Discriminazioni digitali: il diritto antidiscriminatorio alla prova della rivoluzione tecnologica

A prima vista lo spazio virtuale può sembrare il luogo ideale per instaurare relazioni alla pari in realtà i rischi discriminatori sono molteplici e pongono varie sfide al diritto. Bisogna ragionare sulla capacità di resilienza del diritto antidiscriminatorio di matrice europea e sulle modalità di funzionamento delle discriminazioni digitali (distorsioni, bias, categorizzazioni, la cornice normativa europea in evoluzione e la nuova prospttiva dei Critical Data Studies.
Il diritto antidiscriminatorio si fonda su:

- **caratteristiche della persona**; sesso, razza, disabilità, orientamento sessuale, religione, origine etnica.
- **ambiti di applicabilità definiti**; lavoro, welfare, beni e servizi, sicurezza sociale (Race Equality Directive e Gender Goods and Services Directive). Parità di retribuzione, promozioni, accesso al lavoro, a beni e servizi.

Tutti questi aspetti risultano oggi profondamente interessati dalla rivoluzione tecnologica: ad esempio le donne che lavorano nella gig econmy sono discriminate da giudizi e si ha la riduzione di future opportunità di lavoro, oppure le offerte di lavoro personalizzate sulla base di elaborazioni algoritmiche (una recente ricerca ha dimostrato che l'85% degli annunci per impiego come cassiera è stato indirizzato a donne, mentre per quelli di tassista a persone di colore.
Nella realtà digitale sono sempre più rilevanti altre forme di discriminazione: discriminazioni del prezzo che differenziano l'importo delle offerte a seconda del reddito presunto del consumatore, zona di residenza, condizioni di salute; ma anche le classificazioni consguenti all'indicizzazione di risultati attraverso pagine personalizzate che perciò risultano nascoste ad altri e visibili solo ad alcune.
Inoltre nella nuova realtà informazionale i confini tra sferaa lavorativa e professionale sono molto sfumati.
Anche laddove vengano impiegate tecniche di data mining per assumere scelte professionali le metodologi eimpiegate in realtà processeranno una quantità così indifferenziata di informazioni che esse coinvolgeranno diverse sfere della vita delle persone coinvolte sia online che offline (siti visitati, geolocalizzazione, quantità di errori ortografici).
Allora la nuova realtà informazionale colpisce il diritto antidiscriminatorio proprio nei suoi due punti nevralgici.
Se, a prima vista, il ricorso a scelte automatiche può apparire come una forma di garanzia è stato dimostrato che i dati sono sempre attivi e mai neutrali: gli algoritmi tendono a riprodurre le disparità razziali e di genere più radicate attraverso le persone che li elaborano. I dati sono affetti da bias, distorizioni che discriminano ingiustamente determinati individui o gruppi a favore di altri. Vi sono 4 tipologie di bias:

- pre-existing bias; dati incorporati nel software
- technical bias; dipendenti da vincoli o decisioni tecniche
- emergent bias; immessi nel sistema sopo il suo avviamento
- measurement bias; legati alla modalità della raccolta dei dati

Mangiameli scrive che i dati rappresentano la realtà modificandola cioè orientando i comportamenti.
In termini teorici il diritto antidiscriminatorio può essere assediato su tre fonti:

- **funzione classificatoria**; creando classificazioni arbitrarie che possono generare trattamenti o effetti discriminatori

- **funzione veridittiva**; validazione di stereotipi e pregiudizi che, immessi nella procedura, produrrano output stereotipati
- **funzione predittiva**; cristallizzazione di una condizione di discrminazione strutturale conservata e riprodotta nelle scelte future generando uno stigma ineliminabile.

Tutte queste situazioni hanno effetti performativi e pongono sfide complesse al diritto perché sia una norma che differnzia sia un atteggiamneto che cerchi di recepire tali discriminazioni rischiano di fallire l'obiettivo di generare eguaglianza.
Altro profilo problematico è il regime probatorio basato su presunzioni e nessi di causalità diretti: in termini di teoria del diritto antidiscriminatorio risulta complicato tra discriminazioni dirette (trattamento) e indirette (effetti).
Inoltre sorge il problema dell'imputabilità ricondotta a vari profili come il progettista e il provider.
Alcuni rischi potenzialmente inafferabili consistono in:

1. difficoltà del sistema europeo a recepire il metodo intersezionale a scopo probatorio; che guarda alla sovrapposizione con riferimento a determinati gruppi di popolazioni di diversi profili di discriminazioni che agiscono congiuntamente e non separabili. Nelle corti l'atteggiamento respinge tale metodo a favore di altri metodi più tradizionali
2. occorre sviluppare una riflessione su chi possa subire una discriminazione; laddove un robot, ad esempio una macchina a guida autonoma, ci si dovrà chiedere se dovrà essere sanzionato la discriminaizone subita dal sistema di intelligenza artificiale (anche se ultimamente stato ritenuto che non è necessario attribuire personalità giuridica a strumenti digitali).
3. Bisogna comprendere chi possa discriminare; si può avere una dittatura delle probabilità in termini di vigilanza predittiva ad esmepio con ampi riflessi sul diritto di difesa.
4. Utilizzi discriminatori dei dati possono essere sfruttati da una grande varietà di soggetti privati, banche, organizzazioni criminali, aziende, gruppi riconducibili a interessi politici per carpire gli aspetti già fragili del cittadino a sfruttarli a proprio favore. Si ha ad esempio la tendenza degli spazi virtuali a fungere da cassa di risonanza e cià potrebbe radicalizzare la tendenza discriminatoria oppure la tendenza a creare comunità con gli stessi interessi impedendo l'accesso ad altri ambiti. Si può avere una progressiva erosione della capcità di lbera scelta dato che vi è una linea molto sottile tra informare e manipolare.
5. Risulta problematica l'amplificazione virale del fatto; diffusione di contenuti via whatsapp ad esempio offensivi rispetto a un gruppo. Dunque si ha a che fare con una forma di responsabilità gregaria. Sul versante antidiscriminatorio la determinazione del contesto è rilevante, pur essendo la responsabilità penale esclusivamente personale.
6. Infine chi è trattato sfavorevolmente nella rete viene isolato, si ha quindi solitudine della vittima

La risoluzione del 2017 all'art. 5 riconosce che l'uso dei dati può ripercuotersi sulla società con la conseguenza della stigmatizzazione di interi gruppi sociali. Inoltre si ha un impatto delle discriminazioni indirette in termini di equità e pari opportunità dal momento che si possono avere disparità di trattamento per quanto riguarda gli effetti nei confronti di gruppi di persone con caratteristiche particolari (ricerca del lavoro, media sociali).

L'art. 4 del regolamento al quadro Etico ha dato una definzione di *discriminazione*: si intende qualsiasi trattamento differenziato di una persona o un gruppo di persone per un motivo privo di giustificazione obiettiva o ragionevole e pertanto vietando dal diritto dell'Unione.
In questa cornice i Critical Data Studies ancora poco sviluppati sembrano essere promettenti perché, piuttosto che utilizzare la workforce analytics per assumere decisioni, le aziende potrebbero analizzare approfonditamente i dati per valutare il processo decisionale stesso, contrastando così i pregiudizi nascosti.

Reati informatici

Da quando l'informatica ha mosso i primi passi aleggiava l'idea per la quale tali strumenti avrebbero rappresentato un'opportunità di sviluppo e progresso, ma essa comincia ad entrare in crisi negli anni '70.
Infatti si capisce come tali modalità informatiche possano esere utilizzate per riproporre illeciti classici in forma tecnologica.
Ci sono due principio fondamentali del diritto penale che connota qualsiasi Stato di diritto:

- Non vi può essere pena senza una **legge preesistente** alla commissione del reato stesso
- **Principio di tassatività**; il reato ha i suoi elementi costitutivi, se ne manca uno non è configurabile.
- **Divieto di analogia**; proprio per il principio di legalità, tassatività i reati devono avere dei contorni perfettamente limitati. Vige infatti la riserva di legge.

Altro termine utilizzato come "sinonimo" di reati informatici è il termine cyber crimes che riguarda però in generale crimini riguardanti l'uso delle nuove tecnologie, allora dovremmo chiamarli reati necessariamente informatici.
I vecchi illeciti tradizionali che si avvalgono di tecnologie informatiche sono differenti dai nuovi reati, prima impensabili.
Il Consiglio d'Europa innesca tale processo di introduzione di nuove fattispecie criminose con la Raccomandazione 9/1989 e invita tuti gli Stati a prevedere una disciplina giuridica puntuale, fissando una lista minima contenente:

- Frode informatica; diversa dalla truffa
- Falso informatico
- Danneggiamento di dati e programmi informatici
- Sabotaggio informatico; intercettazione o impedimento di comunicazioni telematiche
- Accesso non autorizzato a dati o account
- Riproduzione non autorizzato di materiale coperto da copyright

L'Italia risponde con la **l. 547/1993** che modifica il codice penale attraverso un **metodo** evolutivo (integrando il codice) invece gli altri paesi hanno utilizzato il **metodo organico** cioè hanno elaborato un altro codice.
Ci sono 4 raggruppamenti di reati:

1. Assimilabile all'art. 614, riguardanti il domicilio informatico; artt. 615-ter, quater e quinquies.
   L'art. 615-ter riguarda l'accesso abusivo al sistema informatico o telematico. Il sistema informatico deve essere protetto da misure di sicurezza (password), oppure ci si deve mantenere contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Si tratta di un reato punibile a querela della persona offesa salvo casi in cui si prcede d'ufficio ad esempio se tale fatto è commesso da un pubblico ufficiale o incaricato di pubblico servizio (aggravante).

L'art. 615-quater riguarda la detenzione abusiva di codici di accesso a sistemi informatici. Qui c'è dolo specifico, perché chiunque detenga codici al fine di procurare a sé o ad altri un profitto o arrecare danno commette reato.
L'art. 615-quinquies punisce la diffusione di apparecchiature o programmi diretti a danneggire o interrompere un sistema informatico o telematico. Si procede d'ufficio nel caso in cui chiunque voglia danneggiare, alterare un sistema o favorire l'interruzione totale o parziale del suo funzionamento. Anche qui c'è dolo specifico.

2. Artt. 617-quater, quinquies e sexies; intercettazioni abusive di comunicazioni informatiche o telematiche. "*Fraudolentemente*" significa in modo nascosto, ma è punite anche impedisce o interrompe tali comunicazioni. La formulazione in questo caso non dà particolari problemi. Poi è punita la rivelazione al pubblico di intercettazioni.
   L'art. 617-quinquies riguarda l'installazione di apparecchiature atte a intercettare, interrompere o impedire comunicazioni relative a un sistema informatico o telematico. Si tratta di una previsione anticipata infatti sanziona l'installazione di apparecchiature. Qualora l'apparecchio non funzioni il reato è integrato ugualmente.
   Chi installa ad esempio un keylogger, software che permette di ricavare le password in modo da modificare o falsificare le conversazioni telematiche ma poi non riesce a ricavare quei dati sarà considerato responsabile non del 614-quater ma del 617-quinquies.
   L'art. 617 sexies punisce la falsificazione, alterazione o soppressione di comunicazioni informatiche o telematiche intercettate al fine di arreccare un danno o un vantaggio a sé o ad altri (dolo specifico).
3. Art. 640-ter; frode informatica, simile ma diversa dalla truffa.
4. Artt. 635-bis, ter, quater;

Beni comuni della conoscenza: al di là del copyright

E. Ostrom con questa espressione intende tutte le forme di sapere scientifico, creativo (musica, teatro) conseguite attraverso l'esperienza o lo studio, espresso in forma di cultura locale, erudita o qualsiasi altra. Si tratta di una forma di intelligenza intesa come la possibilità di essere competivi tanto rispetto al pubblico quanto al privato.
Quando è stata costituita la Commissione presso il Ministero della giustizia per modificare le norme del codice civile, Titolo II Libro II, che definiscono i beni, l'idea era elaborare una categoria di beni giuridici, beni comuni, strutturati a prescindere dall'appartenenza cioè dalla titolarità del bene. Tale categoria veniva individuata in quanto espressione dell'utilità fuizonale ai diritti fondamentali della persona, quindi vi era un rapporto stretto tra tutela dei diritti della persona e degli interessi pubblici.
Da questo dibattito è scaturita la possibilità di creare una opzione terza rispetto a un ceontsto istituzionale, giuridico sociale bloccato tra due opzioni classiche tipiche della modernit,: quella proprietaria (Stato) e gestionale il cui garante dell'efficienza econmica è il mercato.
Negli anni '80 nascono le prime associazioni di studio dei commons, che coinvolgono giuristi ed economisti come Ostrom. Il suo obiettivo era mostrare la sostenibilità di formule di autogoverno, ciò che lei chiama **sistema di risorse comuni**, diverse dai beni ad accesso libero. Essa usa la logica pragmatica considerando come fine delle azioni l'esigenza di massimizzare il benessere dal maggior numero di persone (visione utilitarista).

La scuola neoclassica considera i diritti di proprietà privata elemento cruciale da valorizzare per l'efficienza economica, salvo i beni inadeguati al mercato, i beni pubblici (ad esempio l'informazione). Infatti hanno delle caratteristiche intrinseche: non rivale, non escludibile (non si può escludere un altro soggetto dall'uso di un bene). Lo Stato non può produrre beni pubblici se non arrivando a una situazione subottimale.
In sostanza secondo Samuelson i beni pubblici, imperfetti per il loro carattere non rivale e non escludibile, devono essere finanziati per via fiscale e sfuggono all'atmosfera mercantile, essi sono il fallimento del mercato.
In definitiva la conoscenza deve essere considerata bene pubblico perché difficilmente escludibile, lo Stato interviene nella produzione della conoscenza finanziando la ricerca di base messa a disposizione poi della società.
Esistono leggi economiche oggettive che permetterebbero di delimitare la sfera dello Stato e del mercato in relazione a cartteristiche intrinseche di un bene, il che presuppone che anche gli stessi beni abbiano caratteristiche intrinseche e naturali a prescindere dall'uso che se ne può fare.
Ostrom ha iniziato a pensare la conoscenza no più come bene pubblico ma comune a causa dello sviluppo eccessivo dei diritti di proprietà intellettuale, che li ha resi escludibili creando una scarsità artificiale attraverso le barriere di accesso, il copyright.
Il processo di internazionalizzazione ha armonizzato le legislazioni nazionali, poi c'è stata la Convenzione di Berna 1887, anni '70 e i Trattati del 1990.
Questi tre elementi di internazionalizzazione, estensione dei termini temporali e degli ambiti di applicazione ha favorito la creazione del fenomeno della scarsità artificiale di tale bene, quindi spendibile sul mercato.
La rivoluzione di internet ha avuto degli effetti contraddittori: infatti, pur rendendo la conoscenza illimitata grazie alle potenzialità della rete, ha limitato e controllato la diffusione delle informazioni.
Al fine di rendere accessibile le opere si è pensato di strutturare un set di licenze che consente all'autore di dare una serie di diritti a coloro che acquistano il bene:

- ✓ **Attribution**; obbligo di citare espressamente l'autore che risponde al diritto morale d'autore contemplato in tutte le licenze.
- ✓ **Non commercial**; non è autorizzato l'uso dell'opera per scopi commerciali
- ✓ **Non derivative Works**; non sono ammessi lavori derivati dall'opera o basati su parti singole di essa. Non è permesso modificare, rielaborare o alterare i contenuti originali dell'opera.
- ✓ **Share Alike**; è permesso distribuire lavori derivati dall'opera solo se messi in circolazione con il medesimo tipo di licenza applicato all'opera originale.

Phishing

Si tratta di una particolare **condotta fraudolenta** (non un reato) realizzata attraverso messaggi di posta elettronica ingannevoli ma anche con altre condotte materiali.
Abbiamo due possibili alternative di reato di truffa:

1. Art. 640; truffa, chiunque con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.
2. Art. 640-ter; frode informatica, chiunque alterando in qualsaisi modo il funzionamento di un sistema informatico procura a sé o ad altri un ingiusto profitto con altrui danno.

Essi differiscono per la qualificazione giuridica e inoltre il raggirato nel primo reato è l'essere umano mentre nel secondo il sistema informatico.
Il **farming** è una variante di phishing che agisce sul DNS (sistema che consente di tradurre il linguaggio naturale in numeri; invece il trashing consiste nel frugare nei rifiuti per carpire informazioni sulla vittima e mettere in moto una truffa. In sostanza bisogna andare a verificare di volta in volta la qualificazione giuridica.
Le tecnologie informatiche consentono anche lo svolgimento di attività criminali come la pedofilia, il revenge porn, pedopornografia virtuale.

Data protection officer: una nuova professione digitale

L'azienda SOGEI system è titolare dei propri dati ma è anche responsabile, le modalità operative si esplicano attraverso atti esecutivi (salute – tra cui il pass vaccinale, sicurezza, banche dati nazionali).
L'art. 30 GDPR disciplina il registro dei trattamenti dei dati. Vi sono anche l'art. 32, 35 analisi del rischio e della sicurezza consistente in una metodologia proprietaria dell'azione da SOGEI: il titolare effettua una valutazione del rischio in termini di riservatezza, disponibilità ed effettua una serie di misure definendo una soglia di accettabilità del rischio.
Può succedere che le misure di sicurezza debbano essere implementate in un certo tot di tempo durante il quale si accetta il rischio minimo.
Altro tema rilevante della data governance sono gli assesement per venire incontro al principio di accountability e la gestione degli incarichi degli amministratori di sistema.
L'art. 28 riguarda il processo di gestione dei fornitori esterni come responsabili e subresponsabili. Il DPO gestisce anche i diritti dell'interessato, artt. 12-23 invia diretta o per conto del titolare.
Il GDPR non dà una definizione di DPO ma ne delinea le funzioni. È stato reso obbligatorio in quanto i due compiti principali sono la consulenza e informativa al responsabile del trattamento dati e di sorveglianza di conseguenza regolamentando tale funzione l'ente o l'azienda riconosce un certo compenso per il servizio complessivo offerto dal DPO.

Human Enhancement: i diritti alla prova del potenziamento umano

Nel 2009 lo studio dello STOAè un punto di riferimento per il tema del potenziamento umano sia in termini di strumenti scientifici sia giuridici. La Convenzione di Oviedo è stata definita il primo tentativo di mettere allo stesso piano l'evoluzione scientifica e i diritti umani (eguaglianza, autonomia, salute, dignità).
Si intende la modifciazione mirata a migliorare le performance dell'umano attraverso scienza e tecnologia sul corpo umano stesso e si distingue per i interventi non potenzianti ma preventiva, potenzianti terapeutici e potenzianti non terapeutici (definizione dello STOA). Qui emerge anche il tema dei vaccini infatti Harris sottolinea che le prime forme di potenziamento possano essere considerate i vaccini. Tale definizione mette in gioco interventi basati sulla tecnologia e la scienza, il potenziamento umano si ricollega a sviluppi scientifici perciò possiamo ricollegare questo fenomeno a un momento storico preciso, la seconda metà del secolo scorso quando vi è stato uno sviluppo della terapia genica.
Un'altra definizione fa riferimento a un poteznaimento biomedico consistent ein un intervento deliberato che applicala scienza biomedica e mira a migliorare capacità esistenti o crearne di nuove agente direttamente sul corpo e sul cervello.
Tali forme di potenziamento sollevano questioni etiche simili.

Abbiamo varie forme di potenziamento:

- Fisico; doping
- Cognitivo; può avere tre scopi: miglioramento della capacità mnemonica, cambiamento dell'umore in situazioni non patologiche, potenziamento morale.

Il processo del potenziamento umano si innesta ma non si esaurisce sulla medicalizzazione della società che invece è un fenomeno studiato a partire dagli anni '60 da Peter Conrad che consiste in processi medicalizzati legati a patologie cioè descritti con linguaggio medico e trattati con strumenti medici.
Tale fenomeno ha avuto un anticipazione in ambito sportivo negli anni '20, '30 nel contesto americano quando si è iniziato ad applicare la ricerca scientifica per gli atleti d'élite e in ambito europeo durante il fascismo.
Il potenziamento umano ha uno scopo non terapeutico e questo rende difficile trovare una giustificazione etica e giuridica, poi si tratta di un tema incentrato sul superamento di presunti limiti non strettamente legati a patologie.
Il postumanesimo nasce per Badmington nel 1982 ed è una visione per la quale ciò che è umano è soggetto a una trasformazione radicale che porterà a tale sviluppo postumano, la natura umana è malleabile dalla tecnologia.
Poi si è affermata la corrente del Transumanesimo per il quale vi è la necessità di utilizzare la tecnologia per superare i limiti naturali che in questa visione sono valutati come negativi, ad esempio si vorrebbe imporre un obbligo morale e istituzionale di utilizzo delle tecnologie per migliorarsi ma questo significherebbe proporre di utilizzare il diritto per imporre la visione transumanista.
Diventa così rilevante il tema dei diritti fondamentali, l'art. 76 del Codice di deontologia medica Titolo XVI tratta del potenziamento di capacità fisiche e cognitive effettuato dal medico che deve rispettare e salvaguardare la dignità dello stesso, identità e integrità delle sue peculiarità genetiche e i principi di proporzionalità e precauzione. Il problema invece sussiste quando si ritrovi una disciplina specifica per il potenziamento umano perché è fondamentale la tutela del diritto alla salute.

Cyberwar

In tempi antichi l'idea per la quale lo Stato ha il diritto di fare la guerra ha comportato una limitazione della conflittualità bellica nel senso che nel Medioevo vi era la cosiddetta "guerra giusta" dal punto di vista sostanziale.
Oggi nella nuova visione gli Stati si riconoscono e rispettano come tali reciprocamente e si innesca un meccanismo per cui dalla prima guerra mondiale la guerra diventa aerea non più terrestre grazie allo sviluppo tecnologico bellico.
Si è pensata a una responsabilità degli Stati, un tribunale penale internazionale e il Patto di Kellogg-Briand col quale la guerra viene bandita, tuttavia oggi si parla comunque di uso della forza ma che deve essere autorizzato dal Consiglio di Sicurezza dell'ONU o per legittima difesa in caso di attacco attuale. Con la seconda guerra mondiale la guerra ha superato ogni limite.
Dal punto di vista giuridico se a partire da un attacco cibernetico si possa effettuare un inquadramento dal punto di vista giuridico-internazionale e a tale scopo è stato scritto il Manuale di Tallinn.
Oggi si parla di guerra cibernetica per la quale si intende una guerra diversa da quella materiale ma capace di provocare ugualmente perdite umane o di posizioni strategiche (ad esempio l'inserimento di un malware chiamato Stuxnet all'interno di una delle turbine della centrale

nucleare di capace di produrre un danno paragonabile a quello di un bombardamento aereo). Ormai si va verso la robotizzazione della guerra attraverso l'uso di droni tuttavia ci sono anche i malware dedicati ad operazioni di guerra.
La legge del perimetro strategico italiano del 2019 ha regolato la cybersecurity.

Genome editing: biotecnologie innovative e vuoto normativo

Le biotecnologie hanno segnato un asapere di frontiera a livello globale con ricadute sociali ed economiche. tali potenzialità richiedono anche una solida regolamentazione in modo che i risultati sperati siano di beneficio per la società riducendo i rischi. Per questo esse si caratterizzano per l'**analisi rischi-benefici**: bisogna bilanciare gli interessi e le esigenze della scienza, ricercatori e della società stessa.
Dal 1991 in Italia sono stati pubblicati una seire di pareri del comitato nazionale di bioetica sugli interventi tesi a modificare gli organismi in modo da correggere eventuali patologie genetiche (OGM) sia degli essere umani sia di animali e piante; ma anche su altre partiche riguardanti le biotecnologie animali, ambientali come la clonazione e le implicazioni di tale tecnica. Le linee generali sono state definite nel 1997 nelle loro caratteristiche essenziali ma il CNB ha utilizzato termini molto efficaci nel porre l'accento su alcuni elmenti fondamentali come la pervasivitù. Parliamo infatti di tecnologie che, rispetto a quelle tradizionali, investono la salute umana chiamando in causa il rapporto tra salute, politica, economia.
La deifnizione del 1994 data dal Congresso degli U.S.A consiste in ogni tecinca che utilizza organismi viventi o loro parti per migliorare piante o animali e sviluppare organismi specifici.
Nel 2015 è stata scoperta una tecnica di intervento sul genoma umano, genome editing. A seguito dello sviluppo delle biotecnologie si sono create aspettative per un miglioramento della salute, infatti un obiettivo della ricerca è proprio il benessere e l'allungamento dell'aspettativa di vita.
Si parla anche di libertà procreativa positiva difatti si può controllare in laboratorio durante tutto il processo; pensiamo anche all'interoduzione di tecniche di diagnostica per impianto; che permettono di selezionare gli embrioni da usare per la procreazione medicalmente assistita; terapie di sostegno vitale.
i processi di democratizzazione che hanno assecondato maggiori libertà e diritti collettivi (libertà procreativa, consenso informato,) allora possiamo dire che le biotecnologie vanno a inserirsi in tale ambito anche per l'aumento delle tensioni, della responsabilità legate a tali tecniche. in ogni caso esistono limiti invalicabili oltre i quali l'essere umano non può spingersi: l'obiezione più ricorrente viene riassunta nell'espressione "voler fare Dio", infatti gli interventi sulla linea germinale, le modificazioni si trasmettono alle generazioni future, al contrario delle mofidicazioni genetiche concentrate solo sulla linea somatica cellulare.
Altro aspetto fondamentale è l'argomento del *pendio scivoloso* che cerca di individuare a livello normativo i pro e i contro di un piano regolativo giuridicamente solido.
Si è verificato uno scontro tra coloro che ritengono esserci regole di principio giurisprudenziali nel mondo occidentale e coloro per cui alla luce del pluralismo morale e la sensibilità dei temi la regolazione giuridica dovrebbe essere affidata ai giudici capaci di interpretare i principi sanciti dalle costituzioni e da importanti fonti sovranazionali e dunque la soft law.
All'interno di questi due massimi sistemi vi sono varie correnti ma si possono sintetizzare in due modelli:

1. forte; invoca una legisalzione bioetica specifica orientata alla tutela della natura umana che tengano conto dei valori conoscibili e i principi morali oggettivi, orientamento interventista
2. debole; l'unico è trovare un equilibrio tra le istanze in gioco, un diritto guidato dalla plasticità della bioetica ma diviso a sua volta in due sotto-modelli di cui uno liberale che ritiene opportuno disporre dell'apparato giurisprudenziale laddove il giudice svolge una funzione creativa sempre rivedibile.

Ad oggi si pone il problema della precauzione, sicurezza degli interventi a livello germinale consistenti nella produzione di embrioni ad hoc per testarne gli effetti collaterali legati alla sostituzione del gene difettoso con il gene sano.

Data society: governo dei dati e tutela dei diritti nell'era digitale

Il termine deriva dall'evoluzione dell'attuale società, non più trainata dall'ecnomia basata sui dati in cui essi stessi stavano acquisendo centralità ma utilizzati in modo da plasmare la realtà stessa e così l'uomo.

La governance della società digitale passa dalla data governance, diritto deputato a regolare la vita e chiamato a disciplinare dati e algoritmi al fine di tutelare i diritti, sanare i conflitti e fornire certezza giuridica alla data society pervasa dai dati per plasmare l'uomo come data subject.

Il diritto è chiamato a dialogare con la lex informatico o digitalis, le regolo applicate dal codice informatico condizionnano ogni altr aforma di regolazione, compresa quella giuridica.

L'uomo può intervenire sulle stesse attraverso il diritto.

Altra difficoltàperò è rappresentata dalle geometri di potere: infatti gli Stati sono ormai caratterizzati da un assenza di confini, dimensioni globali dell'oggetto di regolazione, indebolimento della sovranità e pretesa di potere, erosione monopolio; colossi tecnologici favoriti da dimensione sovranazionale, libertà di commercio, regole inadeguate si presentano come spazi di libertà ma assumon oforme ed esercitano un ruolo concreto nella regolazione (controllori del pedaggio di accesso alla vita digitale).

SI presenta il rischio big brother, big other e capitalismo della sorveglianza.

Inoltre gli individui sono deboli nei confornti degli uni e degli altri, c'è un'apparente lbiertà, rischio di mercificazione, di scoietà del controllo si è parlato di superpanopticon, una società continua, diffusa, distante da connotazioni carcerarie che ricorda il mondo di Axley in cui infliggendo piacere si infliggeva il dolore del controllo. Il potere è nelle mani di pochi soggetti, vi sono automazioni e dittature dell'algoritmo, contrattazioni inique, discriminazioni, disparità, filter bubble e balcanizzazione delle opinioni quindi apparente libertà.

Enormi volumi di dati detenuti da grandi organizzazioni provenienti da diverse fonti e analizzati per mezzo di algoritmi sono ormai diffusi con tecniche di data mining, apprendimento automatico, deep learning che simulano il ragionamento umano, si parla di big data.

Questa varietà di dati disciplinati da normative diverse genera un problema giuridico e sopratutto la velocità con cui i dati sono elaborati. Parliamo di sistemi che mostrano un comportamento intelligente analizzando il prorpio ammiente e compiendo azioni con un certo grado di autonomia per raggigunere specifici obiettivi. I software agiscono nel mondo virtuale e incorporano l'AI.

Bisogna evidenziare anche il dato fondamentale relativo alla conoscenza sul presente e sul futuro attraverso l'interpretazione di esigenze, profilazione, monitoraggio e supporto alle

decisioni: capacità di predizione e servizi di miglioramento della qualità della vita, difatti si ha l'impiego nei servizi, nello svolgimento di funzioni, nelle previsioni di ordine politico ma anche nel contesto privato.
I big data possono rispondere alla tutela di interessi generali ma anche alla realizzazione di vantaggi economici ed obiettivi privati.
In tale contesto di riferimento emergono una serie di prblematiche etico-giuridiche derivanti in parte dal funzionamento degli algoritmi: innanzitutto l'algoritmo si basa su logiche deterministiche al contrario del nesso causale tipico del ragionamento umano. Muta il modo di conoscere e misurare fatti e persone, si possono analizzare tendenzialmente tutti i dati disponibili, inferenze ecorrelazioni, logica deterministica, probabilità e non causalità, non ci si chiede il motivo. Si crea più confusione e meno esattezza a fronte della conoscenza e comprensione grantita da tali strumenti.
Negli algoritmi in particolare osno presenti alcune criticità: orientamento ai valori, prescrittivo, formale e lento, poggiante su logiche deterministiche.
Si pone la necessità di dati di qualità: le basi dei dati devono essere costituite e annotate correettamente garantendo neutralità e assicurando un elevato grado di correttezza; inoltre si ha una natura inferenziale e probabilistica delle elaborazioni infatti l''nalisi teprica è un processo di approssimazione con il rischio di trarre conclusioni imprecise (rishcio di bias, errori tecnici, manipolazioni umane, discriminazioni).
Sarebbe necessaria una'adeguata contestualizzazione, analisi e interpretazione: saper fare le domande giuste ai dati e saper comprendere le risposte (caso celbre è Winscosin vs Eric del 2016).
Non si tratta solo di un problema di possibile discriminazione ma il rischio è creare un'asimmetria con pochi colossi digitali e poteri pubblici che raccolgono ed elaborano big data.
Si rende necessario il rispetto di principi etico-giuridici appositamente individuati ma è arduo in quanto vengono percepti in maniera differente a seconda delle culture perciò ci si chiede come applicare tale meccanismo a una macchina autonoma.
Si rischia si incidere su posizioni individuali con praticolare peso come il diritto alla vita e in caso di collisione inevitabile bisogna stabilire dei criteri etici.
CI si chiede anche ci sia il titolare dei dati: proprietà tradizionale civilistica, prospettiva contrattuale (autonomia contrattuale), proprietà intellettuale (diritto d'autore).
Inoltre chi sarà responsabile dell'eventuale danno: titolarità diverse a seconda del caso e la partecipazione umana, sistemi agenti (imputabilità autonoma), sistemi di assicurazione obbligatoria e forme di responsabilità oggettiva.
Si rende necessaria anche una classificazione dei livelli di autonomia dell'AI per quanto riguarda la soggettività. Si pongono problematiche utilizzo dell'AI in ambito pubblico relative al rispetto di norme e principi dell'ordinamento (caso del TAR Lazio sull'assegnazione dei docenti alle sedi disponibili nell'organico della scuola).
Ultimo problema è relativo alla protezione dei dati personali: innanzitutto è molto noto il Regolamento sui dati personali e meno quello sui dati non personali. Nel caso dei big data i dati sono legati in modo indissolubile perciò la Commissione europea con un atto informativo ha affermato che in tali casi bisogna applicare la disciplina dei dati personali se anche un piccola parte di essi sono dati personali.
I principi di trattamento previsti dalla noramtiva europea sono: la limitazione delle finalità, minimizzazione dei dati, esattezza e accuratezza dei dati.

Inoltre si pongono problemi relativi al consenso dell'interessato, vi è un'apparente libertà da parte di un soggetto. Poi la stessa distinzione tra dato personale ed anonimo non regge in quanto può non essere sufficiente il consenso dell'interessato dato che le decisioni possono riversarsi su una comunità intera.
L'art. 22 sui processi decisionali automatizzati stabilisce che l'interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato ma è affievolito in quanto non si applica qualora sia necessaria per una trattativa privata.
Alcune strade possono essere percorse dal lato della valorizzazione del ruolo umano, dominare la tecnologia e portare al centro i diritti dell'uomo ma bisogna trovare gli strumenti, perciò sta prendendo piede l'idea dell'accountability, privacy by design, incorporazione del diritto nella tecnica, reponsabilità e sistema sanzionatorio, trasparenza algoritmica tra le informazioni fornite all'interessato e su cui ha accesso.
Il Data governance Act ha voluto valorizzare la natura del dato come bene pubblico rispettando i dati anonimi: sia a livello di negoziazione che di prblematiche può intervenire una forma di tutela collettiva, il singolo può non riuscire a tutelarsi e, ferma l'autonommia individuale, si pensa di intergrare con forme di tutela collettiva (ubi data society, ubi ius).