‘Standard della Community’’ in parola, ritenendo le limitazioni della libertà di espressione ivi previste non violino l’art. 21 Cost. perché poste a tutela di diritti costituzionali parimenti rilevanti, in particolare la salute pubblica.

Contratto e diritti fondamentali

I diritti fondamentali tutelati dalla Costituzione incidono sulla regolamentazione del rapporto tra i privati: la valutazione della vessatorietà delle clausole c.c. di *content moderation* deve essere fatta caso per caso.

L’utente che pubblica fake news è inadempiente al contratto con la piattaforma?

I rimedi alla violazione delle clausola di *content moderation*:

> *L’art. 1460: eccezione d’inadempimento*
>
> *Nei contratti con prestazioni corrispettive, ciascuno dei contraenti può rifiutarsi di adempiere la sua obbligazione, se l'altro non adempie o non offre di adempiere contemporaneamente la propria, salvo che termini diversi per l'adempimento siano stati stabiliti dalle parti o risultino dalla natura del contratto. Tuttavia non può rifiutarsi l'esecuzione se, avuto riguardo alle circostanze, il rifiuto è contrario alla buona fede.*

La soluzione del tribunale di Varese

Non può ritenersi sproporzionata la misura adottata dalla resistente, considerato che il post era stato preceduto da altri, parimenti contrari agli Standard della Community. Il blocco del profilo per giorni 30 è giustificato dunque dalle precedenti violazioni poste in essere dalla ricorrente.

Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali – Lezione 3

Jacopo Fortuna

Diritto alla riservatezza, diritto alla protezione dei dati personali, strategia europea sui dati

- Di right to privacy si inizia a parlare alla fine dell'800 in un articolo sull' «Harvard Law Review» a firma di Warren e Brandeis. Nel testo la privacy viene definita come «right to be let alone».
- In Italia il problema del diritto alla riservatezza nasce nel secondo dopoguerra in relazione alla divulgazione di fatti inerenti alle persone famose: la Cassazione negli anni 50 negò l'esistenza nel nostro sistema del diritto alla riservatezza (Cass. civ n. 4487 del 1956).
- Primo mutamento nell'orientamento della Corte (Sent. n. 990 del 1963): pubblicazione di un libro su Claretta Petacci (compagna di Mussolini).

- La Corte di Cassazione nel 1975 stabilisce che l'ordinamento riconosce e tutela l'interesse di ciascuno a che non siano resi noti fatti o avvenimenti di carattere riservato senza il proprio consenso (diritto alla riservatezza).
- La sentenza afferma che costituisce una lesione della privacy la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica, non essendo giustificata da interessi pubblici preminenti (Sent. n. 2129/1975 caso Soraya Esfandiary, seconda moglie dell'ultimo Scià di Persia).
- Francia, 1970 riforma art. 9 codice civile: riconoscimento del «droit à la vie privée».

Dal diritto a essere lasciati soli al diritto al controllo sulle informazioni

- Il momento che vede la definitiva affermazione in Italia del diritto alla riservatezza coincide con la diffusione dei calcolatori a partire dagli anni ‘70.
- Negli anni ’90 si diffondono in maniera capillare i computer e l’Italia emana la prima legge sul trattamento dei dati personali (l. 675 del 1996) poi confluita nel codice in materia di protezione dei dati personali (d.lgs 196/2003).
- Con l’utilizzo di massa delle reti internet, della diffusione degli smartphone e del contesto digitale contemporaneo si è assistito ad un proliferare di normative anche a livello sovranazionale per disciplinare il trattamento dei dati personali con i calcolatori elettronici.

- Consiglio d'Europa: svariate raccomandazioni sul trattamento automatizzato di dati personali e Convenzione 108 del 1981, ratificata dall'Italia nel 1989.
- L'UE è intervenuta a più riprese sul tema; Attualmente gli atti di riferimento eurounitari sul trattamento dei dati personali sono:

- Regolamento UE 2016/679 del Parlamento e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 CE (Regolamento generale sulla protezione dei dati – c.d. GDPR).
- Direttiva 2002/58 CE sul trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche (emendata dalla direttiva 2009/136/CE)

IL GDPR

- Il nuovo ecosistema digitale ha determinato il cambiamento della nozione e del contenuto del diritto alla riservatezza: dal diritto a essere lasciati soli al diritto al controllo sui propri dati.
- Il Regolamento 2016/679 è noto anche come General Data Protection Regulation (GDPR).
- Il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali (Art. 1).
- Il Diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi dell'art. 8 della Carta dei diritti fondamentali dell'UE (c.d. Carta di Nizza, 2000)

- Art. 4, n. 2): **«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Art. 4, n. 1): **«dato personale»:** qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
- **Il GDPR si applica solo ai dati personali: non si applica ai dati non personali o anonimi, cioè non identificati né identificabili.**

- Art. 9: «Trattamento di categorie particolari di dati personali».

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

- Al paragrafo 2 sono previste una serie di eccezioni alla regola generale prevista al paragrafo 1.

Soggetti del trattamento:

- Interessato: persona fisica identificata o identificabile cui si riferiscono i dati

- Titolare del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali

- Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- Rappresentante del titolare o del responsabile;

- Responsabile della protezione dei dati (o Data Protection Officer – DPO): soggetto designanto dal titolare e dal responsabile del trattamento in talune ipotesi previste dal regolamento cui sono attribuiti compiti di informazione, consulenza e sorveglianza;

Articolo 6

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Principi del trattamento (Art. 5 GDPR)

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).

La sicurezza dei dati

- La normativa in tema di protezione dei dati personali dispone che il trattamento dei dati personali avvenga in un contesto di misure tecniche, informatiche, organizzative logistiche e procedurali di sicurezza (cf. considerando n. 49 del GDPR).
- Il Regolamento impone al titolare del trattamento di osservare alcuni obblighi atti a garantire la sicurezza.

Articolo 32

Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

il caso *VB v. Natsionalna agentsia za prihodite* deciso dalla CGUE

- Sentenza della Corte di Giustizia dell'Unione europea (CGUE) nella causa *VB v. Natsionalna agentsia za prihodite* (C-340/21) emessa il 14 dicembre 2023.

- La sentenza ha chiarito che le misure adottate dal titolare o dal responsabile del trattamento per proteggere la sicurezza informatica dei dati trattati da *cyber-attacks* devono essere proporzionate alle minacce e l'inadeguatezza di tali misure può giustificare il risarcimento dei danni ai sensi dell'articolo 82 del GDPR, compresi i cosiddetti “danni immateriali” causati dall'uso improprio dei dati personali.

- La sentenza si occupa sia della responsabilità per l'inadeguatezza delle misure adottate dal titolare del trattamento dei dati richieste per garantire la sicurezza informatica ai sensi degli articoli 32 e 24 del GDPR, sia del conseguente risarcimento del “danno immateriale”, ossia del danno derivante dal mero timore dell'interessato di un potenziale futuro uso improprio dei suoi dati personali da parte di terzi eventuali criminali informatici che siano autori di una violazione dei dati.
- Nel caso di specie deciso dalla Corte, si era verificato un accesso abusivo al sistema informatico dell'Agenzia nazionale per le entrate pubbliche bulgara, la *Natsionalna agentsia za prihodite* (c.d. “NAP”), a seguito del quale erano stati diffusi online i dati personali di milioni di soggetti coinvolti e uno di questi aveva sollevato un ricorso al Administrativen sad Sofia-grad (Tribunale amministrativo della città di Sofia), chiedendo il risarcimento di una somma pari a 510,00 euro a fronte del danno immateriale subito.

- In primo grado il Tribunale aveva respinto il ricorso perché il ricorrente non era riuscito a dimostrare la mancata o inadeguata adozione di misure di sicurezza da parte della *Natsionalna agentsia za prihodite*.
- Il ricorrente aveva allora impugnato la decisione presso la Varhoven administrativen sad (Corte suprema amministrativa bulgara), la quale aveva sollevato presso la CGUE varie questioni pregiudiziali.
- La Corte di giustizia dell'Unione Europea ha stabilito la necessità di esaminare l'adeguatezza delle misure di sicurezza adottate dal titolare del trattamento in caso di divulgazione non autorizzata o accesso non autorizzato ai dati personali e che tale valutazione va effettuata in concreto.

- Pertanto, il mero fatto che dei criminali informatici abbiano effettuato un *data breach* non può rendere *ex se* tali misure inadeguate, né la violazione dei dati può costituire una presunzione assoluta di responsabilità del titolare. Occorre sottolineare, peraltro, che nel Regolamento (UE) 2016/679 (GDPR) non vi è alcun obbligo alla completa eliminazione dei rischi legati all'attività informatica da parte del titolare del trattamento.

- **Data breach:** si intende la violazione dei dati personali, cioè la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, comma 1, n. 12 GDPR).

- Il titolare del trattamento possiede un margine di discrezionalità per determinare le misure organizzative e tecniche adeguate al fine di garantire un livello di sicurezza proporzionato al rischio e la valutazione della loro adeguatezza è rimessa ai tribunali nazionali.

- Tuttavia, pur essendo necessaria una valutazione in concreto dei predetti tribunali sulle misure fornite dal titolare del trattamento ai fini della protezione dei dati personali, occorre rimarcare che non è ipotizzabile un suo esonero dall'obbligo di risarcire il danno subito dal soggetto coinvolto per il solo fatto che il danno derivi da un accesso non autorizzato e/o da una divulgazione non autorizzata dei dati personali da parte di terzi.

- La CGUE ha stabilito che le preoccupazioni, le ansie e i timori sofferti da un interessato a causa di un possibile futuro uso improprio dei dati oggetto del *data breach* potrebbero costituire un danno integralmente e a tutti gli effetti risarcibile ex l'art. 82 (1) del Regolamento, in quanto rientrante nel concetto di "danno immateriale".
- La Corte, infatti, ritiene che anche il mero timore dell'interessato di un potenziale futuro utilizzo dei propri dati personali da parte di terzi possa essere un idoneo presupposto ai fini del riconoscimento della risarcibilità di un "danno immateriale" e, a differenza del prevalente orientamento della giurisprudenza italiana, tale danno immateriale secondo la Corte è risarcibile anche se non raggiunge una soglia minima.
- Il danno ex art 82 GDPR ricomprende, pertanto, sia il danno già prodotto attraverso l'utilizzo illecito dei dati personali, sia il mero timore dell'interessato che in futuro si verifichi un utilizzo abusivo dei suoi dati.

ALCUNI CHIARIMENTI

Il diritto alla riservatezza e il diritto alla protezione dei dati personali non coincidono.

- **Il diritto alla protezione dei dati personali** consiste nel diritto del soggetto cui i dati si riferiscono di esercitare un **controllo**, anche attivo, su detti dati (diritto che si estende all'accesso e alla rettifica)- c.d. libertà positiva.
- **Il diritto alla riservatezza** (o diritto alla privacy in senso stretto) il diritto di **non subire interferenze** nella propria vita privata. L'individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni – c.d. libertà negativa.
- Questi due diritti sono tutelati, non a caso, da articoli distinti della Carte dei diritti fondamentali dell'UE.

- Il diritto alla riservatezza (come osservato) è un diritto di creazione giurisprudenziale e consiste nell'escludere altri dalla conoscenza di vicende strettamente personali e familiari.

- Il diritto alla riservatezza è diritto contenuto negativo mentre il diritto alla protezione dei dati personali è invece a contenuto positivo.

- Il diritto alla riservatezza, come detto in precedenza, viene ricondotto al famoso articolo di Waren e Brandeis sul «right to be let alone»

- Nuovo approccio europeo ai dati: non più solo finalizzato alla protezione degli stessi ma rivolto all'ottica della **circolazione**, **valorizzazione** e **condivisione** dei dati.

- Sembra delinearsi un mutamento dalla logica proprietaria alla logica dell'uso dei dati: il contratto di licenza sembra adeguato a incarnare questo cambiamento.

- I dati sono riutilizzabili mentre la proprietà è per sua natura un diritto esclusivo.

- Regolamenti europei volti alla valorizzazione, al riutilizzo e alla circolazione dei dati: **Data Governance Act** (che si rivolge a dati personali e non personali) e **Data Act** (dati non personali).

Comparazione giuridica e nuove tecnologie

Corso di Laurea in Mediazione linguistica per l'impresa internazionale e i media digitali – Lezione 4

Jacopo Fortuna

Alcune questioni di fondo…

- Cosa sono i dati personali?
  - *Sono beni?*
- Quali sono gli interessi legati al controllo e gestione dei dati personali?
  - *Interessi economici?*
  - *Interessi non economici?*
- Che cosa accade ai nostri dati al termine del contratto?
  - *Che cosa accade ai dati alla morte del contraente a cui si riferiscono?*

Privacy *post mortem*

2013: Lilian Edwards and Edina Harbinja, “What Happens to My Facebook Profile When I Die?’: Legal Issues Around Transmission of Digital Assets on Death”.

«le persone defunte abbiano il diritto di mantenere i loro segreti dopo la morte e che questo diritto possa prevalere sui diritti (se esistono) della famiglia o degli eredi di accedere o entrare in possesso dei loro profilo, documenti ecc. dopo la morte»

Una serie di questioni aperte:

1) I diritti della personalità possono si estinguono con la morte?
2) I diritti della personalità sono ereditabili?
3) I diritti sui dati sono diritti reali o personali?
4) È concepibile un diritto in relazione ai dati come diritto della personalità?

PUÒ ESISTERE UNA PRIVACY DOPO LA MORTE?

L’esperienza degli Stati Uniti d’America

- La tutela del nome e dell’identità del soggetto:
  - ***Right of privacy*** *: the right to be left alone*
  - ***Right of publicity:*** *an intellectual property right that protects against the misappropriation of a person's name, likeness, or other indicia of personal identity-such as nickname, pseudonym, voice, signature or photograph-for commercial benefit*
- Il *right of publicity* si sviluppa dal Right of privacy ma acquisisce una propria autonomia: decisione Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc. (New York, 1953).

Post-mortem right of publicity?

Regola principale: actio personalis moritur cum personam.

Right of publicity tutela avverso usurpazioni indebite del nome o di altri aspetti della personalità: l'interesse protetto è economico.

Assenza di una disciplina federale	*Riconoscimento del diritto solo in alcuni stati.*

Right to publicity: diversi approcci a livello nazionale

Stato di New York

- *Diritto tutelato nell'ambito della disciplina della privacy:* le legge tutelava inizialmente solo in alcuni casi - s.50-f
- Modifica della legge nel 2020 e poi nel 2022: Riconoscimento di un right to publicity post-mortem.
  - ✓ È un property rights
  - ✓ È tutelato fino a 40 anni dopo la morte
  - ✓ La legge tutela anche avverso l'uso di "repliche artificiali" senza il consenso dell'interessato.

Tutela del right to publicity: Stato della California

- California Civil Code §3344
- **a)** Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof. In addition, in any action brought under this section, the person who violated the section shall be liable to the injured party or parties in an amount equal to the greater of seven hundred fifty dollars ($750) or the actual damages suffered by him or her as a result of the unauthorized use, and any profits from the unauthorized use that are attributable to the use and are not taken into account in computing the actual damages. In establishing such profits, the injured party or parties are required to present proof only of the gross revenue attributable to such use, and the person who violated this section is required to prove his or her deductible expenses. Punitive damages may also be awarded to the injured party or parties. The prevailing party in any action under this section shall also be entitled to attorney's fees and costs. […]
  - *Tutela più ampia*
  - *Tutela dopo la morte del soggetto*
  - *Tutela per 70 anni dopo la morte*

La legge della California sulla tutela del trattamento dei dati personali: California Consumer Privacy Act 2018

- Approccio simile a GDPR sulla definizione di dati e oggetto di tutela, ma diversi i soggetti obbligati: es. CCPA non si applica gli enti pubblici

«“Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

1. (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers. […]

- Il consumatore è definito dalla legge come "**a natural person who is a California resident**" : no tutela giuridica dei dati della persona deceduta.

L'APPROCCIO STATUNITENSE ALLA TUTELA POST MORTEM DI DATI E INFORMAZIONI DIGITALI RELATIVI ALLA PERSONA.

Applicazione della Law of property: staccate dalla persona del vivente tutte queste informazioni sono properties, e possono essere tutelate come tali.

Come properties sono ereditabili?

La «resurrezione digitale» e la tutela dell'interesse a essere «lasciato solo»

C'è una tutela dell'interesse del defunto contro l'uso dei suoi dati per deepfakes?

STATO DI NEW YORK: **approccio proprietario**, tutela mediante *right of publicity.*

la legge consente agli eredi di agire contro l'uso di deepfake, senza il consenso.

STATO DI LOUSIANA: approccio proprietario, §51.470: Property right in an individual's identity: i diritti non si estinguono con la morte del soggetto e sono tutelati fino a 50 anni dopo la morte. I property rights includono l'uso dell'identità del soggetto tramite «digital replicas».

Proposta di legge federale sui Deepfakes (5586 del settembre 2023)

Lo scopo è di proteggere la sicurezza nazionale avverso i pericoli derivanti dall'uso della tecnologie deepfake e di tutelare le vittime di deepfake.

La proposta definisce **«advanced technological false personation record» come un deepfake** stabilendo obblighi di indicazione della provenienza e di disclousure audio e video.

La legge prevede sanzioni penali e civili

È prevista inoltre una tutela privatistica per la persona danneggiata:

«Any person who has been exhibited as engaging in falsified material activity in an advanced technological false personation record may bring a civil action before the appropriate Federal district court for damages under paragraph (2) and injunctive relief under paragraph (3) against a person who violates subsection (a) or alters an advanced technological false personation record to remove or meaningfully obscure the disclosures required under subsection (a)»

Deepfake non autorizzati: la tutela riguarda solo il patrimonio?

Indizi nella recente **proposta di legge dello Stato di New York**

- S. 52 B: proposta di concedere una tutela privata contro uso di deepfake che riguardano aspetti intimi della persona, **indipendentemente dal consenso all'uso delle immagini iniziali**, quando emerge:
  - *A) è un deep fake e la persona aveva la ragionevole aspettativa che quelle immagini o aspetti della sua persona sarebbero rimasti privati;*
  - *B) raffigura la persona svestita o ne espone parti intime o raffigura la persona nel compimento di atti sessuali.*
  - *C) Il deepfake è diffuso senza il consenso*

Morte digitale e tutela dei contenuti on line legati alla persona tra *property* e personality: una questione ancora aperta

1

La teoria dell'*informational body* di Floridi: la persona non è costituita solo dalla sua fisicità ma da tutta una serie di informazioni che la riguardano

2

Le nuove tecnologie cambiano l'idea di persona? Che cos'è la persona?

3

La necessità di rivedere le categorie giuridiche

PROFILAZIONE E MANIPOLAZIONE DEI DATI

- Conoscere i dati delle persone è importante per le aziende perché ciò permette loro di vendere beni e servizi attraverso una pubblicità mirata.

- La protezione dei dati personali favorisce il commercio elettronico perché altrimenti esso potrebbe essere ostacolato se i potenziali clienti si sentissero minacciati dai rischi legati alla diffusione dei loro dati.

- È interesse di chi raccoglie i dati garantire un elevato standard di tutela al titolare dei dati.

- Misure atte a proteggere i dati ⟹ sviluppo dell'economia digitale e del mercato interno.

Nella pratica si verifica una sproporzione tra chi offre e chi accetta servizi sulla rete

- Chi offre servizi digitali spesso può richiedere i dati senza essere obbligato a garantire un levato livello di tutela dei dati: ad esempio, l'utente che ha necessità dell'upgrade del software accetterà spesso comunque di fornire i dati pur di scaricare quanto gli serve.

- Le aziende che offrono servizi come motore di ricerca e social network sono teoricamente gratuiti, ma in realtà paghiamo tali servizi con i nostri dati, che hanno un valore economico.

- Le aziende pagano social network e motori di ricerca affinché questi propongano i loro beni e servizi agli utenti in base ai loro profili.

Profilazione: pubblicità mirata, basata sui comportamenti in rete (Pubblicità comportamentale online). Ad esempio: transazioni effettuate, like, navigazione sui siti, tempo di permanenza su una pagina etc…

Art 4, par. 1, n.4) GDPR

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Il **Centro di psicometria dell'Università di Cambridge** mette a disposizione online un applicativo che definisce il profilo di ciascuno, ricavato dalle tracce digitali del proprio comportamento. Rileva la percezione della propria persona online e fornisce approfondimenti sulla personalità, intelligenza, leadership, soddisfazione nella vita etc…

Rischi della profilazione per finalità di marketing

- Manipolazione;
- Limitazione della libertà di scelta;

Caso Cambridge Analytica.

- Società che operava nel data science che si occupava del rapporto tra dati e campagne elettorali: conoscendo i dati degli elettori si può avere maggiore influenza su di essi.
- Cambridge Analytica si basava sui dati acquisisti prevalentemente da Facebook per creare dei profili psicografici nei quali identificava quali elettori avrebbero votato per un certo candidato ma usava le informazioni per predire e modificare il loro comportamento futuro.
- Cambridge Analytica è stata accusata di aver influenzato alcune campagne elettorali, tra cui quella che ha portato all'elezione di Trump nel 2016, il quale era cliente della medesima società.

- Oltre al rischio di manipolazione esiste il rischio che qualcuno a nostra insaputa possa farsi un'idea errata sul nostro profilo, dal momento che non sempre le tracce digitali che lasciamo ci rispecchiano.

- Ciò può essere fonte di danno da errata profilazione che potrebbe causare anche la lesione del diritto all'identità personale e all'identità digitale.

- Un uso accorto della tecnologia può attenuare i rischi elencati. Il GDPR introduce l'approccio definito come *privacy by design e by default*, cioè con modalità di creazione degli strumenti tecnologici che prenda in considerazione il rispetto della privacy in tutto il suo processo produttivo (art. 25 GDPR).

Se sistemi e programmi informatici devono essere configurati in modo da scongiurare trattamenti incompatibili con i principi stabiliti dalla legge vuol dire che il legislatore affida alla tecnologia il compito di assicurare il perseguimento degli obbiettivi che le norme si prefiggono: **la tecnologia incorpora la legge.**

IL DIRITTO ALL'OBLIO

Diritto a essere dimenticati, ma non può privare gli altri della possibilità di accedere alla conoscenza del passato quando non esiste una specifica violazione dell'identità informazionale (necessità di bilanciamento).

- In una prima accezione: aspetto del diritto alla riservatezza.

- Diritto di un soggetto a non vedere pubblicate alcune notizie relative a vicende, già pubblicate, rispetto all'accadimento delle quali è trascorso un rilevante lasso di tempo.

- Le vicende legittimamente pubblicate a proposito di una persona possono costituire oggetto di nuova pubblicazione?

- Possibile invadenza dei mezzi dell'informazione.

- La prima enucleazione del problema viene dagli Stati Uniti: caso William Sidis.

- Sidis era un *enfant prodige* che a 11 anni aveva tenuto conferenze sulla quarta dimensione di fronte ad eminenti matematici e che a 16 si era laureato ad Harvard. Tuttavia, con l'età la sua intelligenza inizia a scemare e sviluppa una repulsione verso la matematica.
- La sua storia fu ripubblicata dal «The New Yorker» nell'agosto del 1937.
- Sidis nel frattempo era divenuto un tranquillo contabile, collezionista di biglietti del tram e studioso di nativi americani.
- Chiese ai giudici che venisse riconosciuto il suo diritto a essere dimenticato ma non trovò tutela giuridica.
- In Italia il problema si è posto per la prima volta con la Sent. n. 1563 del 1958 della Corte di Cassazione, relativa al caso del questore di Roma coinvolto nella strage delle Fosse Ardeatine.

- Il tema è emerso chiaramente in Italia con una sentenza della Corte di Cassazione del 1998 n. 3679: caso della pubblicazione nel 1983 di articoli in cui alcuni imprenditori vengono accusati di avere rapporti con la mafia, ripubblicati anni dopo. La Cass. stabilisce che:

- Per diritto d'oblio si intende l'interesse di ogni persona a non restare indeterminatamente esposta ai danni causati dalla reiterata pubblicazione di una notizia.
- Non costituisce diritto di cronaca la pubblicazione di fatti già resi noti anni prima, salvo che eventi sopravvenuti rendano nuovamente attuali quei fatti, facendo sorgere un nuovo interesse pubblico alla divulgazione dell'informazione.

- Con l’avvento di internet il problema aumenta, poiché le informazioni sono sempre disponibili online.
- Il diritto di oblio non è più solo il diritto a essere dimenticati, ma anche il diritto alla contestualizzazione degli eventi
- Cass. Civ. del 5225 del 2012: «Il titolare di un organo di informazione è tenuto a garantire la contestualizzazione e l’aggiornamento della notizia di cronaca […] a tutela del diritto dell’interessato al trattamento alla propria identità personale o morale nonché a salvaguardia del diritto del cittadino utente di ricevere un’informazione completa e corretta».
- Terza accezione del diritto all’oblio: diritto alla cancellazione dei dati obsoleti e diritto di ottenere la c.d. deindicizzazione dei dati ad opera del motore di ricerca
- La materia è ora trattata anche dall’Art. 17 (Diritto alla cancellazione) del GDPR.

- Ricostruzione delle vicende storiche e delle fasi del diritto all'oblio da parte delle sezioni unite della Cassazione nella sentenza 19681 del 2019: distinzione e rapporto tra diritto d'oblio e diritto alla rievocazione storica di fatti e vicende del passato.

- Bilanciamento tra l'interesse della collettività ad essere informata su fatti inerenti a personaggi noti o che svolgono un ruolo pubblico e il diritto alla riservatezza rispetto a fatti del passato potenzialmente lesivi della dignità e dell'onore.

- Cass. Civ., ordinanza n. 34658 del 2022, affronta specificamente il tema della deindicizzazione. La deindicizzazione non è l'eliminazione di un contenuto, ma impedisce che esso sia direttamente accessibile tramite motori di ricerca. Il diritto all'oblio consente alle autorità italiane di ordinare al gestore del motore di ricerca di effettuare una deindicizzazione su tutte le versioni (anche extraeuropee) del motore stesso.