Cyber and Computer Law (Italian version)

Argomento 1:

Élite ha il potere di costruire ed eseguire algoritmi, avendo il controllo del trattamento dei dati. L'umanità è soggetta a questo.

Il potere degli algoritmi influenza tutto l'ordine sociale sostituendo le relazioni con connessioni che iniziano l'oblio della relazione interpersonale attraverso le connessioni funzionali numeriche che fluiscono nella rete.

La differenza tra relazioni e connessioni chiarisce l'impatto che ha il potere degli algoritmi sulle persone. La differenza principale è che all'interno delle connessioni, ogni essere umano viene trattato come un elemento calcolabile, privato della creatività.

Il potere degli algoritmi è esercitato da gruppi ristretti in grado di spiare e acquisire un'immensità di dati ed elaborarli tramite il potere dei computer che eseguono grandi quantità di operazioni.

Élite, appunto, considera le relazioni come connessioni esecutive e non come relazioni creative.

La quantità crescente e l'accelerazione dei dati funzionano in modo efficiente se sono confinati negli schemi delle connessioni e non aperti a relazioni discorsive. Questi schemi però non tengono conto della parte più essenziale di un dialogo interpersonale come ad esempio, la differenza tra le due persone, il contenuto del discorso di entrambi e soprattutto i disaccordi tra di loro.

Per questo motivo le connessioni tramite algoritmi sono più efficienti, perché non considerano gli elementi creativi, ma non descrivono in modo esaustivo l'originalità delle relazioni.

Il funzionamento dell'algoritmo è quindi basato sulle tracce lasciati dall'utente in rete, quindi da un immagine più oggettiva dell'utente e non nel dettaglio. È quindi basato sulla quantità delle informazioni e non sulla qualità di esse.

Quindi in conclusione le connessioni sono spersonalizzate, mentre le relazioni sono interpersonali.

Argomento 2:

Algoritmo: è la fase preliminare del programma elettronico che consiste in una serie di istruzioni volte a risolvere un determinato problema tramite un computer. Quindi possiamo dire che è un processo che porta a una soluzione attraverso una serie di regole uniche e limitate.

Dalle origini dell'informatica è nato l'uso dei computer e degli algoritmi relativi alla conoscenza giuridica.

- 1949: Lee Loevinger, ha inventato la giurisprudenza dando inizialmente una definizione generica e un'indagine scientifica sui problemi legali.
- 1950: Norbert Wiener, riferendosi idealmente all'illuminazione legale di Beccaria, scrisse un intero capitolo in uno dei suoi libri dove sosteneva la sua formalizzazione logica e una conseguente attività giurisprudenziale sillogistica volta a risolvere i giudizi.

Beccaria, Wiener e Loevinger, credevano che la meccanizzazione del ragionamento legale sia la soluzione per limitare o addirittura eliminare la lentezza e l'incertezza delle decisioni legali.

- 1950: Alan Turing lanciò il famoso test che dimostrava un'analogia tra cervello artificiale e cervello biologico e nel 1956 nacque l'intelligenza artificiale.

Esistono due metodi per modellare l'intelligenza umana, un logico-cognitivista e un biologo-connettista:

1. Secondo il cognitivismo la mente non è altro che un elaboratore di simboli. Codifica gli stimoli che arrivano dall'esterno, li elabora seguendo regole o meta-regole, arriva a una soluzione e la realizza. Il primo metodo di IA cognitivo è orientato all'uso di sistemi di ragionamento simbolico. Questi sistemi, chiamati esperti, sono simbolici perché trasformano i simboli che rappresentano le cose nel mondo reale in altri simboli secondo regole esplicite.
2. Il connessionismo parte dalla natura biologica dell'intelligenza e, riferendosi alla neuroscienza, cerca di capire come comportamenti intelligenti e umani possano emergere dai sistemi neurali e ormonali. Il secondo metodo di IA neurale adotta un approccio alternativo alla modellazione dell'intelligenza ispirata dalla struttura dei sistemi neuronali biologici che sono composti da milioni di neuroni. Questi sistemi sono chiamati neurali perché imitano questa struttura biologica.

Prospettive dell'IA:

- Negli anni '50 e '60 il campo legale è certamente influenzato dalle prospettive dell'IA, ma il dominio legale usa termini come cibernetica, logica moderna e simbolica, analisi quantitativa, algebra booleana, giustizia artificiale, evitando per il momento il termine intelligenza artificiale.
- Nella metà degli anni '70 iniziò un lungo periodo scientifico-culturale che, collegando la logica, la tecnologia dell'informazione e la legge, svilupperà prima la ricerca sui sistemi sperimentali basati sul paradigma simbolico dell'intelligenza artificiale, poi verso i sistemi neurali basati sul paradigma dell'IA sub-simbolica fino a sistemi basati sulla conoscenza derivata dalla rete e sull'apprendimento gratuito basato esclusivamente o principalmente su questa conoscenza.

Tutti questi sistemi cercano di riprodurre automaticamente il ragionamento legale attraverso diversi algoritmi. Possiamo definire il primo logico-simbolico e "etero diretto" nelle due varianti, basate su regole e basate sul caso (algoritmi esecutivi di regole logiche o semantiche esterne stabilite a priori), il secondo neurale-sub simbolico ed etero diretto (algoritmo di apprendimento empirico-casuistico basato su determinate variabili), ed il terzo neurale-sub simbolico "auto-diretto" (apprendimento empirico-casuale algoritmi parzialmente indeterminati).

La giustizia algoritmica si sviluppa attraverso varie fasi, un comportamento predittivo del comportamento dei giudici basato su elementi presi da quelli precedenti, tipico della cultura dello sguardo deciso, un predittivo logico-deduttivo basato su un formalismo totalmente determinato (che regola algoritmi totalmente determinati), un predittivo empirico-neurale basato sull'apprendimento esperienziale a partire da variabili iniziali di casi iniziali prestabiliti (algoritmi parzialmente determinati). Possiamo infine immaginare una quarta fase ancora futuristica totale empirico-neurale basata sull'apprendimento gratuito. In quest'ultimo caso, viene indicato solo l'obiettivo, i dati sono forniti da Internet e le regole create dal funzionamento della rete neurale.

Argomento 3:

Cos'è la robotica? La robotica è l'area dell'intelligenza artificiale interessata dall'uso dei robot, ovvero, macchine che "percepiscono, pensano e agiscono" (cit. Bekey). È un campo interdisciplinare per eccellenza e coinvolge non solo l'intelligenza artificiale e l'informatica, ma anche la cibernetica, la fisica, la matematica, la meccanica, l'elettronica, le neuroscienze, la biologia e le discipline umanistiche.

La rete europea di ricerca sulla robotica si è classificata in otto tipi, tra cui umanoidi, robot di servizio adattivi, robotica di rete e per esterni, edutainment e così via.

I robot possono essere killers? La prima metafora dei robot come assassini è illustrata dagli avvertimenti di Asimov nei suoi romanzi e dalla prima legge della robotica, secondo la quale nessun essere umano può essere ferito dai robot (ciò che accade spesso nelle storie di Asimov). Una delle aree più rilevanti e sviluppate della

robotica di oggi, dopo tutto, riguarda applicazioni militari come armi intelligenti, soldati robot e persino soldati sovrumani con sistemi di sensori, dispositivi di realtà aumentata o esoscheletri.

La seconda immagine è quella dei "frigoriferi". Gli studiosi usano spesso questa metafora per prevenire alcune sopravvalutazioni nel dibattito attuale, come i killer robot e altri agenti artificiali che superano in astuzia gli esseri umani, in modo che noi, come specie, dovremmo presto affrontare l'estinzione poiché robot intelligenti ci sostituiranno come prossimo passo nell'evoluzione. Contro questo tipo di tecno-determinismo e altre speculazioni di fantascienza, la metafora del frigorifero propone un quadro più sobrio dei robot e della loro peculiare autonomia. (“Possono affrontare con successo i loro compiti, anche se hanno l'intelligenza di un frigorifero”).

Troviamo l'immagine dei robot come "schiavi". Analogamente al modo in cui gli schiavi erano disciplinati dalla legge romana antica, possiamo considerare i robot come agenti autonomi che sono tuttavia semplicemente "cose", alla fine mancano di doveri. Questo terzo parallelismo fa luce su una nuova forma di agenzia, in quanto "come uno schiavo, [il robot] è in grado di prendere decisioni che influenzeranno i diritti (e, in seguito, le responsabilità) del suo padrone. Facilitando le transazioni commerciali, gli agenti autonomi hanno la capacità di aumentare l'efficienza del mercato. Come uno schiavo, un agente autonomo è in grado di fare del male. "(Katz 2008).

Prospettiva legale: Forse è troppo presto per prevedere la responsabilità personale dei robot nelle questioni penali**.** Tuttavia, è giunto il momento di riconoscere seriamente che il comportamento dei robot dovrebbe essere legalmente considerato come una nuova fonte di responsabilità personale per gli atti altrui (ad esempio, il diritto illecito e la responsabilità vicaria nella tradizione del diritto comune e la sua controparte nel diritto civile, ovvero, "responsabilità oggettiva" o responsabilità senza colpa).

Chiarimenti riguardanti 3 questioni:

1. Analizzare come i robot hanno simulato il dibattito accademico sui campi fondamentali della giurisprudenza e della teoria legale/giuridica. Più in particolare, considerare il caso dell'ermeneutica e lavoro di Asimov sulle leggi della robotica.
2. Illustrare l'attuale stato dell'arte nelle scienze giuridiche: un'attenzione particolare è rivolta alle nozioni di agenzia e responsabilità civile.
3. Spiegare i motivi per cui pensiamo che dovremmo aggiungere una nuova forma di responsabilità legale per il comportamento altrui: i robot, proprio come gli schiavi, sono considerati "cose" con significativa autonomia e forse alcuni doveri specifici.

Analogie giuridiche: Da un lato, il ruolo di alcune metafore è quello di afferrare una serie di questioni legali come se i robot fossero assassini, schiavi e simili, al fine di rispettare il dogma del diritto civile come un sistema autoreferenziale in cui l'analogia potrebbe riempire le sue lacune normative. Dall’altro, le metafore possono essere usate per chiarire alcune domande tipiche riguardanti il campo che gli studiosi di solito chiamano giurisprudenza o "teoria generale del diritto". Per esempio, assumendo le leggi della robotica di Asimov, è possibile illustrare alcuni argomenti legali classici.

Le tre leggi della robotica di Isaac Asimov:

1. ***Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno. (purché tali ordini non vadano in contrasto alla Legge Zero).***
2. ***Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla (Legge zero o alla) Prima Legge.***
3. ***Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con (la Legge Zero,) la Prima o con la Seconda Legge.»***

Le Tre Leggi vennero estese con una quarta legge, la 'Legge Zero', così chiamata per mantenere il fatto che una legge con numero più basso soprassedesse a una con numero maggiore.

> 0. ***Un robot non può recare danno all'umanità, né può permettere che, a causa del proprio mancato intervento, l'umanità riceva danno.***

Le altre leggi vennero poi rimodificate aggiungendo alla fine *"Purché questo non contrasti con la Legge Zero".*

Il legame tra le leggi della robotica e la legge naturale ci suggerisce di riconsiderare il significato dei comandi legali, poiché la legge naturale aveva lo scopo di guidare le nostre azioni nello stesso modo in cui le leggi della robotica avrebbero diretto il comportamento dei robot. In entrambi i casi, la legge può essere considerata un imperativo oggettivo la cui violazione implicherebbe una violazione della natura dell'agente.

La prima legge della robotica dovrebbe essere integrata da una meta-legge, che determina che un robot non può agire se le sue azioni non sono soggette alle leggi della robotica. Una seconda sezione è aggiunta alla seconda legge in quanto "un robot deve obbedire agli ordini impartiti da robot superiori". Inoltre, una nuova prima sezione dovrebbe essere inserito nella terza legge e così via.

I problemi etici che coinvolgono la legge dovrebbero essere aggiunti all'elenco dei possibili parallelismi tra le leggi della robotica e la teoria giuridica.

Possiamo sollevare ulteriori domande sul libero arbitrio come base della responsabilità delle persone, questioni di paternalismo robotico e obiettori (oppositori) di coscienza, fino al contenuto minimo delle leggi naturali.

Tre domande:

1. In primo luogo, la proprietà specifica delle leggi della robotica, vale a dire la loro natura astratta e generale, comporta il difficile compito di applicare queste leggi in un determinato contesto: le circostanze del contesto influenzano il modo in cui interpretiamo tali regole generali?
2. La vaghezza del linguaggio ordinario, come nel caso di termini cruciali come "danno" o "ordine", mette a repentaglio la possibilità di assicurare l'osservanza meccanica delle regole: sarebbe possibile sviluppare modelli calcolabili in modo da comprendere non solo le norme giuridiche e concetti ma anche agenti legali?
3. Infine, la corretta comprensione della legge è caratterizzata da una serie di criteri per l'interpretazione delle leggi del sistema.

Come esemplificato dal lavoro di Asimov, i robot usavano adottare una sorta di lettura letterale nei suoi primi romanzi: solo i robot estremamente più sofisticati delle storie successive iniziarono ad impiegare tecniche ermeneutiche complesse come interpretazioni rigorose o estese delle leggi, letture evolutive e teleologiche dei testi e così via.

Ovviamente, dato l'approccio troppo articolato dei teorici legali, il rischio finale (e fatale) di tutte queste analisi sintattiche è la fine della paralisi.

In qualche modo, ciò che gli studiosi dibattono incessantemente in termini di:

- configurazioni meccaniche contro olistiche del sistema,
- lettura letterale contro contestuale dei testi,
- comprensione analitica contro sistematica delle norme,

può portare al risultato di alcune trame di Asimov, cioè lo stallo dei cervelli positronici dei suoi robot.

La responsabilità morale dei robot: Dobbiamo ammettere la responsabilità morale dei robot negli omicidi? Estendendo la classe di agenti moralmente responsabili in modo da includere l'agenzia artificiale dei robot, non dobbiamo ammettere né la loro responsabilità morale né la loro responsabilità penale. Come nel caso delle azioni dei bambini o del comportamento degli animali, la ragione dipende dalla necessità di differenziare la fonte delle azioni morali pertinenti dalla valutazione degli agenti come moralmente responsabile di un determinato comportamento.
Questo è il motivo per cui Floridi e Sanders, che riconoscono la responsabilità morale degli agenti artificiali, ammettono prontamente "che sarebbe ridicolo lodare o incolpare un agente artificiale per il suo comportamento o accusarlo di un'accusa morale".

Secondo l'attuale stato dell'arte del diritto penale, sarebbe inutile discutere davanti a un giudice se un robot debba essere considerato o meno un "assassino", un "ladro" e così via.
Anche se assumiamo che una sorta di responsabilità morale sia un requisito necessario per la responsabilità legale, la prima non rappresenta la condizione sufficiente della seconda, perché gli intervistati dovrebbero essere soggetti al normale processo di apprezzamento morale al fine di determinare se sono colpevoli in nome della legge.
Altrimenti, offuscando la responsabilità, saremmo costretti a tornare ai giorni in cui venivano comunemente condotti processi penali contro animali e persino cose senza vita.

Tre domande:

1. ***Possiamo calcolare i robot che pagano il loro debito con la società?***
2. ***Possiamo correggere il loro carattere morale in modo che i robot capiscano perché non dovrebbero ripetere un male?***
3. ***Dovremmo punirli in modo da dissuadere gli esseri umani dal commettere simili errori?***

Argomento 4:

Algoritmi come strumenti (tools) spersonalizzanti

La ricerca del significato è un atto umano: La creazione di significato è costituzionalmente extra-sistemica.

Il significato non può essere perseguito dalle previsioni prodotte dalle fasi computazionali e operative, e non è determinato da un automatismo macchinico (meccanico?); è una manifestazione del rischio legato alla libertà, che coinvolge altri esseri liberi in una convivenza governata dalle norme legali, stabilite secondo il principio di uguaglianza.

Gioco, Dialogo, Giustizia: L'ego si dimostra centrale, costantemente rivolto a sé stesso nell'indirizzamento essenziale verso gli altri.

L'atto di giocare (playing), il dialogo e le relazioni giuridiche condividono la stessa gratuità della creazione di significato, che costituisce il momento genetico di questi diversi fenomeni e rimane sostanzialmente irriducibile alla funzionalità operativa.

La gratuità è disfunzionale, (sorprendente) genera lo stupore costitutivo di tutti gli itinerari del pensiero umano, non limitato al funzionamento del mercato e ai profitti del sistema basato sulla produzione/consumo, poiché questi itinerari superano ogni quantificazione numerica o determinazione computazionale, trovando il loro vero significato nelle relazioni dialogiche, non pre-calcolabili, non risolvibili nel trattamento dei dati attraverso gli schemi degli algoritmi.

(Dialogo, legge, gioco) Questi fenomeni condividono la struttura comune diretta a indagare e creare un significato, non basato sulla replica delle leggi biologiche, ma sull'istituzione di relazioni intersoggettive regolate da un "accordo di instaurazione" tra gli individui.

Diverse concezioni del tempo: Nella certezza computazionale dell'elaborazione dei dati non è rimasto spazio libero, che consente un possibile senso del futuro.

Al contrario, tutto è confinato in un accordo modellato secondo schemi algoritmici, che racchiudono un senso di tempo assolutamente dilatato in ciò che sta per arrivare, libero da rischi e meraviglie, tipico della non prevedibilità del futuro in aumento nel dialogo.

Ciò che viene dopo è rappresentato dallo sviluppo di un presente già dato, il futuro non ha una qualifica limitata nell'esecuzione di un presente già dato, ma mantiene le ipotesi formative aperte a un senso originale, qualificando la storia come qualcosa che non è riducibile a l'esecuzione di una sequenza algoritmica numerica.

Comunicazioni indirette: La comunicazione è indiretta quando va oltre il flusso di connessioni / informazioni, che passano da un essere umano a un altro.

È indirizzata da una persona all'altra, che la riceve interpretandola, rischiando le proprie scelte interpretative e i comportamenti relazionali che ne discendono, rispettando sempre il principio di uguaglianza per quelle relazioni radicate in una reciprocità dialogica.

Comunicazioni dirette: Le procedure degli algoritmi appartengono interamente ai modelli di comunicazione diretta, ovvero connessioni di informazioni contenenti elaborazione dei dati, che richiedono di essere eseguite in modo impersonale, senza mettere nulla di originale, di una sola persona.

L'affermazione invasiva delle comunicazioni dirette dissolve i modelli delle comunicazioni indirette e quindi annulla il diritto all'autenticità nel processo di creazione di una personalità che è originariamente a rischio di un singolo essere umano.

In questa direzione, il soggetto viene trasformato in entità senza volto, funzionale al flusso e alla concretizzazione di operazioni computazionali che ambiguamente appartengono a tutti e a nessuno, provenienti da un itinerario che impone automatismi esecutivi ed emargina l'originalità degli esseri umani.

Gioco, Dialogo, Legge: Il gioco, il dialogo e la legge sono estranei agli schemi degli automatismi esecutivi.

Se negli esseri umani tutto fosse risolto nell'esecuzione dei risultati degli algoritmi, sarebbero perse:

- la non prevedibilità degli atti di recitazione, dei contenuti dei dialoghi e delle relazioni giuridiche
- la responsabilità / imputabilità dinanzi al giudice delle proprie decisioni che incidono sull'esistenza delle altre

Algoritmi al potere: viene rafforzata l'incidenza degli automatismi che sostituiscono il rischio di scelte, derivante dalla riflessione che prende le distanze dallo stato dei fatti e orienta gli atti verso una creazione di significato, che sorge nel dialogo interpersonale.

Possono gli algoritmi essere legalmente responsabili? Gli algoritmi sono un insieme di operazioni senza intenzioni e quindi privi della capacità di concepire e fare scelte e decisioni legalmente attribuibili a un ego.

Il giudizio giuridico può essere destinato esclusivamente a un "io", chiamato a rispondere prima di un altro "io", quello dei magistrati che esercitano l'attività giurisdizionale, terza e imparziale, attraverso l'arte dell'interpretazione.

Non esiste un tribunale destinato allo svolgimento di un processo, che considera un'entità giudicabile un algoritmo o un insieme di algoritmi.

Argomento 5:

Una responsabilità per i robot: Le ragioni alla base della legittimità di punire la legge penale moderna come la teoria della punizione, della prevenzione speciale e generale, sarebbero prive di significato.

Ricorda le 3 domande, viste precedentemente:

1. *Possiamo calcolare i robot che pagano il loro debito con la società?*
2. *Possiamo correggere il loro carattere morale in modo che i robot comprendano appieno il motivo per cui non dovrebbero ripetere un'azione malvagia?*
3. *Dovremmo punirli in modo da dissuadere gli esseri umani dal commettere simili errori?*

Finché gli avvocati credono che gli omicidi e altre questioni criminali presuppongano necessariamente la responsabilità degli esseri umani, lo stato dell'arte nella scienza giuridica pensa ai robot non come "assassini" o "ladri".

La sua immagine mentale è che i robot sono artefatti tecnologici completamente insignificanti, non diversi dai tostapane o dalle automobili (→ non penalmente perseguibili).

Robot e legge privata: La robotica legale di oggi è rilevante nell'ambito della legge che appartiene al campo del diritto privato, vale a dire gli obblighi contrattuali ed extracontrattuali.

Mettendo da parte rigorosi obblighi contrattuali, poiché le condizioni, i termini e le clausole dipendono sia dall'accordo volontario tra privati che un tribunale farà valere, sia dalla natura commerciale o non commerciale di tale accordo. È sufficiente sottolineare la differenza tra :

- Robotica militare
- Robotica industriale

Ciò che un avvocato inglese o americano definirebbe una sorta di "torto", vale a dire "obblighi tra privati imposti dal governo" per risarcire i danni causati da illeciti.

Possiamo distinguere tre tipi di responsabilità:

- Responsabilità per danni causati da torti intenzionali: La responsabilità per un illecito intenzionale è stabilita quando una persona ha volontariamente compiuto l'azione illecita
- Tortuoso legato alla negligenza: Esiste una responsabilità basata sulla mancanza di debita cura quando la persona ragionevole non riesce a proteggersi da un danno prevedibile.
- Responsabilità senza colpa: La responsabilità rigorosa (strict liability) è stabilita senza colpa come nel caso paradigmatico di responsabilità per prodotti difettosi, che può essere dovuto alla mancanza di informazioni su alcune caratteristiche del manufatto. (→ Motivo per ci sono quelle etichette estremamente dettagliate e talvolta strane sui prodotti, con le quali i produttori avvertono di rischi o pericoli legati all'uso improprio del manufatto.)

Indipendentemente dal tipo di illecito che stiamo affrontando, "quando più parti o più eventi hanno messo in moto una catena di eventi che porta al danno dell'attore, i tribunali americani e britannici usano la dottrina della" causa prossima "(a volte chiamato "causa legale") per guidare le giurie nel decidere dove tagliare la catena di responsabilità ''.

Negligenza: Quando la condotta negligente della querelante ha contribuito alle sue lesioni personali può essere ripartito a causa di negligenza contributiva.

Rispetto a questo tradizionale quadro giuridico, ci sono due ragioni principali per cui i robot sollevano nuovi problemi, il che implica che non dovrebbero essere considerati semplici "tostapane potenziati":

1. Questi artefatti sono (e saranno sempre più) in grado di apprendere le caratteristiche del loro ambiente circostante e degli esseri viventi che lo abitano, acquisendo al contempo conoscenze o abilità dal proprio comportamento. Questa capacità significa che i robot non saranno solo imprevedibili per i loro utenti ma anche per i loro progettisti umani.
   "Quindi, senza necessariamente immaginare alcuni scenari di fantascienza in cui i robot sono dotati di coscienza, libero arbitrio ed emozioni, tra qualche anno conviveremo con robot dotati di conoscenza di sé e autonomia, nel significato ingegneristico di queste parole."
2. È probabile che robot autonomi creino nuove forme di agenzia legale, vale a dire il rapporto con cui una parte concede l'autorità a un'altra per agire per suo conto in modo da trattare con una terza parte. '' Di conseguenza, la responsabilità legale per le azioni di un robot ricade sull'individuo che concede al robot il permesso di agire per suo conto. (...)".
   "Tale legge potrebbe tuttavia comportare un onere troppo pesante per i proprietari di robot, impedendo l'adozione di robot a causa del rischio o proteggendo ingiustamente i produttori che potrebbero condividere la responsabilità di comportamenti scorretti dei robot a causa di progetti inadeguati ''.

Un ulteriore passo avanti nella robotica legale: Prendendo sul serio l'autonomia degli agenti artificiali, alcuni studiosi hanno proposto un suggestivo parallelismo tra robot e schiavi nella misura in cui i giuristi dell'antica Roma avrebbero anticipato molte delle questioni odierne che coinvolgono agenti e robot artificiali, "definendo un quadro giuridico avanzato per coprire diritti e doveri derivanti dalla proprietà degli schiavi".

Ciò non significa, ovviamente, che dovremmo trattare gli attuali agenti artificiali o i robot intelligenti di domani come se fossero i nostri schiavi moderni. Anche se rifiutiamo l'idea che i robot rappresentino una nuova fonte di agenzia morale, i sistemi legali prevedono una serie di sanzioni in caso di abuso intenzionale di potere, atti vandalici, ecc., In modo che i robot, come oggetti informativi , potrebbero essere correttamente considerati i pazienti morali che meritano rispetto e protezione in quanto tali.

Il male appare "come" tutto ciò che danneggia o impoverisce "la natura informativa dell'universo" (cit. Terrell Bynum). Pertanto, nelle ipotesi di umani che danneggiano o distruggono ingiustamente i propri compagni artificiali, possiamo prevedere forme di azione giudiziaria al fine di preservare la coerenza tra i robot e i loro proprietari.

Il parallelismo tra robot e schiavi getta luce su altri due campi del futuro prevedibile della robotica legale:

1. Dobbiamo esaminare in che modo la legge può far fronte sia all'applicazione dei diritti e degli obblighi creati dai robot, sia alla questione della responsabilità per danni causati da essi.
2. Dobbiamo ampliare la nostra prospettiva in modo da tener conto della possibilità stessa che i robot rappresenteranno presto una nuova fonte di responsabilità personale per il comportamento degli altri.

Argomento 6:

Giustizia giurimetrica (jurimetric → giurisprudenza): La giurisprudenza si muove attraverso due approcci:

- Comportamento sociologico basato su una serie di fattori che riflettono i fatti o le circostanze del caso.
- Comportamento delle parti.

Decisioni precedenti: L'idea di base è una forma di sguardo deciso. Si presume che il giudice, a breve termine, sia coerente con sé stesso in modo da consentirgli di prevedere il suo comportamento futuro a partire dalle decisioni precedenti.

Tipi di giudizio (judgments): Sono stati suggeriti due tipi di tecniche di previsione del giudizio basate sugli elementi esplicativi delle decisioni:

1. *Micro-descrittori: sono fatti molto specifici che possono essere estratti dalle opinioni giudiziarie stesse o da fattori derivati da teorie sociologiche o politiche, ovvero elementi come essere neri o procedere contro uno stato degli Stati Uniti del sud nelle decisioni sulle libertà pubbliche o in procedimenti penali.*
2. *Approccio è quello formalista: è orientato all'uso di linguaggi logico-formali per la legge. Innanzitutto, per scoprire ambiguità, antinomie e contraddizioni, per migliorare la comunicazione e l'espressione della legge.*

Tutto per rappresentare le dichiarazioni normative in una forma logica in modo da costruire sistemi esperti che potrebbero facilmente applicare il sillogismo aristotelico. I due approcci daranno vita alle due tendenze nella costruzione di sistemi esperti:

- Logico - Deduttivo
- Empirico - Casuistico.

Logico – Deduttivo (Logic symbolic algorithmic justice): Negli anni '80 sviluppa la giustizia algoritmica simbolica con sistemi di intelligenza artificiale basati su regole. Il modo decisionale logico del sistema giuridico dà vita allo sviluppo sfrenato verso sistemi esperti. Si pensava che evocasse Beccaria; sillogismo che, come allora, ha dovuto risolvere gran parte delle incertezze e della lentezza della giurisdizione.

Questi sistemi consistevano di tre componenti:

1. La ***base di conoscenza*** è il database di informazioni di cui il sistema ha bisogno per fornire una risposta a un determinato problema (così come l'essere umano con esperienza che ha la conoscenza specifica della materia da applicare per risolvere il problema). Questo è l'archivio in cui sono salvate (archiviate) informazioni e regole che consentono al sistema di implementare un argomento.
2. Il ***motore dell'inferenza (o inferenziale)*** è un insieme di regole logiche costituite da implicazioni se poi congiunzioni e disgiunzioni che, combinando le varie dichiarazioni di ragionamento, ci consentono di giungere a una conclusione.
3. L'***interfaccia utente*** infine consente all'utente di sfruttare il motore inferenziale attraverso un dialogo di domande e risposte più o meno amichevoli.

Il limite maggiore di questi sistemi: difficile rappresentare per mezzo di regole semantiche.
Questo limite semantico ha posto all'angolo sistemi deduttivi esperti che si rivelano essere "elefanti che danno alla luce topi".

Empirico – Casuistico (Casuistic symbolic algorithmic justice): Per superare i limiti dei sistemi simbolici basati su regole, specialmente nell'area anglosassone, vengono sviluppati sistemi in cui la conoscenza è rappresentata da strutture e reti semantiche e non da catene di inferenze logiche. I casi sono descritti con

insiemi di elementi considerati significativi e quindi confrontati. Quando le somiglianze superano le differenze, viene stabilita una somiglianza che può portare alla previsione di soluzioni simili.

Anche con questi metodi il problema dei sistemi esperti logico-simbolici non viene eliminato perché tutto dipende dalla determinazione degli elementi rappresentativi del caso, e determinare i molti elementi per confrontare e valutare il grado di somiglianza o differenza sono tipicamente operazioni semantiche.

Anche qui arriva l'interpretazione dei fatti: così come nel simbolico deduttivo era necessaria l'interpretazione delle affermazioni normative, nel simbolico casuistico si deve dare un significato preciso ai fatti.
I fatti, come le norme, non sono facilmente binarizzabili e riducibili a 0-1 (vero-falso).

Sia i sistemi procedurali deduttivi logici che i sistemi esperti basati su casi dichiarativi si sono pertanto dimostrati insufficienti a fornire i risultati sostenuti dai sostenitori dell'intelligenza artificiale.

Sia i sistemi esperti delle regole di produzione sia i ragionamenti basati su casi simbolici adottano il ragionamento simbolico.

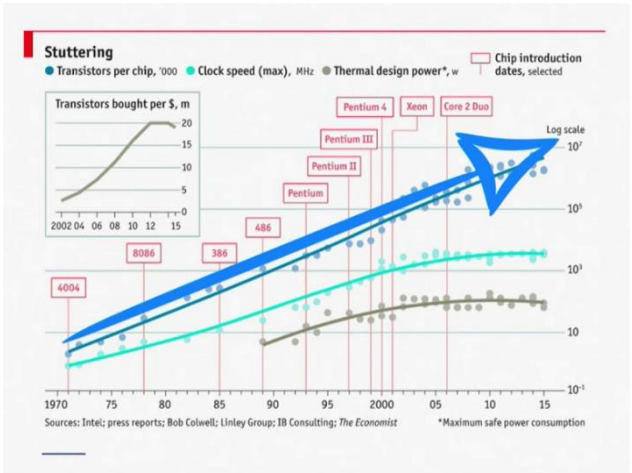
I sistemi esperti delle regole di produzione cercano di codificare la legge sotto forma di regole di logica. I ragionatori basati su casi simbolici codificano aspetti di casi, come gli attributi fattuali che poi subiscono trasformazioni e sono ragionati secondo regole esplicite. Un grave problema di giurisprudenza con il sistema di ragionamento simbolico è che dipende dalla conoscenza giuridica composta da regole esplicitamente dichiarate.

Infine, mentre i sistemi simbolici basati su regole logiche si sono rivelati totalmente inadatti a rappresentare il ragionamento legale, i sistemi simbolici basati su casi basati sulla ricerca di somiglianza di situazioni di fatto, aprono la strada alla cosiddetta tecnologia dell'intelligenza connessa.
Questa fase, chiamata sub-simbolica, si sviluppa in tre sottofasi: apprendimento debole o superficiale, forte o profondo e troppo forte o nero.

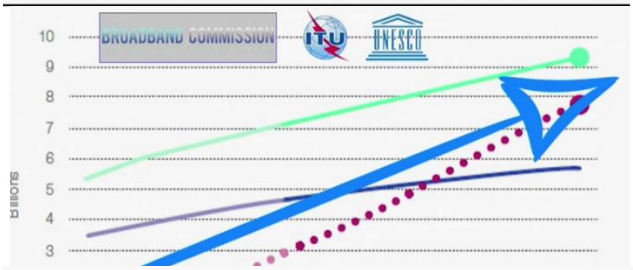
Argomento 7:

Quadro di rivoluzione digitale:

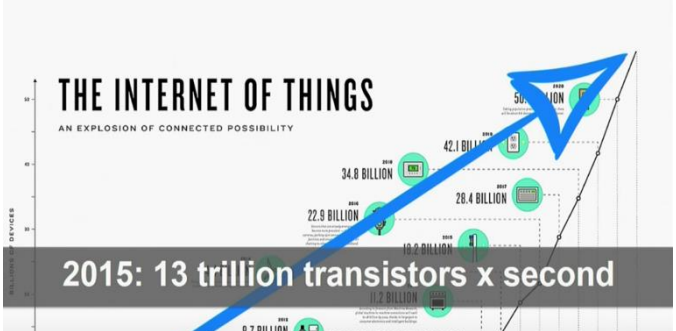
- Tendenza della potenza degli strumenti di calcolo dagli anni '70 ad oggi.
- La tecnologia informatica ha fornito una capacità di potenza incessantemente crescente, soprattutto dal 2000 in poi.



- Numero di utenti che si abbonano a Internet.
- Dal 2010 al 2020, il numero è in costante aumento, fino al punto in cui vi sono più abbonamenti rispetto agli utenti (oltre 8 miliardi di persone).

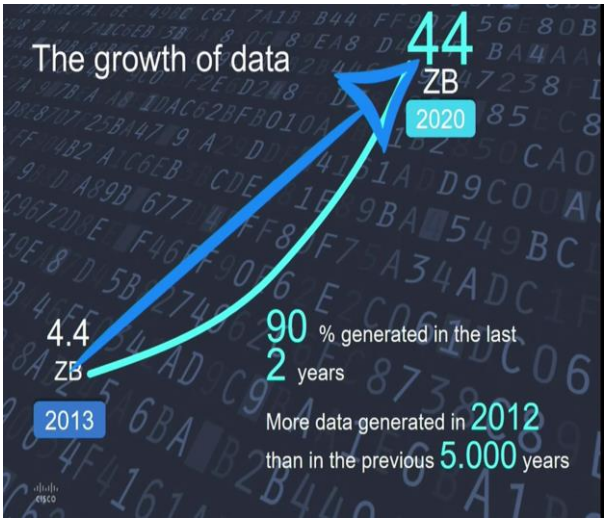


- Osserviamo che non è solo una questione di persone che comunicano: in effetti, abbiamo sviluppato reti in grado di



connettere "strumenti intelligenti".

- Produciamo 13 trilioni di transistor al secondo, mantenuti in un ambiente intelligente chiamato "Internet delle cose".
- Nel 2020, ci sono 50 miliardi di cose interconnesse (una media di 7 strumenti/tools a persona)



Big Data: I big data presentano diversi problemi da affrontare:

- Acquisizione / Conservazione
- Usabilità
- Sicurezza
- Analitica
- Legge / Etica
- Costi

Tempo: ITC (Tecnologia dell'informazione e delle comunicazioni) ha rivoluzionato le comunità umane nello spazio di alcuni decenni.

Stiamo vivendo un'era iperstorica → le società contemporanee non solo sono basate, ma dipendono completamente dalle tecnologie digitali (sensibilità alla criminalità informatica).

Spazio: L'infosfera è una dimensione creata dall'uomo, un "altro habitat" che al giorno d'oggi può essere considerato complementare alla biosfera: la sfera digitale e quella analogica coesistono e interagiscono. Non esiste più la condizione dicotomica di on-line / off-line → on-life.

Analogico → Digitale: Il passaggio dall'analogico al digitale comporta una trasformazione ontologica dell'identità umana e delle sue capacità.

Attraverso la tecnologia dell'informazione, la realtà è stata strutturata sempre più saldamente come risposta alle logiche basate sull'intelligenza artificiale e non all'intelligenza umana.

L'intelligenza artificiale non è l'unione tra l'artificialità dell'ingegneria e la capacità biologica di comprendere e creare connessioni, ma è la separazione tra la capacità di agire con successo per uno scopo e la necessità di essere intelligenti come un essere umano per farlo.

Da questa separazione nascono tutte le sfide dell'era contemporanea, specialmente nel sistema legale.

Perché un algoritmo non può sostituire un giudice? La giustizia è un sistema basato sulla ricerca del significato.

- L'ordinamento giuridico combina una gerarchia istituzionale con una logica delle regole tra loro.
- Questa logica delle regole tra loro porta alla causalità legale, il che significa che applichiamo le regole relative a tale principio o tale regola superiore.
- Quando la legge è limitata dalle regolarità osservate dai professionisti, l'idea stessa di una causalità legale scompare e rimangono solo i collegamenti tra parentesi. È, quindi, una scomparsa della distinzione tra legge e fatto.

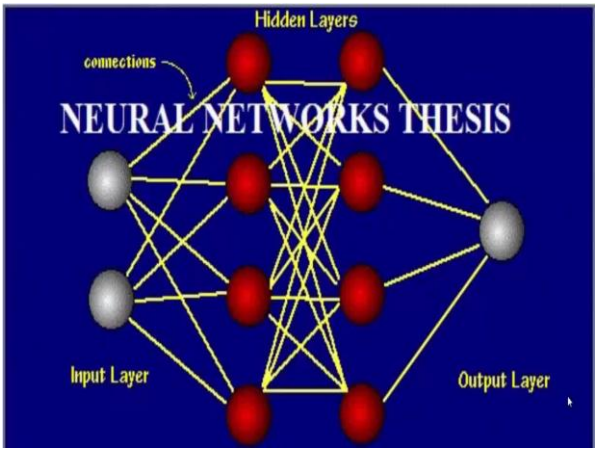
La giustizia predittiva è vera giustizia? La giustizia predittiva si basa sulla sostituzione della capacità di ragionamento (legale) con la capacità computazionale, non si nutre di conoscenze giuridiche ma di dati (cioè informazioni su casi simili) in cui queste conoscenze sono già state digerite e applicate.

Il momento più importante nella struttura legale è la parte ermeneutica, che può essere semplicemente realizzata dalla ragione umana, e si basa sulla capacità del giudice di valutare gli elementi prudenzialmente. In realtà, non è sostituibile da un dispositivo IA.

Argomento 8:

Rete neurale e apprendimento automatico (machine learning) (sub-simbolica / empirico-neurale giustizia algoritmica): Le reti neurali sono modelli di computer ispirati alla struttura dei sistemi neurali biologici. I neuroni sono collegati da assoni e dendriti. Un neurone riceve il segnale da altri neuroni attraverso i dendriti e invia il suo segnale ad altri neuroni attraverso i suoi assoni. Dove un dendrite si collega a un altro neurone c'è sinapsi. Sinapsi è di plastica, nel senso che la forza della loro connessione al neurone può aumentare o diminuire. Le reti neurali artificiali imitano questa struttura.

Secondo questa tecnologia, negli anni ’90 si sviluppa l'idea di utilizzare modelli neurali per riprodurre un ragionamento più simile a quelli che si sviluppano nel cervello umano. La rete neurale artificiale può essere definita come un sistema di elaborazione costituito da una serie di elementi di elaborazione semplici e altamente interconnessi, che elaborano le informazioni attraverso la loro risposta dinamica dello stato agli input esterni.



La rete neurale. I neuroni si trovano di solito in livelli, che possono essere di tre tipi:

1. *Livello di input (Input Layer)* per ricevere informazioni dall'esterno al fine di imparare a riconoscere ed elaborare le stesse informazioni ricevute.

2. *Livello nascosto (Hidden Layers)* che collegano il livello di input con il livello di output e aiutano la rete neurale ad apprendere le complesse relazioni analizzate dai dati. Spesso i livelli nascosti sono più di uno.
3. *Output Level (Output Layer)* che mostra il risultato di ciò che il programma è riuscito a imparare.

Le reti neurali sono programmate per apprendere usando un algoritmo chiamato Back-Reproduction (Back-Propagation). Prevede di confrontare il risultato ottenuto da una rete con l'output che si vuole effettivamente ottenere: utilizzando la differenza tra i due risultati, comporta la modifica dei pesi delle connessioni tra i livelli di rete a partire dal livello di output.

I sistemi neurali che danno vita alle macchine che apprendono (machine learning) suscitano l'interesse dei giuristi a cercare di superare i limiti dei sistemi simbolici logico-deduttivi e casuistici. Alla fine degli anni '80, iniziano a sperimentare in campo legale reti di classificazione neurale che apprendono con un singolo livello nascosto per consigli e previsioni (apprendimento automatico, definibile superficiale).

Va notato che quasi tutti questi esperimenti iniziali sono alimentati, almeno inizialmente, da insiemi di dati più o meno estesi forniti dai progettisti esperti. Il sistema si basa su giudizi ed elementi noti come variabili legali e fattuali. Solo pochi utilizzano già tecniche di apprendimento più complesse (deep learning), in particolare per il riconoscimento delle lingue.

Fine degli anni '90 → Passaggio dalle reti neurali a uno strato nascosto a reti neurali con più strati nascosti.

Coglierei quindi due periodi:

- Un periodo debole-pioneristico con sistemi con un singolo strato chiamato macchine per l'apprendimento superficiale (*shallow-learning*) .
- Un periodo difficile con sistemi in cui gli strati diventano più numerosi di quelli chiamato macchine per l'apprendimento profondo (*deep learning*).

Machine learning: Attualmente stiamo vivendo un terzo periodo con l'apprendimento genetico automatico in cui i dati di partenza sono oscuri e il meccanismo di apprendimento (apprendimento automatico in black box) è oscurato.

Periodo di apprendimento superficiale (Shallow-Learning; anni '80 e '90): Il primo periodo vede gli esperimenti concentrarsi sul ragionamento con casi per classificare i modelli e quindi imitare il ragionamento analogico, per risolvere la trama aperta dei problemi, affrontare difficili problemi di ragionamento con norme giuridiche contrastanti e mantenere aggiornato la conoscenza del sistema.

L'atto di furto (The Theft Act): La maggiore omogeneità tra legge comune (common law) e tecnica neurale favorisce lo sviluppo della giustizia algoritmica neurale nell'area anglosassone piuttosto che nel mondo del diritto civile. Un uso della rete neurale per imitare l'aspetto analogico del ragionamento è un indice del Theft Act del 1968. In questo indice una situazione di fatto viene analizzata dai ricercatori per la presenza o l'assenza di vari concetti, i concetti specificati dal testo della legge.

Il progetto diviso (The Split Up Project): Notevole è il progetto PROLEXS che utilizza tecniche basate sui dati forniti dalla progettazione e sui dati ottenuti dalla sua formazione. Tra le previsioni significative vi è il progetto Split Up, sviluppato nel 1991 dall'Università La Trobe di Melbourne, per creare un sistema di attuazione di tale disciplina sulla condivisione della proprietà dei coniugi dopo lo scioglimento del matrimonio, come richiesto dall'Australian Family Act.

Nell'ambito del diritto civile vengono sviluppati progetti neurali per gestire i conflitti sia per giungere a una composizione sia per consigliare la scelta tra ipotesi contrastanti. Significativo è ECHO, come modello di sistema in competizione con le teorie che usano la rete neurale usando il ragionamento abduttivo.

Il progetto MAIRILOG: Il progetto MAIRILOG utilizza le reti neurali per trarre regole logiche dai casi.

C'è anche progetto predittivo tedesco sul danno immateriale in cui l'organismo legale di base era composto da 200 sentenze del tribunale tedesco e le variabili erano il tipo, la gravità e la durata dell'incidente, la gravità e la durata delle conseguenze, il sesso, la disabilità rispetto a lavoro, gravità particolare, responsabilità medica per colpa. Inizialmente l'apprendimento è un meccanismo di feed forward ('alimentare', 'inoltrare') che in caso di errori non è in grado di riconfigurarsi.

I limiti di questo primo esperimento vengono superati con una rete a tre livelli che minimizza gli errori (regola delta).

Il primo progetto è un apprendimento superficiale, il secondo è un apprendimento profondo.

Nel primo periodo appartiene un progetto italiano che analizza le decisioni della Corte di cassazione per stabilire la responsabilità dei veicoli a motore. A partire dalla metà degli anni 2000, nascono reti neurali di apprendimento profondo, costituite da almeno 2 livelli nascosti. In realtà, le applicazioni di Deep Learning contengono molti più livelli (ad esempio 10 o 20 livelli nascosti).

Lo sviluppo del Deep Learning in questo periodo dipendeva sicuramente dall'aumento esponenziale dei dati (big data): maggiore è la quantità di dati che possono essere analizzati dal software, maggiore è il livello di apprendimento → prestazioni maggiori rispetto agli algoritmi precedenti.

L'aumento delle prestazioni del computer: ha migliorato i risultati ottenuti e ridotto significativamente i tempi di calcolo.

Argomento 9: VEDI ARGOMENTO 2.

Argomento 10: VEDI DA ARGOMENTO 21 IN POI.

Argomento 11:

Periodo di apprendimento profondo (deep-learning): Un secondo periodo di esperimenti inizia a combinare tecniche di apprendimento superficiale con tecniche di apprendimento profondo sia per fornire consulenza sia per prevedere le decisioni.

Tra i sistemi di consulenza sottolineo che l'IBM Ross è in grado di svolgere accurate ricerche legali, fornire pareri anche se il cliente non riesce a fornire una descrizione precisa del caso in questione e a ritirare contratti, statuti aziendali, testamenti e registri privati.

(Viene utilizzato il sistema di elaborazione del linguaggio Watson che tenta di superare il limite semantico di IA.)

Altri recenti progetti di reti neurali per risolvere i problemi legali sono il ADJUSTED WINNER, un algoritmo per dividere i beni divisibili tra due parti il più equamente possibile e il CLAUDETTE per il diritto dell'UE che analizza le clausole dei contratti firmati online per identificare "l'ingiustizia". Utilizzando il metodo Bag-of-Words (Borsa-di-parole).

Tra i sistemi predittori, spiccano due esperimenti italiani:

- Uno progetto realizzato presso l'Università di Trento di una rete neurale dotata di variabili iniziali per calcolare l'indennità di mantenimento nella separazione dei coniugi.
- Un progetto realizzato presso la LUISS per realizzare una rete neurale in grado di riprodurre il ragionamento fatto dalla magistratura nelle controversie, correlato all'infiltrazione di acqua da marciapiedi o terrazze solari utilizzati da un condominio.

Le disposizioni combinate dell'art. 1126 e 2051 del Codice civile italiano stabilisce che il condominio è tenuto a risarcire i 2/3 dei danni, mentre il proprietario della pavimentazione rimborsa 1/3 e può liberarsi della responsabilità solo se tenta il caso fortuito.

Alla rete di formazione sono state fornite 9 variabili di input e 30 sentenze definitive della Corte di cassazione e della corte d'appello.
Dopo l'allenamento, 15 nuovi casi vengono forniti alla rete neurale per decidere.
I risultati sono molto soddisfacenti e mostrano che il sistema neurale ha imparato a decidere in modo tendenzialmente corretto. Ma è nell'area anglosassone che i sistemi predittivi sono più diffusi.

Caso CRUNCH: Un sistema neurale che tenta di prevedere l'esito delle decisioni in Gran Bretagna. Ha partecipato a un concorso con un centinaio di avvocati per quanto riguarda la previsione di circa 750 decisioni. Mentre gli avvocati hanno previsto correttamente l'esito del 62% delle controversie, il sistema di intelligenza artificiale neurale ha raggiunto l'86%.

Un altro algoritmo predittivo è quello sviluppato dall'University College di Londra e dall'Università di Sheffield, che è in grado di prevedere i verdetti della Corte europea dei diritti dell'uomo.

I recenti progressi nell'elaborazione del linguaggio naturale e l'apprendimento automatico forniscono gli strumenti per costruire modelli predittivi che possono essere utilizzati per svelare schemi che guidano le decisioni giudiziarie.

Questo può essere utile, sia per gli avvocati che per i giudici, come strumento di assistenza per identificare rapidamente i casi ed estrarre schemi che portano a determinate decisioni. Questo documento presenta il primo studio sistematico sulla previsione dell'esito del caso archiviato dalla Corte europea dei diritti dell'uomo basato esclusivamente sul contenuto testuale.

Classificazione binaria: Formuliamo un'attività di classificazione binaria in cui l'input dei nostri classificatori è il contenuto testuale estratto da un caso e l'output di destinazione è il giudizio effettivo sul fatto che vi sia stata una violazione di un articolo della convenzione sui diritti umani. Le informazioni testuali sono rappresentate usando sequenze di parole contigue, ovvero N-grammi e argomenti.

I nostri modelli possono prevedere le decisioni del tribunale con una forte precisione (79% in media).

La nostra analisi empirica indica che i fatti formali di un caso sono la previsione più importante.

Sottolineo infine alcuni sistemi algoritmici americani in materia penale basati su irrazionali e piccoli fattori giuridici. Uno più vecchio e uno più recente:

- Il primo aveva lo scopo di prevedere quali condanne a morte sarebbero state eseguite.
  I risultati sono nel senso che i meno abbienti e appartenenti a gruppi etnici afroamericani, asiatici e latinoamericani sono più frequentemente soggetti alla pena capitale.
- Il secondo è la profilazione gestionale correttiva di Compass (Compass Correctional Offender Management Profiling) per sanzioni alternative (Alternative Sanctions), un algoritmo predittivo per la valutazione del rischio di ricorrenza.
  Nel febbraio 2013 un cittadino americano è stato arrestato per due reati che potremmo qualificare in Italia come ricevere (un'auto) e resistenza a un pubblico ufficiale. Per questi fatti è stato condannato a una pena detentiva di sei anni, una pena particolarmente grave determinata sulla base del punteggio elevato (punteggio) a sue spese da COMPAS.
  Il cittadino ha contestato il giudizio del tribunale distrettuale sostenendo che l'uso da parte del giudice di primo grado di un algoritmo predittivo per raggiungere la sentenza aveva violato le garanzie del giusto processo (diritto a un giusto processo) in quanto COMPAS è un algoritmo proprietario, il cui meccanismo di funzionamento - che si basa sulla raccolta e l'elaborazione dei dati

emersi dal fascicolo di prova e sull'esito di un test di 137 domande a cui l'imputato è soggetto per quanto riguarda l'età, il lavoro, la vita sociale, il grado di istruzione, i legami, l'uso di droghe, opinioni personali e procedimenti penali - non è noto pubblicamente e quindi la sua validità scientifica non può essere accertata.

La corte suprema del Wisconsin: Dichiarandosi in appello, all'unanimità ha dichiarato la legittimità dell'uso giudiziario di algoritmi che misurano il rischio di recidiva, specificando, tuttavia, che lo strumento non può essere l'unico elemento su cui una dichiarazione di condanna "... mentre la nostra partecipazione oggi consente un tribunale conduttore per considerare COMPAS, non concludiamo che un sentimento giudiziario possa fare affidamento su COMPAS per la sentenza che impone".

Risulta quindi che il risultato dell'algoritmo può essere un sussidio per la decisione ma non l'elemento decisivo. Naturalmente la forza semplificatrice degli algoritmi potrebbe influenzare notevolmente il giudizio dei giudici.

Argomento 12:

Robot e obblighi contrattuali: Il primo motivo per confrontare lo status dei robot con quello degli schiavi nell'antica Roma è che gli schiavi erano considerati "cose" che, tuttavia, svolgevano un ruolo cruciale nel commercio e nel commercio.

L'élite, come nel caso paradigmatico degli schiavi dell'imperatore, era gestori immobiliari, banchieri e commercianti. Avevano la capacità legale di stipulare contratti vincolanti, di rappresentare i loro padroni, di svolgere lavori importanti come dipendenti pubblici o per l'azienda di famiglia dei loro padroni, di accumulare, gestire e utilizzare la proprietà.

Sebbene la maggior parte degli schiavi non avesse certamente alcun diritto di rivendicare contro i propri padroni, alcuni schiavi godettero di una significativa "autonomia" (Serman e Trofimova 1975, 53).

Di conseguenza, considerando come gli agenti artificiali di oggi negoziano, stipulano contratti, stabiliscono diritti e doveri tra umani, ***c'è qualcosa che possiamo imparare dall'antica legge romana?***

Da questo punto di vista, uno dei meccanismi più interessanti previsti dalla legge romana è il "peculium".

Nel fraseggio del Digesto di Giustiniano, è *"la somma di denaro o proprietà concessa dal capofamiglia a uno schiavo o al figlio al potere.*
Sebbene considerato per alcuni scopi come un'unità separata, e quindi consentendo a un'azienda gestita da schiavi di essere utilizzata quasi come una società a responsabilità limitata, è rimasta tecnicamente di proprietà del capofamiglia." (Watson 1988).

Come una specie di società a responsabilità limitata, il peculium puntava a trovare un equilibrio tra la pretesa dei padroni di non essere rovinati dalle attività commerciali dei loro schiavi e l'interesse delle controparti degli schiavi a effettuare transazioni sicure con loro.

Mentre, la maggior parte delle volte, la responsabilità dei padroni era limitata al valore stesso del peculium dei loro schiavi, la sicurezza legale di quest'ultimi (queste controparti) garantiva alle controparti degli schiavi che gli obblighi sarebbero stati rispettati. Pertanto, a seconda del tipo di attività e dello stato degli schiavi come dispensatori, ordinari, ecc. (Per la lunga lista vedi Sermantaerman e Trofimova 1975, 82), c'erano diversi tipi di azioni legali o azioni: esercitoria, institoria, tributaria, ecc.

Alcuni studiosi (Katz 2008) hanno quindi suggerito di applicare questo vecchio meccanismo alle transazioni contemporanee mediate da agenti artificiali e dai robot intelligenti di domani.

Data la crescente estensione della loro autonomia, un nuovo tipo di peculium potrebbe infatti rappresentare il modo giusto di avvicinarsi e bilanciare i diversi interessi umani coinvolti.

Considerando che, impiegando robot o agenti artificiali per fare affari, transazioni o contratti, le persone potrebbero rivendicare una responsabilità limitata, il peculium dei robot garantirebbe alle loro controparti umane, o altri robot, che gli obblighi sarebbero realmente rispettati.

Rispetto ad altri agenti artificiali e al tipico problema dell'anonimato su Internet, la maggior parte delle interazioni con i robot avrà il vantaggio di evitare un problema così duro di anonimato, in quanto le transazioni, i contratti e le imprese saranno spesso nel 'mondo reale.'

Ciò non significa, ovviamente, che non avremo bisogno di modelli di business come sono stati proposti nel caso di agenti artificiali: basti ricordare il modello assicurativo illustrato da Curtis Karnow (1996), il modello di autenticazione di Andrew Katz (2008).

I robot solleveranno effettivamente problemi di:

- Fiducia (Trustfulness)
- Affidabilità
- Tracciabilità

Tuttavia, da un punto di vista legale, non dovremmo perdere il punto cruciale: l'idea stessa del peculium (peculio) e il parallelismo tra robot e schiavi è così attraente, mostrano un modo valido per prevenire qualsiasi legislazione che potrebbe impedire l'uso di robot a causa dei loro rischi e del conseguente onere eccessivo per i proprietari (piuttosto che, per esempio, per i produttori e i progettisti) dei robot.

Individuando un equilibrio tra la pretesa della gente di non essere fatiscente dalle attività dei suoi robot e l'interesse delle controparti dei robot da proteggere durante le transazioni con loro, una forma aggiornata di peculium sembra particolarmente interessante al fine di affrontare una nuova generazione di obblighi contrattuali e anche una nuova fonte di agenzia.

(Responsabilità limitata per i proprietari di robot.)

Indipendentemente dal fatto che tu sia pronto ad ammettere che i robot sarebbero "persone giuridiche" (Solum 1992; Teubner 2007), il pragmatismo caratteristico dei giuristi dell'antica Roma indica come ottenere entrambe le forme di responsabilità limitata per i proprietari di robot e di garanzia commerciale per le controparti dei robot.

Robot e obblighi extracontrattuali: La robotica legale non riguarda solo l'applicazione dei diritti e degli obblighi creati dall'attività dei robot, poiché i robot sollevano anche problemi di responsabilità extracontrattuale per i danni causati da essi.

Questo scenario trascende il meccanismo del peculium e coinvolge ciò che i giuristi romani definirono in termini di protezione aquiliana (Zimmermann 1988, 1017); vale a dire, la forma di responsabilità che deriva dall'idea generale che le persone siano ritenute responsabili per danni illeciti o accidentali causati ad altri a causa di colpa personale: Alterum non laedere (Pagallo 2009).

Tuttavia, come sottolineato nella sezione precedente, questo tipo di responsabilità extracontrattuale comprende forme specifiche di "tipi di responsabilità rigorosa" che corrispondono all'idea di: "Responsabilità oggettiva" o responsabilità senza colpa nella tradizione di diritto civile.

Indipendentemente da qualsiasi comportamento illecito o colpevole, in altre parole, le persone sono ritenute responsabili sia per i danni causati dalle proprie attività pericolose, come nel caso di alcuni tipi di "responsabilità del prodotto", sia per i danni causati dai propri figli, animali e persino impiegati.

Considerando che i robot sono interattivi, autonomi e adattabili, avremo quindi bisogno di un nuovo tipo di responsabilità legale per il comportamento degli altri: se il meccanismo di peculium può garantire una forma di responsabilità legale per ciò che i robot fanno nel campo degli obblighi contrattuali, è probabile che avremo

un nuovo tipo di responsabilità senza colpa per le conseguenze del comportamento dei robot nell'ambito degli obblighi extracontrattuali.

Al fine di illustrare come tale responsabilità può essere costruita, è importante capire come viene assegnato l'onere della prova in questi casi.

Argomento 13:

Robot e obblighi extracontrattuali: A volte, la legge impone la responsabilità indipendentemente dall'intenzione del soggetto o dal suo uso delle cure ordinarie.

I datori di lavoro, ad esempio, sono spesso ritenuti responsabili per qualsiasi azione illecita che i dipendenti intraprendono nell'ambito delle loro attività di contratto di lavoro.

Nel caso dei robot, tale politica potrebbe ovviamente essere attenuata in modo da prevenire il rischio che le persone pensino due volte prima di utilizzare o impiegare robot.

- ***Assicurazione per robot?*** Potremmo forse rendere obbligatoria l'assicurazione come abbiamo fatto nella maggior parte dei sistemi legali con le automobili.

Potremmo anche estendere il meccanismo del peculium determinando che la responsabilità extracontrattuale umana dovrebbe essere limitata al valore del portafoglio dei propri robot (più, eventualmente, l'assicurazione obbligatoria di cui sopra).

Comunque, i sistemi legali prevedono anche limiti a tale responsabilità senza colpa. Questo è ciò che accade in genere ai genitori che sfuggono alla responsabilità del comportamento dei loro figli quando dimostrano di non poter impedire le loro azioni.

Questo è anche ciò che accade ai proprietari di animali quando dimostrano che si è verificato un evento fortuito. Mentre per quanto riguarda l'insieme di attività pericolose, alcuni sistemi legali escludono la responsabilità quando è dimostrato che hai adottato tutte le "misure appropriate" al fine di prevenire qualsiasi tipo di danno, possiamo indovinare quale tipo di responsabilità limitata si adatta ai nostri robot.

Una volta che siamo d'accordo che non sono né assassini né semplici frigoriferi, ***il comportamento dei nostri schiavi moderni dovrebbe essere legalmente assimilato alle azioni dei nostri figli?***

In alternativa, ***dovremmo supporre che il comportamento dei robot sia ontologicamente o intrinsecamente pericoloso?*** Oppure, come afferma David McFarland (2008), ***dovremmo confrontare il comportamento dei robot con le azioni dei nostri animali domestici?***

Conclusioni: È improbabile che ci imbattiamo in un'unica metafora per cogliere la prossima generazione di questioni legali relative ai robot nel regno degli obblighi extracontrattuali.

È plausibile che tale responsabilità varierà a seconda della diversa tipologia di robot cui ci troviamo di fronte. In alcuni casi, si tratterà di prevenire le azioni dei robot (robot da bambini); in altri, dovremmo dimostrare che si è verificato un evento fortuito (robot come animali domestici).

Quindi, quando si discute di forme di responsabilità senza colpa, dovremo decidere se la responsabilità umana debba essere limitata al valore del peculium dei robot e all'importo della loro possibile assicurazione obbligatoria (robot come dipendenti).

In ogni caso, gli avvocati dovranno presto risolvere un nuovo tipo di responsabilità extracontrattuale per le azioni altrui perché i robot rappresentano un passo decisivo in una nuova generazione di casi che coinvolgono la responsabilità degli agenti artificiali. Come loro controparti umane, i robot agiscono pienamente come sistemi di transizione di stato: la responsabilità degli agenti artificiali.

Non interagiscono solo tra loro e con il loro ambiente nella misura in cui possono cambiare le loro proprietà e stati interiori, senza che tale cambiamento sia una risposta diretta all'interazione. Anche se non hanno alcuna responsabilità morale (poiché i robot non possono essere assassini), a volte sono responsabili (perché i robot possono davvero essere cattivi frigoriferi).

I robot saranno sempre più la fonte di azioni malvagie o buone e saremo costretti a riflettere sulla possibilità di concepirli come legalmente responsabili di ciò che fanno con il peculio dei loro proprietari (robot come schiavi).

Pertanto, insieme a una serie specifica di obblighi contrattuali, dovremo affrontare due tipi di nuove responsabilità.

- Da un lato, avremo una nuova *responsabilità morale* perché i robot sono agenti che migliorano la natura informativa dell'universo.
  Poiché "bene" o "male" possono essere convenientemente rappresentati come qualsiasi cosa che possa migliorare o danneggiare la complessità informativa dell'insieme, dovremmo preservare, coltivare e arricchire le proprietà dei nostri robot perché sono oggetti informativi per eccellenza.
  Non è improbabile, su questa base, che possano essere previste nuove forme di azione giudiziaria contro gli umani per evitare che i proprietari danneggino o reprimano ingiustamente i loro robot (Pagallo 2010).
- D'altra parte, la *responsabilità legale* dovrà essere ulteriormente estesa: oltre agli obblighi contrattuali e ai casi di responsabilità senza colpa che coinvolgono animali ed esseri umani, saremo responsabili di ciò che alcuni agenti artificiali fanno autonomamente. La necessità di introdurre un nuovo tipo di protezione extracontrattuale dipende dal fatto che i robot agiscono: indipendentemente dal fatto che siano "realmente" coscienti, "meccanicamente" coscienti (Aleksander e Dunmall 2003) o "fenomenologicamente" coscienti (Franklin 2003).

I robot sono in grado di acquisire conoscenze dal proprio comportamento, diventando così imprevedibili. Considerando che valuteremo le loro azioni in termini di possibili danni e danni, è altamente probabile che il punto legale chiave in settori come la robotica correlata all'edutainment, l'assistenza sanitaria o le applicazioni di qualità della vita riguarderà il modo in cui educhiamo, trattiamo o gestiamo i nostri robot .

Come accade per i bambini e gli animali domestici, questo tipo di obbligo extracontrattuale non esclude l'autonomia dei robot poiché manterranno una certa sfera di libertà compatibile con la responsabilità legale dei proprietari. La novità di questo tipo di responsabilità senza colpa è che, molto presto, includerà la responsabilità legale di ciò che un sistema di transizione di stato artificiale sceglie di fare!

Argomento 14: GUARDA ARGOMENTO 4

Argomento 15: VIDEO NON DISPONIBILE

Argomento 16:

Periodo di giustizia algoritmica evolutiva (evlutionary algorithmic justice): Un'altra frontiera algoritmica è quella genetica o evolutiva. Oggi riguarda principalmente la questione della responsabilità dei robot.

Qual è la differenza tra algoritmi neurali classici e algoritmi neurali evolutivi?

- Il primo sono i tentativi di emulare il funzionamento della rete neurale in un sistema vivente, il processo di memorizzazione delle informazioni modifica il sistema stesso e quindi non è possibile accedere ai dati in un secondo momento.
- Il secondo invece comporta un livello molto elevato di auto-modifica del sistema.
  Questo, creato per svolgere un determinato compito, è il prodotto di un processo ripetuto di riproduzione selettiva, mutazione casuale e ricombinazione genetica.
  (Qui) Invece di programmare un'intelligenza artificiale di sistema con istruzioni dettagliate su come completare un'attività specifica.

Ontologia della giustizia algoritmica: Le caratteristiche essenziali della giustizia algoritmica sono la valutazione quantitativa non qualitativa, l'uso probabilmente illegittimo, la comprensione non semantica della logica morfo-sintattica e l'intelletto inconsapevole.

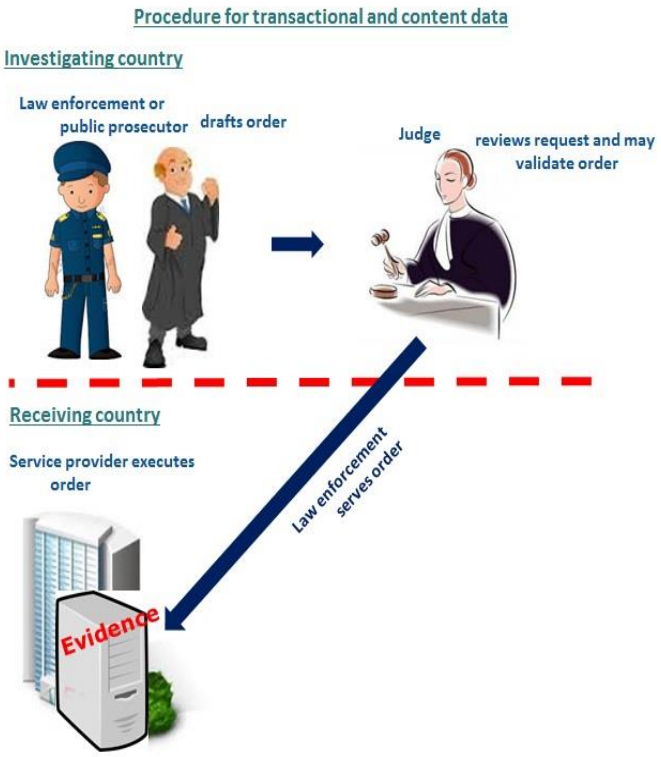
Da notare che quasi tutti i sistemi neurali meno oscuri non sono indeterminati ma si basano su elementi di input forniti dal giurista o programmatore esperto.

Anche l'approccio neurale, basato sull'apprendimento a posteriori a differenza dell'apprendimento a priori dell'approccio logico, incontra difficoltà nella fase iniziale simili a quelle incontrate dai sistemi esperti.

I dati di input che devono aumentare il primo strato della rete neurale devono essere calcolabili e quindi enumerabili, come sottolineato da Paolo Zellini.

È necessario ridurre le qualità a quantità anche se flessibile (scala di peso). Quindi questi dati devono essere derivati da una serie di situazioni che a volte sono difficili da identificare completamente.

La vera novità delle reti neurali consiste nel fatto che una volta che avranno imparato a imparare su una serie di casi x saranno in grado di eseguire lo stesso metodo anche su casi diversi e più numerosi.



I sistemi criminali americani ci costringono a riflettere sul loro rapporto con i diritti fondamentali. Gli algoritmi basati sui dati forniti dall'esperto umano (avvocato, programmatore) presentano dubbi sulla legittimità costituzionale, specialmente se considerati decisivi per le decisioni legali.

Un'ulteriore riflessione generale dobbiamo fare sulla di

- processo e processo semplicemente automatico;
- vera intelligenza artificiale.

Penso che questo limite sia molto debole e che tendiamo a considerare processi intelligenti che non sono intelligenti e viceversa.

A livello di legalità, forse alcuni processi considerati solo automatici senza intelligenza potrebbero invece nascondere aspetti dell'illegittimità in quanto privi di motivazione?

L'algoritmo è, come il computer, un meccanismo morfo-sintattico che riconosce solo sequenze di significanti e non capisce il significato.

Perfino l'algoritmo genetico, sebbene appaiamente omogeneo con l'intelligenza naturale, calcola i processi casuali non logici ma non si rende conto di calcolare, non pensa a sé stesso.

Dov'è la giustizia digitale? Il potere pubblico deve rimanere al centro della protezione e del controllo e deve trovare le forme di regolamentazione per garantire i diritti delle persone al fine di impedire l'imposizione delle regole del mercato ICT.

In effetti, oggi studiamo i casi di giustizia predittiva per capire se ci sono violazioni dei diritti umani, ma siamo convinti che la giustizia digitale sia già regolata in alcuni sistemi legali violi e comprenda molti diritti.

In ogni caso per la cosiddetta giustizia predittiva come per la giustizia digitale, non dobbiamo dimenticare che le nostre società (e i nostri legislatori) cercano nelle macchine un elemento di certezza non controverso. Ma le macchine non sono in grado di dare certezza.

Soprattutto in alcune aree del diritto sono i sistemi legali che non possono accettare, perché il ruolo del decisore è ancora centrale (come nelle decisioni giudiziarie), limitato da molte regole di procedura e di responsabilità.

Le norme proteggono le persone e i loro diritti da disparità di trattamento o misure sproporzionate.

Ciò si applica in generale a tutti i servizi pubblici e privati di Internet, anche se oggi gli Stati e i legislatori sono troppo timidi con gli operatori di Internet, in particolare dei PTOM (paesi e territori d'oltremare, OCT), che limitano alcuni diritti delle persone (p.s. diritto alla privacy, segretezza, informazione).

Siamo paradossali: Mark Zuckerberg, CEO di Facebook, ha recentemente scritto:

“Internet ha bisogno di nuove regole. Credo che abbiamo bisogno di un ruolo più attivo per i governi e le autorità di regolamentazione. Aggiornando le regole per Internet, possiamo preservare ciò che è meglio al riguardo: la libertà delle persone di esprimersi e degli imprenditori di costruire nuove cose - proteggendo al contempo la società da danni più ampi. Da quello che ho imparato, credo che abbiamo bisogno di una nuova regolamentazione in quattro aree: contenuto dannoso, integrità elettorale, privacy e portabilità dei dati.”

In realtà da molti anni abbiamo parlato dell'importanza delle regole pubbliche per la trasparenza nella società dell'informazione "verso una società intelligibile" (Pasquale, 2015, 189 ss).

Argomento 17:

Giustizia e rispetto per la diversità: La svolta digitale sta influenzando le relazioni umane?

- ***Cos’è il rispetto?*** Letteralmente, rispetto significa "guardare indietro". Sta per considerazione e cautela [Rücksicht].
  L'interazione rispettosa con gli altri comporta l'astenersi da uno sguardo curioso. Il rispetto presuppone uno sguardo distante: il pathos della distanza. Oggi ci si sta arrendendo allo sguardo invadente dello spettacolo.
  Il verbo latino spectare, da cui deriva lo spettacolo, è uno sguardo voyeuristico privo di considerazione riguardosa, cioè rispetto.
  La distanza è ciò che rende il rispetto diverso dallo spettacolo. Una società senza rispetto, senza il pathos della distanza, apre la strada alla società dello scandalo.

Distanza e rispetto sono collegati: Il rispetto costituisce la base per la sfera pubblica o civile. Quando il primo si indebolisce, il secondo collassa.

Il declino della società civile e una crescente mancanza di rispetto si condizionano a vicenda. Tra le altre cose, la società civile richiede di distogliere rispettosamente lo sguardo da ciò che è privato. Prendere la distanza è ciò che costituisce la sfera pubblica.

Oggi prevale una completa mancanza di distanza e rispetto: le cose intime sono messe in mostra e il privato è reso pubblico.

Senza distanza, è impossibile essere in regola.

La comunicazione digitale sta abolendo le distanze. Il corollario della diminuzione della distanza spaziale è l'erosione della distanza mentale.

Isolamento e vicinanza irrispettosa: La medialità digitale funziona a scapito del rispetto.

Al contrario, isolare e separare - come nell'adyton (la parte dei templi greci completamente chiusa all'esterno) - genera ammirazione e riverenza.

Lo spazio ibrido dell'infosfera: Quando la distanza risulta carente, il pubblico e il privato si confondono.

La comunicazione digitale sta promuovendo questa dimostrazione pornografica dell'intimità e della sfera privata. I social network finiscono per essere sale espositive per questioni altamente personali.

Pertanto, il mezzo digitale privatizza la comunicazione spostando il sito in cui vengono prodotte le informazioni. “La sfera privata è quella zona dello spazio, del tempo, in cui non sono un'immagine, un oggetto” (*Roland Barthes) .*

In questo senso, non abbiamo più alcuna sfera privata: non esiste alcuna zona in cui non sono un'immagine, in cui nessuna fotocamera è in funzione. Google Glass trasforma persino l'occhio umano in una fotocamera. L'occhio stesso genera immagini. Di conseguenza, la sfera privata non può reggere. L'icono-pornografia compulsiva la sta abolendo del tutto.

Collegamento tra rispetto e responsabilità giuridica: Il rispetto è legato ai nomi. Anonimato e rispetto si escludono a vicenda.

La comunicazione anonima promossa dai media digitali sta smantellando il rispetto su vasta scala. È anche responsabile della crescente cultura dell'indiscrezione e della mancanza di rispetto.

Nomi e rispetto sono collegati → nome fornisce la base per il riconoscimento, che si verifica sempre per nome.

Anche le pratiche che implicano responsabilità e affidabilità sono legate al nome. La fiducia può essere definita come fede nel nome. Dare risposte e promettere sono anche atti del nome.

Il supporto digitale - che separa i messaggi dai messaggeri, le notizie dalla sua fonte - sta distruggendo i nomi.

Potenza, dialogo e rispetto: Il potere è uno stato di asimmetria. Trova una relazione gerarchica. La comunicazione del potere non avviene dialogicamente.

A differenza del potere, il rispetto non implica necessariamente condizioni asimmetriche. Il rispetto è spesso sentito per modelli di ruolo o superiori, ma il rispetto reciproco è possibile sulla base di un riconoscimento simmetrico.

Homo digitalis e lo sciame virtuale: Oggi l'Homo digitalis è tutt'altro che "nessuno".

Mantiene la sua identità privata, anche quando fa parte dello sciame. Sebbene si esprima in forma anonima, di norma ha un profilo e lavora incessantemente per ottimizzarlo.

Invece di essere "nessuno", è insistentemente qualcuno che si esibisce e si contende l'attenzione. D'altra parte, nessuno mediato in massa non rivendica l'attenzione per sé stesso.

La sua identità privata è estinta. È svanito nella massa. Questo rappresenta anche la sua fortuna: dopo tutto, se non è nessuno, non può essere anonimo.

D'altra parte, l'Homo digitalis sale spesso sul palco in modo anonimo. Non è un nessuno ma un qualcuno, un anonimo.

Dal socius (sociale/membro) to solus (solo): L'homo digitalis non è in grado di radunarsi in una massa.

Quelli soggetti all'economia neoliberista non costituiscono un noi capace di un'azione collettiva. La crescente egoizzazione e atomizzazione della società sta riducendo lo spazio per l'azione collettiva. Come tale, blocca la formazione di una contro-potenza che potrebbe essere in grado di mettere in discussione l'ordine capitalista. Socius ha ceduto al solus. Nello sciame la società contemporanea non è modellata dalla moltitudine tanto quanto dalla solitudine. Il collasso generale del collettivo e del comunale lo ha travolto. La solidarietà sta svanendo. La privatizzazione ora raggiunge le profondità dell'anima stessa. L'erosione della comunità sta rendendo sempre più improbabili tutti gli sforzi collettivi.

Argomento 18:

La giustizia è troppo futurista? È importante sottolineare. Anche in Italia, come vedrai più avanti, la legge ha regolato diversi campi di giustizia. Per molti anni, in Europa la tarda digitalizzazione è stata contrassegnata come uno dei maggiori problemi.

1. Secondo l'OCSE (Organizzazione per la cooperazione e lo sviluppo economico, in inglese OECD Organization for Economic Co-operation and Development), la "cattiva giustizia" causata soprattutto dai ritardi nella digitalizzazione ha contribuito alla scarsa protezione dei diritti (PIETRANGELO (2016), 161).
2. La relazione OCSE spiega che esiste un ampio margine per ulteriori informazioni sulle attività giudiziarie nei paesi OCSE.
3. La maggior parte dei tribunali nei paesi dell'OCSE dispongono di moduli elettronici, siti Web e registri elettronici, ma molti paesi non hanno ancora implementato le strutture online e la possibilità per gli avvocati di seguire i casi online o lo hanno fatto solo in una minoranza di tribunali.

"Gli investimenti nell'informatizzazione dei tribunali sono legati a una maggiore produttività dei giudici (misurati come casi risolti per giudice), in particolare nei paesi in cui l'alfabetizzazione informatica è diffusa facilitando l'adozione di opportunità basate sulle ICT (Information and Comunication Technologies)" (OCSE 2013, 1).

Fino a qualche anno fa stavamo parlando di un ritardo nella giustizia digitale. Negli ultimi anni, tuttavia, non si fa menzione della digitalizzazione o dell'automazione ma dell'intelligenza artificiale, come se il primo passo fosse già compiuto ed efficace.

In qualche modo ciò è confermato dalle istituzioni pubbliche che oggi sono certamente interessate all'abilità tecnica e agli esperimenti di giustizia predittiva, da tempo praticati in così tanti Stati, che finora legiferano solo sui casi di giustizia digitale.

- Processo telematico o informatizzazione dei procedimenti?
  - I paragrafi precedenti meritano ulteriori studi sull'evoluzione del processo telematico nell'ordine italiano.

- Il legislatore italiano del decennio 2000-2010 ha dovuto affrontare la possibilità di procedere secondo due metodi:
    - Innanzi tutto, c'era la possibilità di avviare un percorso culturale che sfruttava la tecnologia dell'informazione per attuare cambiamenti strutturali nelle regole procedurali, finendo per influenzare in modo significativo i principi relativi al giusto processo (articolo 111 della Costituzione).
    - In secondo luogo, era concepibile adottare la tecnologia dell'informazione non come portatrice di una nuova idea di processo ma come mero catalizzatore dell'attività tout court della giustizia, sia per quanto riguarda il processo in senso stretto, sia in riferimento a le attività amministrative sono collaterali al processo, andando a incidere non tanto sulle regole del giusto processo ma sull'efficacia dell'azione amministrativa e in generale sul buon andamento dell'PA, Pubblica Amministrazione (articolo 97 della Costituzione).

Di fronte a una prima iniziativa pionieristica, che sembrava abbracciare il primo approccio, tutti gli interventi regolatori effettivamente attuati hanno avuto un impatto sul secondo metodo, rendendo il "sistema giudiziario" più fluido senza influenzare in modo significativo il processo e le regole del rituale.

Nell'ultimo decennio si è verificata una proliferazione di "processi telematici": le riforme hanno riguardato il processo civile, il processo amministrativo, il processo contabile e il processo fiscale.

Parallelamente all'informatizzazione della giustizia c'è stata l'adozione, con mezzi legislativi, di nuovi codici relativi a processi che fino ad allora erano governati da discipline ingombranti e nebulose: ci riferiamo, in particolare, al nuovo codice del processo amministrativo (d. lgs. 2 luglio 2010, n. 104) e al nuovo codice di giustizia contabile (d.lgs. 26 agosto 2016, n. 174).

Per motivi di sintesi, l'attenzione sarà focalizzata su alcuni aspetti peculiari del P.C.T. (Processo Civile Telematico) e del P.A.T. (Processo Amministrativo Telematico), per verificare se e in che modo l'informatizzazione del processo ha influito sulla natura del processo stesso o se si trattava di una mera automazione del procedimento.

La conclusione, come dovremo evidenziare, tende alla seconda ipotesi.

Argomento 19:

Definizione stessa di "Processo Telematico": La definizione stessa di "processo telematico" sembra in realtà essere portatrice di incomprensioni: in nessun caso, infatti, il legislatore ha introdotto un vero processo telematico.

Sebbene significativi, gli interventi normativi degli ultimi dieci anni hanno infatti consentito agli uffici pubblici di ottimizzare le proprie attività in vista dell'efficienza dell'azione amministrativa.

Allo stesso tempo, l'attuazione delle più recenti riforme ha permesso ai dipendenti del Ministero di lavorare più facilmente e gli operatori legali esterni all'amministrazione (prima di tutto, gli avvocati) di agire più da vicino con gli uffici pubblici.

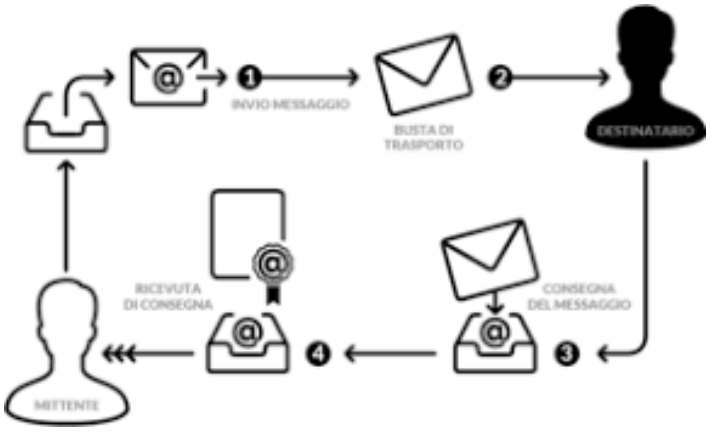
Questo cambiamento ha radicalmente modificato il lavoro dei professionisti legali, ma non ha influito sulle norme procedurali, che sono rimaste invariate.

Non vi è dubbio, tuttavia, che un meccanismo di giustizia predittiva basato sull'intelligenza artificiale sia meglio combinato con i sistemi basati sulla regola dell'associazione precedente. Viceversa, nei sistemi di diritto civile la procedura inferenziale del Giudice mantiene una connotazione fortemente personale e rende difficile generalizzare i metodi rintracciati nella prima parte di questo lavoro.

Nel processo italiano, quindi, al momento non vi è traccia di sistemi (chiusi o aperti) di giustizia predittiva, né di cambiamenti sostanziali nella struttura del processo.

Quindi sembra corretto parlare, piuttosto che "processo telematico", di informatizzazione (e talvolta automazione) di una serie di adempimenti relativi al processo.

Il processo civile telematico italiano (P.C.T.):



Il progetto Bassanini (l. 15 marzo 1997, n. 59, realizzato sul punto con DPR 13 febbraio 2001, n. 123):

Fu portatore di un'idea rivoluzionaria (per il tempo) di giustizia elettronica, iniziando un percorso che avrebbe condotto nel tempo a una riorganizzazione progressiva dell'amministrazione della giustizia, usando la tecnologia per favorire la creazione di database in grado di guidare l'interprete attraverso il immediata conoscenza delle linee guida della giurisprudenza.

Dopo l'abbandono del progetto "Bassanini", l'evoluzione del processo civile telematico è stata regolata da una serie di fonti regolatorie assolutamente frastagliate, tali da rendere difficile persino un lavoro di sistematizzazione. Sebbene la legislazione del settore sia principalmente contenuta nelle disposizioni di rango secondario (regolamenti), ci sono state alcune modifiche al codice rituale.

Quest'ultimo, tuttavia, riguardava disposizioni specifiche, che erano semplicemente aggiornate in relazione alle esigenze e agli effetti dei documenti e delle comunicazioni elettroniche (articoli 83, 133, secondo paragrafo, 136, secondo paragrafo, 137, 149-bis, 366, cpc, come nonché numerosi articoli relativi al processo esecutivo e ad altrettante disposizioni, fuori dal codice di rito, relative alle comunicazioni e alle notifiche del Registro).

La disciplina organica del cosiddetto "processo telematico" è contenuta in un decreto ministeriale (decreto ministeriale del 21 febbraio 2011, n. 44). La scelta appare almeno discutibile a livello sistematico e sembra che nasconda la filosofia alla base delle misure di riforma dell'ultimo decennio, nella parte in cui il "processo telematico" è concepito solo come un insieme di regole e protocolli informatici che La giustizia è richiesta per conformarsi. La visione sembra essere molto lontana dalle idee, forse eccessivamente lungimiranti per il momento, promosse dalla fine degli anni '90.

In sintesi, è possibile ritenere che il processo elettronico civile in Italia sia ridotto, ad oggi, in una serie di regole che favoriscono l'uso dello strumento informatico per perseguire una maggiore efficienza dell'amministrazione della giustizia.

I dati pubblicati dal Ministero, aggiornati al 31 dicembre 2018, mostrano un quadro generale di costante crescita nell'uso del processo elettronico, che per la maggior parte è ora obbligatorio.

L'aumento dei pagamenti telematici effettuati nel 2018 è particolarmente significativo.

Tuttavia, dall'esame degli stessi dati forniti dal Ministero della giustizia, è chiaro che le riforme del decennio 2000-2010 hanno riguardato solo l'amministrazione della giustizia, ma solo minimamente sulla natura e le regole del processo.

A tal fine sembra del tutto fuorviante parlare di "processo telematico". Anzi, sarebbe più corretto parlare di automazione dell'amministrazione della giustizia.

Rinviare, per *de jure condito* (giuste condizioni) analisi dell'attuale disciplina, ai numerosi contributi scientifici in materia, sembra opportuno soffermarsi brevemente sull'opportunità di sviluppare ulteriormente il processo civile per raggiungere finalmente un efficace "processo telematico".

Lo sviluppo del processo telematico non può essere separato da una scelta del campo: è ancora necessario un punto di svolta culturale, che consenta di superare il paradigma di efficienza IT dell'AP. abbracciare un'idea più profonda che combina l'uso dello strumento IT con le esigenze del giusto processo.

A tal fine, lo sviluppo del processo civile telematico dovrebbe svilupparsi secondo tre diverse linee:

- La razionalizzazione dell'attività dei dipendenti dell'amministrazione della giustizia;
- la creazione di strumenti idonei a guidare l'interprete nell'approccio alla giurisprudenza;
- la modifica di alcune regole procedurali che incidono sull'organizzazione del processo.

1. In primo luogo, l'adozione sempre crescente di moduli telematici preparati per lo svolgimento di attività di parte sta gradualmente alleggerendo il carico di lavoro degli uffici amministrativi, che attualmente rimangono principalmente organizzati sulla base delle regole preesistenti. Il personale amministrativo è ora privato di gran parte degli obblighi, che sono preparati direttamente dalle parti e che in ogni caso possono essere soggetti a un meccanismo di diffusione sempre crescente. A tal fine, il personale della giustizia potrebbe essere, nel tempo, riallocato, migliorando da un lato la professionalità con forti competenze informatiche e, dall'altro, rafforzando il ruolo del registrar (cancelliere, ufficiale di stato civile, direttore amministrativo) nell'assistenza alle audizioni e nell'esercizio delle funzioni del pubblico ufficiale.
2. In secondo luogo, la natura informatica (sempre crescente) delle misure giurisdizionali è senza dubbio adatta alla creazione di una banca dati nazionale e pubblica di giurisprudenza al merito, uno strumento attualmente esistente ma che merita di essere notevolmente rafforzato.
   L'uso di un unico "contenitore" di tutte le misure giurisdizionali, pubbliche e utilizzabili dai cittadini, potrebbe facilmente guidare l'interprete e l'operatore legale nelle scelte procedurali da compiere, con ovvie conseguenze sia sull'efficienza dell'AP, ma soprattutto sulla certezza del diritto.
   Su questo punto, i profili relativi al dovuto rispetto della riservatezza nel contesto dei dati giudiziari non possono essere omessi, come evidenziato dalla nuova versione dell'art. 59 del decreto legislativo 196/2003 sulla base delle disposizioni del GDPR (General Data Protection Regulation).
   Allo stesso tempo, l'uso da parte dei redattori di disposizioni di una sintassi logica, lineare e adeguata alle esigenze del "ricevitore IT", consentirebbe un'immediata sistematizzazione della giurisprudenza.
3. (Sistema che, come si vedrà di seguito, è già efficacemente utilizzato dalla giustizia amministrativa)
   In terzo luogo, il legislatore dovrebbe intervenire sulle norme che governano il processo civile, che si svolge lungo una serie cospicua di audizioni che, in pratica, mirano esclusivamente a segnare le fasi della procedura e che spesso hanno poca importanza pratica.

Argomento 20:

Sfruttamento del potenziale dell'IT: In questo senso, si potrebbe ipotizzare un maggiore sfruttamento del potenziale dello strumento IT per introdurre forme sperimentali di pubblico telematico. L'innovazione, che

al momento sembra materialmente fattibile, potrebbe favorire una maggiore rapidità dei processi, in particolare quelli governati da rituali basati precisamente sulla velocità (esempi sono il rito del lavoro e il processo di sintesi della cognizione ai sensi dell'articolo 702-bis cpc).

Un primo esempio di applicazione dell'audizione telematica è stato recentemente introdotto con riferimento alle procedure fallimentari. Articolo. 95, comma 3, della Legge Fallimentare (come modificato dal decreto legislativo 3 maggio 2016, n. 59) prevede oggi che il giudice delegato possa stabilire che l'udienza si svolge elettronicamente in modo idoneo a salvaguardare l'avversario e l'effettiva partecipazione di creditori, anche utilizzando le strutture informatiche rese disponibili alla procedura da terzi.

In assenza di disposizioni specifiche che consentano di estendere la norma all'intero processo civile, la giurisprudenza ha comunque colto l'opportunità di sperimentare forme di & quot; telematico contraddittorio & quot. Un esempio è una recente ordinanza interlocutoria di un tribunale al merito (Tribunale di Bologna, Sezione II civile, 26.3.2019) con cui, a fronte di una domanda di una delle parti volta a modificare un provvedimento emesso in precedenza, il giudice ha considerato: “l’opportunità, nel peculiare caso di specie, di utilizzare le potenzialità del processo civile telematico per instaurare il contraddittorio (telematico, appunto) sull’istanza così proposta dall’attrice, senza necessità di fissazione di una autonoma udienza, nella linea della dematerializzazione del processo civile”.

Inoltre, la grande rapidità dello strumento informatico potrebbe favorire l'introduzione di un principio generale di dimissioni delle audizioni in caso di assenso comune da parte di tutte le parti e da parte del giudice. In tal caso, l'audizione (intesa in senso fisico) potrebbe essere sostituita da una dichiarazione elettronica congiunta delle parti costituita e approvata dal giudice.

Un tale intervento regolamentare avrebbe la conseguenza di alleviare in modo significativo il lavoro dei magistrati, migliorando anche una celebrazione approfondita delle audizioni in cui la discussione assume un significato pratico tangibile.

Il processo amministrativo telematico italiano (P.A.T.): Il processo amministrativo elettronico costituisce senza dubbio il sistema di automazione della giustizia italiano più avanzato. Il sistema, valido per tutti i processi dinanzi ai tribunali amministrativi (ad eccezione, quindi, di ricorsi straordinari al Presidente della Repubblica) è obbligatorio a cominciare dall'1.1.2017.

Anche in questo caso, il sistema è stato concepito come un insieme di regole tecniche (che significa regole tecniche del computer) e non come una mutazione delle regole procedurali.

In effetti, in linea con quanto accaduto per il PCT, l'art. 13 dell'allegato 2 al decreto legislativo 2 luglio 2010, n. 104 (codice del processo amministrativo) ha chiesto alla Presidenza del Consiglio dei Ministri di regolare le regole tecnico-operative per la sperimentazione, l'applicazione graduale e l'aggiornamento del processo amministrativo telematico.

Con D.P.C.M. (Decreto del Presidente del Consiglio del Ministero /Decreto Ministeriale) 16 febbraio 2016, n. 40, il governo ha approvato le regole tecniche e il P.A.T. entrato in vigore il seguente 1.1.2017.

L'attuazione del P.A.T. configura un sistema molto più avanzato di P.C.T. e si basa su moduli informatici che sono preparati e firmati interamente dai difensori delle parti, che forniscono i relativi depositi tramite posta elettronica certificata.

Una volta che il modulo con firma digitale raggiunge la sua destinazione, il sistema informativo di giustizia amministrativa elabora automaticamente la richiesta, trasmettendo automaticamente la comunicazione di ricezione dell'atto con il numero di protocollo. Il sistema è così automatizzato che molto spesso alcune comunicazioni di cancelleria vengono effettuate di notte o durante le vacanze.

Di fronte all'informatizzazione completa e (quasi) incondizionata degli obblighi connessi al processo amministrativo, persistono disposizioni di "garanzia" che impongono agli utenti di giustizia amministrativa di utilizzare entrambi gli strumenti informatici secondo le regole tecniche del P.A.T. (come detto, obbligatorio) è il tradizionale sistema cartaceo. Ci riferiamo, in particolare, all'obbligo delle parti di procedere al deposito del cosiddetto; Copie di cortesia; di documenti procedurali (successivamente rinominati come copie obbligatorie).

È, infatti, un obbligo previsto dall'art. 7, comma 4, decreto legislativo 168/2016, di cui "per le sentenze presentate con i ricorsi presentati, in primo o secondo grado, deve essere presentata almeno una copia cartacea del ricorso e degli scritti di difesa, con l'attestazione di conformità al relativo deposito elettronico ".

La mancata osservanza del sopra citato adempimento comporta anche una grave conseguenza procedurale, in quanto impedisce la fissazione dell'udienza, anche nella fase cautelare della sentenza. Pertanto, a fronte di un sistema, in gran parte prezioso, di automazione della giustizia, le parti mantengono, ad oggi, l'obbligo di depositare anche su carta ciò che è già stato depositato con l'aiuto del P.A.T.

Pertanto, anche nel caso del processo amministrativo telematico, il legislatore (rettifica, il governo nell'esercizio del potere regolamentare) ha influenzato in modo significativo il processo, ma non il processo in senso stretto. Tuttavia, la struttura stessa del processo amministrativo (molto più snella rispetto al processo civile) potrebbe difficilmente trarre ulteriori benefici dallo strumento IT, che pertanto sembra essere sfruttato al massimo delle sue potenzialità. Sebbene la dittatura dell'algoritmo; rimane molto distante anche dal processo amministrativo, il sistema ha introdotto alcune forme automatizzate di controllo della regolarità dei documenti procedurali.

Secondo l'art. 3, comma 10, dell'allegato A del D.P.C.M. 40/2016, esiste la possibilità che il sistema informativo di giustizia amministrativa effettuerà "funzionalità automatizzate per il controllo della regolarità, anche fiscale, degli atti e dei documenti depositati da ciascuna parte". Come effettivamente osservato (VIOLA), la disposizione ha introdotto (inoltre a titolo di regolamento) una serie di cause limitate per il rigetto di alcuni atti procedurali, che sono trattati dal sistema informativo attraverso una funzione di blocco automatizzato che sostituisce il controllo manuale del Giudice, con evidenti ripercussioni sulla compatibilità con l'art. 111, comma 1 della Costituzione.

Conclusioni: La giustizia algoritmica fino ad oggi, sembra essere molto lontana dal processo italiano. Con questo breve contributo, l'attenzione si è concentrata sull'evoluzione di I.A. e sullo stato di avanzamento del processo telematico. È stato dimostrato che la stessa espressione processo telematico allude, ad oggi, a un uso crescente (a volte obbligatorio) dello strumento IT per l'esecuzione di requisiti procedurali, per la formazione di misure e per la relativa comunicazione.

Tuttavia, anche nel sistema più avanzato (il PAT) l'introduzione di nuove regole tecniche non ha influenzato, se non minimamente, la natura del processo, che rimane ancorato ai paradigmi tradizionali. Inoltre, l'idea stessa di una giustizia dettata dagli algoritmi sfugge totalmente a un ordine che massimizza il ruolo interpretativo del giudice. È vero che, a differenza di altri settori dell'AP, il servizio fornito dall'amministrazione della giustizia è spesso ostacolato da barriere e impedimenti di natura puramente formale che ne ostacolano la velocità e in alcuni casi la stessa utilità.

Rafforzare lo strumento IT anche con l'aiuto di I.A. potrebbe essere uno strumento essenziale per rimuovere questi ostacoli, garantendo una maggiore fruibilità della giustizia, una riduzione della durata dei procedimenti e l'adozione di forme organizzative più efficienti per l'AP.

Argomenti 21 – 34 (Argomento 10):

Riassunto: L'intelligenza artificiale e altre tecnologie digitali emergenti, come l'Internet delle cose (of Things) o le tecnologie di contabilità distribuita, hanno il potenziale per trasformare in meglio le nostre società ed economie. Tuttavia, il loro lancio deve prevedere garanzie sufficienti, per ridurre al minimo il rischio di danno che queste tecnologie possono causare, come lesioni personali o altri danni. Nell'UE, le norme di sicurezza dei prodotti assicurano che ciò avvenga. Tuttavia, tali regolamenti non possono escludere completamente la possibilità di danni derivanti dal funzionamento di queste tecnologie. Se ciò accade, le vittime chiederanno un risarcimento. Generalmente lo fanno sulla base dei regimi di responsabilità di diritto privato, in particolare del diritto illecito, eventualmente in combinazione con l'assicurazione. Solo la rigorosa responsabilità dei produttori per prodotti difettosi, che costituisce una piccola parte di questo tipo di regimi di responsabilità, è armonizzata a livello UE dalla Direttiva sulla responsabilità per danno da prodotti, mentre tutti gli altri regimi - ad eccezione di alcune eccezioni in settori specifici o in virtù di una legislazione speciale - sono regolati dagli stessi Stati membri.

Nella sua valutazione dei regimi di responsabilità esistenti sulla scia delle tecnologie digitali emergenti, la Formazione di nuove tecnologie del gruppo di esperti ha concluso che i regimi di responsabilità in vigore negli Stati membri assicurano almeno una protezione di base delle vittime il cui danno è causato dall'operazione di tali nuove tecnologie. Tuttavia, le caratteristiche specifiche di queste tecnologie e delle loro applicazioni, tra cui complessità, modifiche tramite aggiornamenti o autoapprendimento durante il funzionamento, la prevedibilità limitata e la vulnerabilità alle minacce alla ciybersecurity - può rendere più difficile offrire a queste vittime una richiesta di risarcimento in tutti i casi in cui ciò sembra giustificato. Può anche accadere che l'allocazione della responsabilità sia ingiusta o inefficiente.

Per ovviare a questo, è necessario apportare alcune modifiche ai regimi di responsabilità nazionali e dell'UE.

Di seguito sono elencati i risultati più importanti di questo rapporto su come dovrebbero essere progettati i regimi di responsabilità - e, se necessario, modificati - per far fronte alle sfide che le tecnologie digitali emergenti comportano.

- Una persona che utilizza una tecnologia consentita che comporta tuttavia un aumento del rischio di danni agli altri, ad esempio robot basati sull'intelligenza artificiale negli spazi pubblici, dovrebbe essere soggetta a una responsabilità rigorosa per i danni derivanti dal suo funzionamento.
- Nelle situazioni in cui un fornitore di servizi che garantisce il quadro tecnico necessario ha un grado di controllo più elevato rispetto al proprietario o all'utente di un prodotto o servizio reale dotato di AI, questo dovrebbe essere preso in considerazione nel determinare chi gestisce principalmente la tecnologia.
- Una persona che utilizza una tecnologia che non presenta un rischio maggiore di danno per gli altri dovrebbe comunque essere tenuta a rispettare i doveri per selezionare, utilizzare, monitorare e mantenere correttamente la tecnologia in uso e - in mancanza - dovrebbe essere responsabile per la violazione di tale doveri in caso di colpa.
- Una persona che utilizza una tecnologia che ha un certo grado di autonomia non dovrebbe essere meno responsabile per il conseguente danno che se tale danno fosse stato causato da un ausiliario umano.
- I produttori di prodotti o contenuti digitali che incorporano la tecnologia digitale emergente dovrebbero essere responsabili per i danni causati da difetti nei loro prodotti, anche se il difetto era causato da modifiche apportate al prodotto sotto il controllo del produttore dopo che era stato immesso sul mercato.
- Per situazioni che espongono terzi a un aumentato rischio di danni, l'assicurazione obbligatoria di responsabilità civile potrebbe offrire alle vittime un migliore accesso al risarcimento e proteggere i potenziali torturatori dal rischio di responsabilità.

- Laddove una particolare tecnologia accresca le difficoltà nel provare l'esistenza di un elemento di responsabilità oltre a quanto ci si possa ragionevolmente aspettare, le vittime dovrebbero avere il diritto di facilitare la prova.
- Le tecnologie digitali emergenti dovrebbero essere dotate di funzionalità di registrazione, se del caso nelle circostanze, e la mancata registrazione, o di fornire un accesso ragionevole ai dati registrati, dovrebbe comportare un'inversione dell'onere della prova al fine di non andare a danno della vittima.
- La distruzione dei dati della vittima dovrebbe essere considerata come un danno, risarcibile in condizioni specifiche.
- Non è necessario conferire personalità giuridica ai dispositivi o ai sistemi autonomi, in quanto i danni che questi possono causare possono e devono essere imputabili a persone o corpi esistenti.

Risultati chiave

1. La digitalizzazione apporta cambiamenti fondamentali ai nostri ambienti, alcuni dei quali hanno un impatto sul diritto della responsabilità. Ciò riguarda, in particolare, il
   (a) complessità,
   (b) opacità,
   (c) apertura,
   (d) autonomia,
   (e) prevedibilità,
   (f) guidabilità dei dati e (Data- Driveness)
   (g) vulnerabilità
   delle tecnologie digitali emergenti.

2. Ognuno di questi cambiamenti può essere di natura graduale, ma la dimensione del cambiamento graduale, la gamma e la frequenza delle situazioni interessate e l'effetto combinato si traducono in perturbazioni.
3. Sebbene le norme esistenti in materia di responsabilità offrano soluzioni in relazione ai rischi creati dalle tecnologie digitali emergenti, i risultati potrebbero non sembrare sempre appropriati, dato il mancato raggiungimento di:
4. È pertanto necessario prendere in considerazione adattamenti e modifiche ai regimi di responsabilità esistenti, tenendo presente che, data la diversità delle tecnologie digitali emergenti e la gamma di rischi corrispondente che possono comportare, è impossibile trovare un'unica soluzione adatto per l'intero spettro di rischi.
    a) un'allocazione equa ed efficiente delle perdite, in particolare perché non può essere attribuita quelle:
        - il cui comportamento discutibile ha causato il danno; o
        - che hanno beneficiato dell'attività che ha causato il danno; o
        - che avevano il controllo del rischio che si è materializzato; o
        - chi era il più economico evitatore di costi o il più economico acquirente di assicurazioni.
    b) una risposta coerente e adeguata del sistema giuridico alle minacce agli interessi degli individui, in particolare perché le vittime di danni causati dall'uso di tecnologie digitali emergenti ricevono un risarcimento inferiore o nullo rispetto alle vittime in una situazione funzionalmente equivalente che coinvolge la condotta umana e tecnologia convenzionale;
    c) un accesso effettivo alla giustizia, in particolare perché i contenziosi per le vittime diventano indebitamente onerosi o costosi.

5. Rischi comparabili dovrebbero essere affrontati da regimi di responsabilità simili, idealmente le differenze esistenti dovrebbero essere eliminate. Ciò dovrebbe anche determinare quali perdite sono recuperabili in quale misura.
6. La responsabilità per guasto (presunta o meno la colpa), così come la responsabilità rigorosa per i rischi e per i prodotti difettosi, dovrebbero continuare a coesistere. Nella misura in cui queste si sovrappongono, offrendo così alla vittima più di una base per chiedere un risarcimento contro più di una persona, disciplinano le norme sui torturatori multipli ([31]).
7. In alcuni ecosistemi digitali, la responsabilità contrattuale o altri regimi di indennizzo si applicheranno a fianco o invece della responsabilità illecita. Questo deve essere preso in considerazione nel determinare in che misura è necessario modificare quest'ultimo.
8. Ai fini della responsabilità, non è necessario conferire ai sistemi autonomi una personalità giuridica
9. La responsabilità oggettiva è una risposta adeguata ai rischi presentati dalle tecnologie digitali emergenti, se, ad esempio, sono gestiti in ambienti non privati e possono in genere causare danni significativi.
10. La responsabilità rigorosa dovrebbe spettare alla persona che controlla il rischio connesso al funzionamento delle tecnologie digitali emergenti e che beneficia del loro funzionamento (operatore).
11. Se vi sono due o più operatori, in particolare
    a) la persona che decide principalmente e beneficia dell'uso della tecnologia pertinente (operatore frontend) e
    b) la persona che definisce continuamente le caratteristiche della tecnologia pertinente e fornisce supporto backend essenziale e continuo (operatore back-end), la responsabilità rigorosa dovrebbe spettare a chi ha un maggiore controllo sui rischi dell'operazione
12. Difese esistenti ed eccezioni statutarie dalla responsabilità oggettiva potrebbero dover essere riconsiderate alla luce delle tecnologie digitali emergenti, in particolare se tali difese ed eccezioni sono adattate principalmente alle nozioni tradizionali di controllo da parte dell'uomo.
13. La responsabilità rigorosa del produttore dovrebbe svolgere un ruolo chiave nel risarcimento del danno causato da prodotti difettosi e dai loro componenti, indipendentemente dal fatto che assumano una forma tangibile o digitale.
14. Il produttore dovrebbe essere rigorosamente responsabile per i difetti nelle tecnologie digitali emergenti anche se tali difetti compaiono dopo che il prodotto è stato messo in circolazione, purché il produttore avesse ancora il controllo degli aggiornamenti o degli aggiornamenti della tecnologia. Una difesa dal rischio di sviluppo non dovrebbe applicarsi.
15. Se è dimostrato che una tecnologia digitale emergente ha causato danni, l'onere della prova del difetto dovrebbe essere annullato in caso di difficoltà o costi sproporzionati per stabilire il livello di sicurezza pertinente o dimostrare che tale livello di sicurezza non è stato soddisfatto . Ciò non pregiudica l'inversione dell'onere della prova di cui ai punti [22] e [24].
16. Gli operatori delle tecnologie digitali emergenti dovrebbero conformarsi a una gamma adattata di doveri di cura, anche per quanto riguarda
    a) scegliere il sistema giusto per il compito e le competenze giuste;
    b) monitoraggio del sistema; e
    c) manutenzione del sistema.
17. I produttori, anche se incidentalmente agiscono anche come operatori ai sensi di [10], dovrebbero:
    a) progettare, descrivere e commercializzare i prodotti in modo tale da consentire agli operatori di adempiere ai compiti di cui [16]; e
    b) monitorare adeguatamente il prodotto dopo averlo messo in circolazione.
18. Se il danno è causato dalla tecnologia autonoma utilizzata in modo funzionalmente equivalente all'impiego di ausiliari umani, la responsabilità dell'operatore per l'utilizzo della tecnologia dovrebbe

corrispondere al regime di responsabilità vicaria altrimenti esistente di un preponente per tali ausiliari.

19. Il parametro di riferimento per la valutazione delle prestazioni mediante tecnologia autonoma nel contesto della responsabilità vicaria è principalmente quello accettato per gli ausiliari umani. Tuttavia, una volta che la tecnologia autonoma supererà gli ausiliari umani, questo sarà determinato dalle prestazioni di una tecnologia comparabile disponibile che l'operatore potrebbe aspettarsi di utilizzare, tenendo conto dei doveri di cura dell'operatore ([16]).
20. Dovrebbe esserci l'obbligo per i produttori di dotare la tecnologia di mezzi di registrazione delle informazioni sul funzionamento della tecnologia (registrazione per progettazione), se tali informazioni sono in genere essenziali per stabilire se un rischio della tecnologia si è materializzato e se la registrazione è appropriata e proporzionata, tenendo conto, in particolare, della fattibilità tecnica e dei costi della registrazione, della disponibilità di mezzi alternativi per la raccolta di tali informazioni, del tipo e dell'entità dei rischi presentati dalla tecnologia e di eventuali conseguenze negative che la registrazione può avere i diritti degli altri.
21. La registrazione deve essere effettuata in conformità con la legge altrimenti applicabile, in particolare la legge sulla protezione dei dati e le norme relative alla protezione dei segreti commerciali.
22. L'assenza di informazioni registrate o l'incapacità di fornire alla vittima un accesso ragionevole alle informazioni dovrebbe innescare una presunzione confutabile che le condizioni di responsabilità che devono essere dimostrate dalle informazioni mancanti siano soddisfatte.
23. Se e nella misura in cui, a seguito della presunzione di cui al punto [22], l'operatore fosse tenuto a risarcire il danno, l'operatore avrebbe dovuto presentare una domanda di ricorso nei confronti del produttore che non era riuscito a dotare la tecnologia di strutture di registrazione.
24. Laddove il danno sia del tipo che le norme di sicurezza dovevano evitare, il mancato rispetto di tali norme di sicurezza, comprese le norme in materia di cybersecurity, dovrebbe comportare un'inversione dell'onere della prova
    a) causalità e / o
    b) guasto e / o
    c) l'esistenza di un difetto.
25. Come regola generale, la vittima dovrebbe continuare a essere tenuta a provare ciò che le ha causato il danno.
26. Fatta salva l'inversione dell'onere della prova proposto in [22] e [24] (a), l'onere della prova del nesso di causalità può essere alleggerito alla luce delle sfide delle tecnologie digitali emergenti se un bilanciamento dei seguenti fattori warrant che lo fanno:
    a) la probabilità che la tecnologia abbia almeno contribuito al danno;
    b) la probabilità che il danno sia stato causato dalla tecnologia o da qualche altra causa all'interno della stessa sfera;
    c) il rischio di un difetto noto all'interno della tecnologia, anche se il suo impatto causale effettivo non è evidente;
    d) il grado di tracciabilità e intelligibilità ex post dei processi all'interno della tecnologia che possono aver contribuito alla causa (asimmetria informativa);
    e) il grado di accessibilità ex post e la comprensibilità dei dati raccolti e generati dalla tecnologia
    f) il tipo e il grado di danno potenzialmente ed effettivamente causato.
27. Se è dimostrato che una tecnologia digitale emergente ha causato danni e la relativa responsabilità è subordinata all'intenzione o alla negligenza di una persona, l'onere della prova della colpa dovrebbe essere annullato se le difficoltà ei costi sproporzionati di stabilire il pertinente standard di cura e di provare la loro violazione lo giustifica. Ciò non pregiudica l'inversione dell'onere della prova proposto in [22] e [24] (b).

28. Se una causa di danno è attribuibile alla vittima, i motivi per ritenere responsabile un'altra persona dovrebbero applicarsi di conseguenza nel determinare se e in quale misura la richiesta di risarcimento della vittima possa essere ridotta.
29. Quando due o più persone cooperano su base contrattuale o simile nella fornitura di diversi elementi di un'unità commerciale e tecnologica e laddove la vittima può dimostrare che almeno un elemento ha causato il danno in modo da innescare una responsabilità ma non quale elemento, tutti i potenziali torturatori dovrebbero essere responsabili in solido nei confronti della vittima.
30. Nel determinare ciò che conta come unità commerciale e tecnologica ai sensi di [29] si deve considerare
    a) qualsiasi commercializzazione congiunta o coordinata dei diversi elementi;
    b) il grado della loro interdipendenza tecnica e interoperabilità; e
    c) il grado di specificità o esclusività della loro combinazione.
31. Laddove più di una persona è responsabile per lo stesso danno, la responsabilità nei confronti della vittima è generalmente solidale (congiunta). Le richieste di risarcimento tra i torturatori dovrebbero riguardare solo azioni identificate (diverse), a meno che alcune di esse non costituiscano un'unità commerciale e / o tecnologica ([29] - [30]), nel qual caso i membri di questa unità dovrebbero essere responsabili in solido per la loro quota cumulativa anche per il torturatore che cerca riparazione.
32. I danni causati ai dati possono comportare responsabilità laddove
    a) la responsabilità deriva dal contratto; o
    b) la responsabilità deriva dall'interferenza con un diritto di proprietà sul supporto su cui sono stati memorizzati i dati o con un altro interesse protetto come un diritto di proprietà ai sensi della legge applicabile; o
    c) il danno è stato causato da una condotta che viola il diritto penale o altre norme giuridicamente vincolanti il cui scopo è quello di evitare tale danno; o
    d) c'era l'intenzione di causare danni.
33. Maggiore è il danno potenziale frequente o grave derivante dalla tecnologia digitale emergente e minore è la probabilità che l'operatore sia in grado di indennizzare le vittime individualmente, più adeguata è l'assicurazione obbligatoria di responsabilità civile per tali rischi.
34. I fondi di compensazione possono essere utilizzati per proteggere le vittime di illeciti che hanno diritto a un risarcimento in base alle norme di responsabilità applicabili, ma le cui richieste non possono essere soddisfatte.

Contesto: L'intelligenza artificiale (AI) e altre tecnologie digitali emergenti, come Internet of Things e of Services (IoT / IoS) o tecnologie di contabilità distribuita (DLT), hanno un potenziale straordinario di trasformare prodotti, servizi e attività, procedure e pratiche, in una moltitudine di settori economici e in relazione a molti aspetti della società. Sebbene alcune di queste tecnologie non siano nuove, la loro crescente applicazione a una crescente varietà di scopi e le nuove combinazioni di una gamma di diverse tecnologie digitali emergenti, aprono possibilità senza precedenti. Tutto ciò viene fornito con la promessa di rendere il mondo un posto più sicuro, più equo, più produttivo, più conveniente, di aiutare a combattere malattie, povertà, criminalità, discriminazione e altre forme di ingiustizia e di collegare le persone in tutto il mondo. Sebbene ci si aspetta che molte di queste promesse si realizzino, il potenziale nuovo o potenziato comporta nuovi rischi o aumenta quelli esistenti.

Nel corso della storia, le norme, i concetti e i principi legali hanno superato le sfide poste dal progresso scientifico, tecnico e, più recentemente, tecnologico. Negli ultimi decenni, i principi adattabili di neutralità tecnologica ed equivalenza funzionale hanno soddisfatto l'impatto delle tecnologie digitali. Questi principi sono serviti da base per la risposta internazionale all'avvento e alle prime fasi di sviluppo dell'economia digitale e hanno ampiamente guidato le iniziative legislative e regolamentari sul commercio elettronico (e sui servizi della società dell'informazione) finora adottate.

L'adeguatezza e la completezza dei regimi di responsabilità di fronte alle sfide tecnologiche sono di fondamentale importanza per la società. Se il sistema è inadeguato o difettoso o presenta carenze nel trattamento dei danni causati dalle tecnologie digitali emergenti, le vittime possono finire totalmente o parzialmente non compensate, anche se un'analisi equa globale può giustificare l'indennizzo. L'impatto sociale di una potenziale inadeguatezza nei regimi giuridici esistenti, nell'affrontare i nuovi rischi creati dalle tecnologie digitali emergenti, potrebbe compromettere i benefici previsti. Alcuni fattori, come la presenza sempre crescente di tecnologie digitali emergenti in tutti gli aspetti della vita sociale e l'effetto moltiplicatore dell'automazione, possono anche esacerbare il danno che queste tecnologie causano. I danni possono facilmente diventare virali e propagarsi rapidamente in una società densamente interconnessa.

Background: Il 16 febbraio 2017 il Parlamento europeo ha adottato una risoluzione sulle norme di diritto civile in materia di robotica con raccomandazioni alla Commissione.

Ha proposto tutta una serie di iniziative legislative e non legislative nel campo della robotica e dell'intelligenza artificiale. In particolare, ha chiesto alla Commissione di presentare una proposta per uno strumento legislativo che fornisca norme di diritto civile sulla responsabilità dei robot e dell'intelligenza artificiale. Nel febbraio 2018, il servizio di ricerca parlamentare europeo (EPRS) ha pubblicato uno studio su "Un approccio comune dell'UE alle norme in materia di responsabilità e assicurazione per i veicoli connessi e autonomi" come una valutazione del valore aggiunto europeo che accompagna la risoluzione sulle norme di diritto civile.

Il programma di lavoro della Commissione per il 2018 ha annunciato che la Commissione avrebbe cercato di sfruttare al meglio l'intelligenza artificiale, poiché svolgerà sempre più un ruolo nelle nostre economie e società.

Il 14 dicembre 2017, in una dichiarazione congiunta, i presidenti della Commissione, del Parlamento e del Consiglio hanno convenuto di garantire "un livello elevato di protezione dei dati, diritti digitali e standard etici, acquisendo al contempo i benefici ed evitando i rischi di sviluppo dell'intelligenza artificiale e della robotica '. Il 25 aprile 2018, la Commissione ha pubblicato un documento di lavoro dei funzionari su "Responsabilità per le tecnologie digitali emergenti" che accompagna una comunicazione della Commissione alle altre istituzioni lo stesso giorno, "Intelligenza artificiale per l'Europa".

La presente comunicazione e la comunicazione Sibiu del maggio 2019 sottolineano che "un solido quadro normativo dovrebbe affrontare in modo proattivo le questioni etiche e giuridiche relative all'intelligenza artificiale". Nella sua comunicazione AI del 2018 la Commissione ha inoltre annunciato l'adozione di una relazione che valuta le implicazioni delle tecnologie digitali emergenti sui quadri di sicurezza e responsabilità esistenti entro la metà del 2019. Nel suo programma di lavoro per il 2019, ha confermato che "continuerà a lavorare sulla sfida emergente dell'intelligenza artificiale consentendo azioni coordinate in tutta l'Unione europea".

Nel marzo 2018, la Commissione ha istituito un gruppo di esperti sulla responsabilità e le nuove tecnologie, operando in due diverse formazioni: la direttiva sulla responsabilità del prodotto e la formazione sulle nuove tecnologie.

Nell'invito a presentare candidature è stato chiesto alla formazione di nuove tecnologie (NTF) di valutare "se e in che misura i regimi di responsabilità esistenti siano adattati alle realtà dei mercati emergenti a seguito dello sviluppo di nuove tecnologie come l'intelligenza artificiale,

robotica avanzata, IoT e problemi di sicurezza informatica ". Agli esperti è stato chiesto di esaminare se gli attuali regimi di responsabilità sono ancora "adeguati per facilitare l'adozione di ... nuove tecnologie promuovendo la stabilità degli investimenti e la fiducia degli utenti". In caso di carenze, l'NTF dovrebbe formulare raccomandazioni per le modifiche, senza limitarsi agli strumenti giuridici nazionali e dell'UE esistenti. Tuttavia, le raccomandazioni dovrebbero essere limitate alle questioni di responsabilità

extracontrattuale, lasciando da parte in particolare le norme corrispondenti (e complementari) sulla sicurezza e altre norme tecniche.

L'NTF si è riunito per la prima volta nel giugno 2018 e ha tenuto altre nove riunioni fino a maggio 2019. Dopo aver analizzato le leggi nazionali pertinenti e esaminato casi d'uso specifici, confronta vari aspetti dei regimi di responsabilità esistenti. Questo rapporto presenta i risultati del NTF.

Responsabilità per le tecnologie digitali emergenti ai sensi delle leggi vigenti in Europa

Panoramica dei regimi di responsabilità esistenti: La legge sugli illeciti negli Stati membri dell'UE è in gran parte non armonizzata, ad eccezione della legge sulla responsabilità per danno da prodotti ai sensi della direttiva 85/374 / CE, alcuni aspetti della responsabilità per violazione della legge sulla protezione dei dati (articolo 82 del regolamento generale sulla protezione dei dati (GDPR)) e responsabilità per violazione del diritto della concorrenza (Direttiva 2014/104 / UE). Esiste anche un regime consolidato che disciplina l'assicurazione di responsabilità civile in relazione ai danni causati dall'uso di autoveicoli (direttiva 2009/103 / CE), sebbene senza toccare la responsabilità per gli incidenti stessi. Il diritto dell'UE prevede inoltre un quadro legislativo sul conflitto di illeciti, nella forma del regolamento Roma II.

A livello nazionale, si può generalmente osservare che le leggi degli Stati membri non contengono (ancora) regole di responsabilità specificamente applicabili ai danni derivanti dall'uso di strumenti digitali emergenti

tecnologie come l'IA. In via eccezionale, le giurisdizioni che già consentono l'uso sperimentale o regolare di veicoli altamente o completamente automatizzati di solito prevedono anche la copertura di eventuali danni causati, sia a titolo assicurativo sia in riferimento alle regole generali.

Oltre a questa legislazione, gli effetti dannosi del funzionamento delle tecnologie digitali emergenti possono essere compensati dalle leggi ("tradizionali") esistenti in materia di danni contrattuali e illeciti in ciascuno Stato membro. Ciò vale per tutti i campi di applicazione dell'IA e di altre tecnologie digitali emergenti analizzate dall'NTF del gruppo di esperti.

In generale, queste leggi nazionali in materia di illecito civile comprendono una regola (o regole) che introduce la responsabilità basata sulla colpa con un ambito di applicazione relativamente ampio, accompagnato da diverse regole più specifiche che modificano i locali della responsabilità basata sulla colpa (in particolare la distribuzione dell'onere di provare la colpa) o stabilire una responsabilità indipendente dalla colpa (di solito chiamata responsabilità oggettiva o responsabilità basata sul rischio), che assume anche molte forme che variano in relazione all'ambito di applicazione della norma, alle condizioni di responsabilità e all'onere della prova.

La maggior parte dei regimi di responsabilità contiene la nozione di responsabilità per gli altri (spesso chiamata responsabilità vicaria).

Tuttavia, questi regimi potrebbero non portare sempre a risultati soddisfacenti e adeguati.

Inoltre, date le differenze significative tra le leggi sull'illecito di tutti gli Stati membri, l'esito dei casi sarà spesso diverso a seconda della giurisdizione applicabile.

Come dimostrato dall'esperienza con la direttiva sulla responsabilità del prodotto, gli sforzi per superare tali differenze armonizzando solo alcuni aspetti del diritto in materia di responsabilità potrebbero non portare sempre al livello desiderato di uniformità dei risultati.

Alcuni esempi dell'applicazione dei regimi di responsabilità esistenti alle tecnologie digitali emergenti: Nella maggior parte delle giurisdizioni, i danni causati dai veicoli a motore sono soggetti a un regime di responsabilità speciale.

Come accennato in precedenza, esiste un regime assicurativo a livello UE, sotto forma della direttiva (ricodificata) di assicurazione autoveicoli (MID), ma il MID armonizza solo la copertura assicurativa di responsabilità civile, non la responsabilità civile stessa. Gli Stati membri continuano pertanto a disciplinare la responsabilità illecita per gli incidenti che coinvolgono gli stessi autoveicoli, a loro discrezione limitati solo dal principio di efficacia del MID.

Queste regole di solito impongono la responsabilità al proprietario / detentore di un veicolo e / o al conducente, anche se ci sono sistemi che introducono reclami diretti nei confronti dell'assicuratore indipendentemente dalla responsabilità di qualsiasi altra persona. L'adeguatezza dei regimi di responsabilità del traffico esistenti per i veicoli autonomi (AV) può essere contestata, in particolare per quanto riguarda i sistemi che si basano sulla responsabilità fondata sui guasti in generale (ad esempio Malta) o in circostanze limitate, come nel caso di una collisione (Polonia ad esempio), o per determinati tipi di danni (ad esempio la Spagna), o che comportano l'applicazione del regime di responsabilità del traffico subordinato al coinvolgimento di un conducente (Italia). In caso di incidente con un solo veicolo possono emergere lacune di responsabilità nella misura in cui, in base alle norme sulla responsabilità del traffico esistenti, il proprietario / detentore ferito è escluso dal risarcimento. Alcuni sistemi giuridici escludono persino i passeggeri dalla protezione sotto la stretta responsabilità del traffico, o in generale (Grecia o Paesi Bassi ad esempio) o solo in circostanze specifiche (Polonia o Austria ad esempio). Questo sarebbe difficile da accettare per incidenti che coinvolgono AV. Dato il carattere complesso dell'ambiente di guida autonomo, anche l'esclusione della responsabilità oggettiva in caso di intervento di terzi può rivelarsi problematica, in particolare nel contesto dei rischi per la cibersicurezza, ad esempio in caso di violazione di un AV collegato o di un incidente è stato causato perché l'infrastruttura ICT ha inviato segnali sbagliati. Laddove il danno sia stato causato da un veicolo difettoso, possono essere applicate la responsabilità del prodotto o la responsabilità del produttore in caso di illecito, ma di solito diventano rilevanti solo nella fase di ricorso.

Per la maggior parte degli ecosistemi tecnologici (con cui intendiamo sistemi con dispositivi o programmi che interagiscono), tuttavia, non esistono regimi di responsabilità specifici. Ciò significa che la responsabilità del prodotto, le norme generali sul diritto illecito (responsabilità per colpa, illecito, violazione del dovere statutario) e, eventualmente, la responsabilità contrattuale, occupano il centro della scena. Più questi ecosistemi diventano complessi con le tecnologie digitali emergenti, più diventa difficile applicare i quadri di responsabilità.

Un esempio potrebbe essere il caso d'uso di reti e sistemi domestici intelligenti. Laddove i dispositivi di casa intelligente fossero già difettosi nel momento in cui sono stati messi in circolazione, si applica la legge sulla responsabilità del prodotto. Nella maggior parte delle giurisdizioni il produttore può anche essere responsabile ai sensi della legge generale sui reati, che potrebbe andare oltre la responsabilità del prodotto rendendo responsabile il produttore per, ad esempio, servizi digitali accessori difettosi e per gli aggiornamenti, nonché per guasti nella sorveglianza o nel monitoraggio del prodotto. In caso di danni causati dal venditore di un prodotto, possono presentarsi un fornitore di servizi di installazione / configurazione, un fornitore di servizi Internet, un fornitore di energia, un operatore cloud e altri soggetti coinvolti nello scenario della casa intelligente, sia la legge generale in materia di illecito civile, sia l'eventuale responsabilità contrattuale in gioco. Alcuni paesi (come la Spagna o la Grecia) possono utilizzare i loro regimi speciali di responsabilità per servizi difettosi, sulla base di un presunto errore da parte del fornitore di servizi. Altri sistemi legali operano esclusivamente o principalmente sulla base delle disposizioni generali in materia di responsabilità per colpa (clausole generali) o concetti relativamente aperti di diritto illecito (illecito per negligenza, violazione del dovere statutario). Queste disposizioni o concetti giuridici di solito richiedono la prova del mancato rispetto da parte del convenuto dello standard di cura richiesto.

Quando l'utente nello scenario della casa intelligente è contrattualmente legato all'attore (venditore, fornitori di servizi di installazione, fornitore di servizi Internet, fornitore di energia, operatore cloud), quest'ultimo potrebbe essere responsabile in contratto all'utente per danni causati da inadempienza. Alcuni

sistemi giuridici (Germania, Austria o Grecia, e in una certa misura la Danimarca, ad esempio) estendono la responsabilità contrattuale a determinate condizioni, consentendo a terzi di invocare un contratto che non erano parti a sé stessi. Ciò si applica alle situazioni in cui si ritiene che il contratto stabilisca doveri per proteggere anche tali soggetti terzi, consentendo a questi ultimi di intentare causa per risarcimento in caso di violazione.

Il terzo protetto deve essere prevedibilmente vicino al partner contraente, tuttavia, confrontato in modo simile con il pericolo derivante dall'inadempimento (come familiari o ospiti). Qualsiasi tipo di responsabilità contrattuale è tuttavia generalmente soggetta a limitazioni contrattuali (e talvolta anche statutarie).

Allo stesso modo, situazioni complesse possono comportare casi in cui il danno è stato causato da applicazioni sanitarie autonome. Tale danno sarebbe di solito soggetto a responsabilità per colpa, sia in contratto che per illecito. Molte giurisdizioni consentono alla vittima di presentare reclami simultanei in base al contratto e in caso di illecito. In alcune giurisdizioni, tuttavia, ciò non è possibile, nel qual caso diventa necessario scegliere l'uno o l'altro. Quando un danno è innescato da un difetto presente prima della messa in circolazione di tali applicazioni, può applicarsi la responsabilità del prodotto, se l'applicazione o il dispositivo è considerato un prodotto ai fini della legge sulla responsabilità del prodotto. Ulteriori complessità derivano dall'interazione tra questi regimi e i sistemi di assicurazione sociale e / o sanitaria.

I danni causati dall'uso di algoritmi o AI nel mercato finanziario sono attualmente soggetti a riparazione in base ai regimi tradizionali basati sui guasti. Alcune giurisdizioni, tuttavia, consentono al richiedente di invocare il diritto amministrativo (regolamenti finanziari) per stabilire il parametro di riferimento in base al quale deve essere valutata la condotta dell'autore. A livello contrattuale, l'asimmetria informativa risultante dall'uso dell'IA può giustificare l'applicazione di un regime di responsabilità precontrattuale (legale o giurisprudenziale) (culpa in contrahendo e concetti simili). Sembra più probabile, tuttavia, che la reazione del sistema giuridico a potenziali irregolarità nel contratto con l'uso di algoritmi si baserà su strumenti di diritto contrattuale per valutare e contestare la validità dei contratti (consenso viziato, mancanza di equità, ecc.).

L'uso della blockchain, in particolare le criptovalute, non è soggetto a particolari regole di responsabilità e la nuova legislazione già adottata o in discussione in alcuni Stati membri, correlata tra l'altro alle offerte iniziali di monete, alle certificazioni delle piattaforme e alla sicurezza informatica, non si estende a risarcimento del danno. Nella misura in cui questa legislazione prevede i doveri e le responsabilità dei partecipanti a una blockchain o delle autorità pubbliche, può essere rilevante per stabilire lo standard di cura ai fini dell'applicazione delle regole di responsabilità basate su colpa.

Sfide specifiche per gli attuali regimi di diritto illecito posti dalle tecnologie digitali emergenti: È possibile applicare i regimi di responsabilità esistenti alle tecnologie digitali emergenti, ma alla luce di una serie di sfide e a causa delle limitazioni dei regimi esistenti, ciò potrebbe lasciare le vittime insufficientemente o totalmente non compensate. L'adeguatezza delle norme di responsabilità esistenti può quindi essere discutibile, considerando in particolare che queste regole sono state formulate decenni o addirittura secoli fa, sulla base di concetti ancora più vecchi e incorporando un modello principalmente antropocentrico e monocausale di danno inflitto.

Danno (Damage): Lo scopo principale della legge sul crimine è indennizzare le vittime per le perdite che non dovrebbero dover sopportare interamente sulla base di una valutazione di tutti gli interessi coinvolti. Tuttavia, verrà indennizzato solo un danno risarcibile, il che significa un danno a una gamma limitata di interessi che un sistema legale ritiene meritevoli di protezione.

Sebbene vi sia un accordo unanime sul fatto che lesioni a una persona o alla proprietà fisica possano scatenare una responsabilità dolorosa, ciò non è universalmente accettato per pura perdita economica.

I danni causati da algoritmi di autoapprendimento sui mercati finanziari, ad esempio, rimarranno pertanto spesso non compensati, poiché alcuni sistemi giuridici non forniscono alcuna protezione del diritto illecito per tali interessi o solo se sono soddisfatti requisiti aggiuntivi, come un rapporto contrattuale tra parti o la violazione di alcune specifiche regole di condotta. Né è universalmente accettato in tutta Europa che il danneggiamento o la distruzione dei dati sia una perdita di proprietà, poiché in alcuni sistemi legali la nozione di proprietà è limitata agli oggetti corporali ed esclude gli intangibili.

Altre differenze esistono quando si tratta del riconoscimento dei diritti della personalità, che possono anche essere influenzati negativamente dalle tecnologie digitali emergenti, se alcuni dati vengono rilasciati, ad esempio violando il diritto alla privacy.

Tuttavia, in generale, l'IA e altre tecnologie digitali emergenti non mettono in discussione l'attuale gamma di danni risarcibili di per sé. Piuttosto, alcune delle categorie di perdite già riconosciute potrebbero essere più rilevanti nei casi futuri che negli scenari tradizionali di illecito. Anche il danno come prerequisito per la responsabilità è un concetto flessibile: l'interesse in gioco può essere più o meno significativo e anche l'entità del danno a tale interesse può variare. Ciò a sua volta può avere un impatto sulla valutazione complessiva della legittimità o meno di una richiesta di risarcimento in un singolo caso.

Causa (Causation): Uno dei requisiti più essenziali per stabilire la responsabilità è un nesso causale tra il danno della vittima e la sfera dell'imputato. Di norma, è la vittima che deve dimostrare che il loro danno ha avuto origine da un comportamento o un rischio attribuibile al convenuto. La vittima deve quindi produrre prove a sostegno di questo argomento. Tuttavia, meno evidente è la sequenza di eventi che ha portato alla perdita della vittima, più complessa è l'interazione di vari fattori che hanno contribuito congiuntamente o separatamente al danno, più collegamenti cruciali nella catena di eventi sono sotto il controllo dell'imputato, più sarà difficile per la vittima riuscire a stabilire la causalità senza alleviare il proprio onere della prova. Se la vittima non riesce a persuadere il tribunale, secondo lo standard di prova richiesto, che qualcosa per cui l'imputato deve giustificare il danno che ha subito, perderà il caso, indipendentemente da quanto forte sarebbe stato contro l'imputato altrimenti (ad esempio, a causa di evidente negligenza da parte del convenuto).

Per quanto sia difficile dimostrare che alcuni difetti hardware sono stati il motivo per cui qualcuno è stato ferito, ad esempio, diventa molto difficile stabilire che la causa del danno sia stata un algoritmo difettoso.

> ***Illustrazione 1.*** *Se un rilevatore di fumo in un ambiente domestico intelligente non attiva un allarme a causa di un cablaggio difettoso, questo difetto può essere identificabile (e in questo caso è persino visibile). Se, d'altra parte, il rilevatore di fumo non si è spento a causa di un errore del firmware, questo potrebbe non essere dimostrato così facilmente (anche se l'assenza di un allarme di per sé può essere facilmente provata), anche solo perché richiede un attento analisi del codice del firmware e della sua idoneità per i componenti hardware del rilevatore di fumo.*

È ancora più difficile se l'algoritmo sospettato di causare danni è stato sviluppato o modificato da alcuni sistemi di intelligenza artificiale alimentati dall'apprendimento automatico e dalle tecniche di apprendimento profondo, sulla base di molteplici dati esterni raccolti dall'inizio del suo funzionamento. Anche senza modifiche alla progettazione originale del software, i criteri integrati che guidano la raccolta e l'analisi dei dati e il processo decisionale potrebbero non essere facilmente spiegabili e spesso richiedono costose analisi da parte di esperti.

Questo di per sé può essere un ostacolo pratico primario nel perseguire una domanda di risarcimento, anche se tali costi dovrebbero in definitiva essere recuperabili fintanto che le probabilità di successo sono difficili da prevedere per la vittima in anticipo.

In caso di responsabilità oggettiva, dimostrare la causalità può essere più facile per la vittima, e non solo nelle giurisdizioni in cui si presume la causalità in tali casi.

Invece di stabilire un comportamento illecito nella sfera del convenuto, la vittima deve solo provare che il rischio di innescare una responsabilità rigorosa si è materializzato. A seconda di come questo rischio è stato definito dal legislatore, ciò può essere più semplice, considerando che, ad esempio, gli attuali statuti di responsabilità per i veicoli a motore richiedono semplicemente un "coinvolgimento" dell'auto o il suo "funzionamento" quando si è verificato l'incidente.

Oltre alla complessità iniziale dei sistemi di intelligenza artificiale al momento del rilascio, molto probabilmente saranno soggetti ad aggiornamenti più o meno frequenti che non sono necessariamente forniti dal produttore originale.

Identificare quale parte di un codice ora difettoso era errata dall'inizio o è stata modificata in modo negativo nel corso di un aggiornamento, richiederà almeno (di nuovo) un significativo contributo di esperti, ma farlo è essenziale per determinare chi richiedere un risarcimento.

Il funzionamento dei sistemi di intelligenza artificiale spesso dipende da dati e altri input raccolti dai sensori del sistema o aggiunti da fonti esterne. Non solo tali dati possono essere imperfetti in sé, ma anche l'elaborazione di dati altrimenti corretti può essere imperfetta. Quest'ultimo può essere dovuto a difetti originali nella progettazione del trattamento dei dati o alla conseguenza di distorsioni delle capacità di autoapprendimento del sistema dovute alla maggior parte dei dati raccolti, la cui casualità può portare il sistema di intelligenza artificiale in questione a erroneamente percepire e classificare erroneamente il successivo input.

I problemi di causalità incerta non sono ovviamente nuovi per i sistemi giuridici europei, anche se sono posti in modo diverso a seconda dello standard di prova applicabile.

Fintanto che l'incertezza supera tale soglia, la vittima rimarrà non compensata, ma non appena la probabilità della teoria causale su cui poggia il caso della vittima soddisfa lo standard di prova, sarà completamente compensata (soggetti agli ulteriori requisiti di responsabilità).

Questo dilemma del tutto o niente è già stato affrontato in tutta Europa da alcune modifiche che aiutano la vittima a dimostrare causalità in determinate circostanze. I tribunali possono ad esempio essere disposti ad accettare prove prima facie in scenari complessi, come quelli che emergono dalle tecnologie digitali emergenti, in cui l'esatta sequenza di eventi può essere difficile da dimostrare.

Sebbene l'onere di provare la causalità non sia ancora spostato, è chiaramente alleviato per la vittima, che non ha bisogno di provare ogni singolo anello della catena di causalità se i tribunali accettano che un determinato risultato sia l'effetto tipico di un certo sviluppo in quella catena. Inoltre, come hanno dimostrato casi passati di negligenza medica, i tribunali tendono ad essere disposti a porre l'onere di produrre prove sulla parte che è o dovrebbe avere il controllo delle prove, con la mancata presentazione di tali prove risultanti in una presunzione a svantaggio di quella festa. Se, ad esempio, alcuni file di registro non possono essere prodotti o letti correttamente, i tribunali possono essere preparati a trattenerli contro la parte che era responsabile di queste registrazioni (e / o della tecnologia per analizzarle).

In alcuni casi, alcuni legislatori europei sono intervenuti e spostato del tutto l'onere di provare il nesso di causalità, presumendo in tal modo che il danno della vittima sia stato causato dall'imputato, pur lasciando al convenuto la possibilità di confutare ciò.

Resta da vedere in che misura uno di questi strumenti verrà utilizzato a favore della vittima se il loro danno potrebbe essere stato causato dalle tecnologie digitali emergenti.

È già difficile dimostrare che una certa condotta o attività è stata la causa del danno, ma diventa ancora più complesso se entrano in gioco altre cause alternative. Questa non è una novità, ma diventerà molto più un problema in futuro, data l'interconnessione delle tecnologie digitali emergenti e la loro maggiore dipendenza da input e dati esterni, rendendo sempre più dubbioso il fatto che il danno in questione sia stato innescato da un singolo originale causa o dall'interazione di più (effettive o potenziali) cause.

Gli attuali regimi di diritto illecito in Europa gestiscono tali incertezze nel caso di molteplici potenziali fonti di danno in modo abbastanza diverso. Anche se è stato dimostrato che qualcosa ha innescato il danno (ad esempio, perché un'auto autonoma si è scontrata con un albero), la vera ragione di ciò non è sempre altrettanto evidente. L'auto potrebbe essere stata progettata in modo inadeguato (sia esso hardware, software preinstallato o entrambi), ma potrebbe anche aver letto erroneamente corretto, o ricevuto dati errati, o un aggiornamento software fatto dal produttore originale o da un terzo la parte potrebbe essere difettosa o l'utente potrebbe non essere riuscito a installare un aggiornamento che avrebbe impedito la collisione, per fornire solo alcuni esempi, per non parlare di una combinazione di più di questi fattori.

La classica risposta delle leggi sul crimine esistenti in Europa in tali casi di causalità alternativa, se non è chiaro quale delle diverse possibili cause sia stata l'influenza decisiva per innescare il danno, è che nessuno è responsabile (poiché le prove della vittima non riescono a raggiungere la soglia per dimostrare la causa di una causa) o che tutte le parti sono responsabili in solido, che è l'opinione della maggioranza.

Il primo risultato è indesiderabile per la vittima, il secondo per quei torturatori semplicemente possibili che in realtà non hanno causato danni, ma possono ancora essere obiettivi attraenti per le controversie a causa della loro disponibilità procedurale e / o della loro più promettente capacità finanziaria di pagare effettivamente un risarcimento. Pertanto, il problema di chi ha realmente causato il danno in questione spesso non sarà risolto nel primo ciclo di controversie avviato dalla vittima, ma a livello di ricorso, se mai. Approcci più moderni prevedono una responsabilità proporzionale almeno in alcuni casi, riducendo il reclamo della vittima nei confronti di ogni potenziale torturatore a una quota corrispondente alla probabilità che ciascuno di essi abbia effettivamente causato il danno in questione.

Errori e difetti: Come già accennato nella panoramica di cui sopra, le leggi sul crimine in Europa sono tradizionalmente basate su colpa, fornendo un risarcimento alla vittima se l'imputato è responsabile del danno del precedente.

Tale colpa è comunemente legata alla deviazione da una condotta prevista, ma non dimostrata, dal torturatore. Se un sistema giuridico distingue tra illeciti oggettivi o soggettivi e / o divide la base della responsabilità per colpa in illecito e colpa, due cose rimangono cruciali: identificare i doveri di cura che l'autore del reato avrebbe dovuto assolvere e dimostrare che la condotta di l'autore del danno non ha assolto tali doveri.

I compiti in questione sono determinati da vari fattori. A volte sono definiti in anticipo da un linguaggio statutario che prescrive o proibisce determinati comportamenti specifici, ma spesso devono essere ricostruiti dopo il fatto dal tribunale sulla base di convinzioni sociali sulla condotta prudente e ragionevole delle circostanze.

Le tecnologie digitali emergenti rendono difficile l'applicazione di regole di responsabilità basate su guasti, a causa della mancanza di modelli consolidati di corretto funzionamento di queste tecnologie e della possibilità del loro sviluppo come risultato dell'apprendimento senza controllo umano diretto.

I processi in esecuzione nei sistemi di intelligenza artificiale non possono essere tutti misurati in base a doveri di cura progettati per la condotta umana o non senza aggiustamenti che richiederebbero ulteriori giustificazioni.

Poiché i sistemi giuridici europei tendono a regolare in anticipo i requisiti di prodotto e di sicurezza più di altre giurisdizioni, è possibile che vengano introdotte almeno alcune norme minime (se non altro, ad esempio, i requisiti di registrazione che alleviano un'analisi, dopo il fatto, di ciò che è effettivamente accaduto), per aiutare a definire e applicare i doveri di cura rilevanti per la legge sui reati in caso di danni. Una violazione di tali requisiti statutari o regolamentari può anche innescare la responsabilità più facilmente per la vittima, spostando ad esempio l'onere della prova di colpa in molti sistemi.

Tuttavia, tali requisiti non saranno presenti fin dall'inizio e potrebbero essere necessari anni prima che tali regole emergano, sia nella legislazione che nei tribunali.

I requisiti legali devono essere distinti dagli standard del settore (o pratiche) non ancora riconosciuti dal legislatore. La loro rilevanza in un'azione illecita è necessariamente più debole, anche se i tribunali possono considerare anche tali requisiti quando valutano a posteriori se la condotta è stata rispettata o meno con i doveri di cura che dovevano essere espletati in tali circostanze.

Fare un passo indietro e spostare l'attenzione su uno sviluppatore di software che ha scritto il firmware per alcuni gadget intelligenti, ad esempio, non risolve completamente il problema, poiché - come già accennato - il software potrebbe essere stato progettato per adattarsi a situazioni senza precedenti o almeno per far fronte a nuovi input che non corrispondono a nessun dato preinstallato. Se il funzionamento di alcune tecnologie che includono l'IA, ad esempio, è legalmente consentito, presumendo che lo sviluppatore abbia fatto uso di conoscenze all'avanguardia al momento del lancio del sistema, qualsiasi scelta successiva effettuata dalla tecnologia AI in modo indipendente può non necessariamente attribuibile a qualche difetto nel suo design originale. Si pone quindi la questione se la scelta di ammetterlo sul mercato o di implementare il sistema di intelligenza artificiale in un ambiente in cui il danno è stato successivamente causato, costituisce di per sé una violazione dei doveri di cura applicabili a tali scelte.

Oltre alle difficoltà nel determinare ciò che costituisce un difetto nel caso di un danno causato da una tecnologia digitale emergente, potrebbero esserci anche problemi con la dimostrazione del difetto. In generale, la vittima deve dimostrare che l'imputato (o qualcuno la cui condotta è attribuibile a loro) era in colpa. Pertanto, la vittima non solo deve identificare quali doveri di cura l'imputato avrebbe dovuto espletare, ma anche dimostrare al tribunale che tali doveri erano stati violati. Dimostrare che l'imputato è in colpa implica fornire al tribunale prove che possano indurlo a credere quale fosse lo standard di cura applicabile e che non è stato soddisfatto. La seconda parte di questo è fornire prove di come si è verificato l'evento che ha causato il danno. Più complesse sono le circostanze che portano al danno della vittima, più è difficile identificare prove pertinenti.

Ad esempio, può essere difficile e costoso identificare un bug in un codice software lungo e complicato. Nel caso dell'IA, esaminare il processo che porta a un risultato specifico (come i dati di input hanno portato ai dati di output) può essere difficile, molto dispendioso in termini di tempo e costoso.

Responsabilità Vicaria (Vicarius Liability): Le leggi sul crimine esistenti in Europa differiscono sostanzialmente nel loro approccio a ritenere qualcuno (il principale) responsabile della condotta di un altro (ausiliario).

Alcuni attribuiscono al preside un comportamento ausiliario senza ulteriori requisiti, a parte il fatto che l'ausiliario ha agito sotto la direzione del preponente e a beneficio del preponente. Altri ritengono il principale responsabile nel diritto illecito solo in circostanze molto eccezionali, come la pericolosità nota dell'assistente o la completa inadeguatezza dell'assoluto per il compito assegnato o se l'imputato era in errore nella scelta o nel controllo dell'assistito.

Esistono anche giurisdizioni che utilizzano entrambi gli approcci.

Le giurisdizioni con una definizione neutra (e quindi più ampia) di responsabilità oggettiva (come responsabilità senza colpa della persona responsabile in generale) considerano la responsabilità vicaria come una semplice variante di questa responsabilità rigorosa (o senza colpa). Se la nozione di responsabilità oggettiva è equiparata alla responsabilità di alcuni rischi specifici, oggetti o attività pericolosi, la responsabilità vicaria è piuttosto associata alla responsabilità per colpa, come responsabilità del principale senza colpa personale propria, ma per il (pass-on) 'colpa' del loro ausiliario invece, anche se la condotta del ausiliario non viene quindi necessariamente valutata in base ai parametri di riferimento applicabili a loro stessi, ma ai parametri di riferimento per il principale.

Indipendentemente da tali differenze, il concetto di responsabilità vicaria è considerato da alcuni come un possibile catalizzatore per sostenere che gli operatori di macchine, computer, robot o tecnologie simili dovrebbero anche essere strettamente responsabili per le loro operazioni, sulla base di un'analogia con la base della responsabilità vicaria . Se qualcuno può essere ritenuto responsabile per le azioni illecite di alcuni aiutanti umani, perché il beneficiario di tale sostegno non dovrebbe essere ugualmente responsabile se affidano invece le loro funzioni a un aiutante non umano, considerando che beneficiano ugualmente di tale delega? L'argomento politico è abbastanza convincente che l'uso dell'assistenza di un autoapprendimento e di una macchina autonoma non dovrebbe essere trattato in modo diverso dall'impiego di un ausiliario umano, se tale assistenza porta a danni a terzi ("principio di equivalenza funzionale"). Tuttavia, almeno in quelle giurisdizioni che considerano la responsabilità sussidiaria una variante della responsabilità per colpa, ritenendo il principale responsabile della violazione di un altro, potrebbe essere difficile identificare il parametro di riferimento in base al quale saranno valutate le operazioni degli aiutanti non umani al fine di rispecchiare l'elemento di cattiva condotta degli ausiliari umani. Il potenziale parametro di riferimento dovrebbe tenere conto del fatto che in molti settori di applicazione gli ausiliari non umani sono più sicuri, che è meno probabile che causino danni agli altri rispetto agli attori umani e che la legge non dovrebbe almeno scoraggiarne l'uso.

Responsabilità rigorosa (strict): In particolare, a partire dal diciannovesimo secolo in poi, i legislatori hanno spesso risposto ai rischi causati dalle nuove tecnologie introducendo una responsabilità rigorosa, sostituendo la nozione di responsabilità per cattiva condotta con responsabilità indipendentemente dalla colpa, collegata a rischi specifici collegati a qualche oggetto o attività ritenuti ammissibili, a scapito di un rischio residuo di danno ad esso collegato.

Finora, queste modifiche alla legge hanno riguardato, ad esempio, mezzi di trasporto (come treni o veicoli a motore), energia (come energia nucleare, linee elettriche) o condotte.

Ancor prima, le leggi sul crimine spesso rispondevano a maggiori rischi spostando l'onere della prova della colpa, rendendo più facile per la vittima avere successo se l'imputato aveva il controllo di particolari fonti di danno come animali o beni immobili difettosi.

Il panorama della responsabilità oggettiva in Europa è piuttosto vario. Alcuni sistemi legali sono restrittivi e hanno fatto un uso molto limitato di tali regimi di responsabilità alternativi (spesso espandendo invece la responsabilità per colpa). Altri sono più o meno generosi, pur non consentendo l'analogia con le responsabilità rigorose definite individualmente (con la sola eccezione dell'Austria). Alcuni Stati membri hanno anche introdotto una regola generale (più o meno ampia) di responsabilità oggettiva, in genere per alcune "attività pericolose", che i tribunali di tali giurisdizioni interpretano in modo abbastanza diverso.

In alcune giurisdizioni, il mantenimento di una cosa innesca una responsabilità oggettiva, che è un altro modo per prevedere una deviazione piuttosto ampia rispetto al classico requisito di colpa.

Le norme esistenti in materia di responsabilità oggettiva per i veicoli a motore (che possono essere riscontrate in molti, ma non in tutti gli Stati membri dell'UE) o gli aeromobili possono anche essere applicate a veicoli o droni autonomi, ma ci sono molte potenziali lacune di responsabilità.

La responsabilità rigorosa per il funzionamento di computer, software o simili è finora ampiamente sconosciuta in Europa, anche se ci sono alcuni esempi limitati in cui i paesi prevedono la responsabilità dell'operatore di alcuni sistemi informatici (tipicamente definiti in modo ristretto), come i database gestiti dallo stato.

Il vantaggio della responsabilità oggettiva per la vittima è evidente, in quanto li esonera dal dover provare qualsiasi illecito all'interno della sfera dell'imputato, nonché il legame causale tra tale illecito e la perdita della vittima, consentendo alla vittima di concentrarsi invece solo sul rischio causato dalla tecnologia materializzata causando loro danni. Tuttavia, si deve tenere presente che spesso le responsabilità rigorose sono associate a limiti di responsabilità o altre restrizioni al fine di controbilanciare il rischio aumentato di responsabilità di coloro che beneficiano della tecnologia. Tali limiti sono spesso ulteriormente giustificati in quanto contribuiscono a rendere assicurabile il rischio, poiché gli statuti di responsabilità rigorosa spesso richiedono un'adeguata copertura assicurativa per i rischi di responsabilità.

Un fattore che qualsiasi legislatore che considera l'introduzione della responsabilità oggettiva dovrà prendere in considerazione è l'effetto che tale introduzione può avere sull'avanzamento della tecnologia,

poiché alcuni potrebbero essere più restii a promuovere attivamente la ricerca tecnologica se il rischio di responsabilità è considerato dissuasivo. D'altra parte, questo presunto effetto agghiacciante della legge sul crimine è ancora più forte fintanto che la questione della responsabilità è del tutto irrisolta e quindi imprevedibile, mentre l'introduzione di una specifica soluzione statutaria almeno più o meno chiaramente delimita i rischi e contribuisce a rendere loro assicurabili.

Responsabilità del prodotto: Per più di 30 anni, il principio della rigida responsabilità del produttore per lesioni personali e danni ai beni di consumo causati da prodotti difettosi è stato una parte importante del sistema europeo di protezione dei consumatori. Allo stesso tempo, l'armonizzazione delle rigorose norme in materia di responsabilità ha contribuito a raggiungere condizioni di parità per i produttori che forniscono i loro prodotti a paesi diversi.

Tuttavia, mentre tutti gli Stati membri dell'UE hanno attuato la direttiva sulla responsabilità da prodotto (PLD), la responsabilità per i prodotti difettosi non è del tutto armonizzata. Oltre alle differenze nell'attuazione della direttiva, gli Stati membri continuano a preservare percorsi alternativi alla compensazione oltre alla rigida responsabilità dei produttori per prodotti difettosi ai sensi del PLD.

Il PLD si basa sul principio secondo cui il produttore (ampiamente definito lungo il canale di distribuzione) è responsabile per i danni causati dal difetto in un prodotto che ha messo in circolazione a fini economici o nel corso della propria attività.

Gli interessi tutelati dal regime europeo di responsabilità da prodotto sono limitati alla vita, alla salute e alla proprietà dei consumatori.

Il PLD è stato redatto sulla base del principio di neutralità tecnologica. Secondo l'ultima valutazione delle prestazioni della direttiva, il suo regime continua a fungere da strumento efficace e contribuisce a migliorare la protezione dei consumatori, l'innovazione e la sicurezza dei prodotti.

Tuttavia, alcuni concetti chiave alla base del regime dell'UE, adottati nel 1985, sono oggi una corrispondenza inadeguata per i potenziali rischi delle tecnologie digitali emergenti.

La progressiva sofisticazione del mercato e la penetrazione pervasiva delle tecnologie digitali emergenti rivelano che alcuni concetti chiave richiedono chiarimenti. Questo perché gli aspetti chiave del regime di responsabilità del PLD sono stati progettati tenendo conto dei prodotti e dei modelli di business tradizionali: oggetti materiali immessi sul mercato da un'azione una tantum del produttore, dopo di che il produttore non mantiene il controllo sul prodotto . Le tecnologie digitali emergenti mettono alla prova l'attuale regime di

responsabilità da prodotto sotto diversi aspetti per quanto riguarda le nozioni di prodotto, difetto e produttore.

L'ambito di applicazione del regime di responsabilità del prodotto si basa sul concetto di prodotto. Ai fini della direttiva, i prodotti sono definiti oggetti mobili, anche se incorporati in un altro oggetto mobile o immobile, e comprendono l'elettricità. Finora, la distinzione di prodotti e servizi non ha incontrato difficoltà insormontabili. Tuttavia, le tecnologie digitali emergenti, in particolare i sistemi di intelligenza artificiale, sfidano questa chiara distinzione e sollevano domande aperte. Nei sistemi di intelligenza artificiale, i prodotti e i servizi interagiscono in modo permanente e una separazione netta tra loro è impossibile. È anche discutibile se il software sia coperto dal concetto legale di prodotto o componente del prodotto. Si discute in particolare se la risposta debba essere diversa per il software incorporato e non incorporato, compresi gli aggiornamenti software via etere o altri feed di dati. In ogni caso, laddove tali aggiornamenti o altri feed di dati siano forniti al di fuori del SEE, la vittima potrebbe non avere nessuno a cui rivolgersi all'interno del SEE, poiché in genere non vi sarà un importatore intermediario domiciliato all'interno del SEE nel caso di download diretti .

Il secondo elemento chiave del regime di responsabilità del prodotto è la nozione di difetto. La difettosità viene valutata sulla base delle aspettative di sicurezza di un consumatore medio, tenendo conto di tutte le circostanze rilevanti. L'interconnettività di prodotti e sistemi rende difficile identificare la difettosità. Sofisticati sistemi autonomi di intelligenza artificiale con capacità di autoapprendimento sollevano anche la questione se le deviazioni imprevedibili nel percorso decisionale possano essere

trattati come difetti. Anche se costituiscono un difetto, può essere applicata la difesa più avanzata. Inoltre, la complessità e l'opacità delle tecnologie digitali emergenti complicano le possibilità per la vittima di scoprire e provare il difetto e provare la causa.

Dato che il PLD si concentra sul momento in cui il prodotto è stato messo in circolazione come punto di svolta fondamentale per la responsabilità del produttore, ciò interrompe le richieste per qualsiasi cosa il produttore possa successivamente aggiungere tramite qualche aggiornamento o upgrade. Inoltre, il PLD non prevede alcun obbligo di controllo dei prodotti dopo averli messi in circolazione.

I sistemi di intelligenza artificiale altamente sofisticati potrebbero non essere prodotti finiti immessi sul mercato in modo tradizionale. Il produttore può mantenere un certo controllo sull'ulteriore sviluppo del prodotto sotto forma di aggiunte o aggiornamenti dopo la circolazione. Allo stesso tempo, il controllo del produttore può essere limitato e non esclusivo se l'operazione del prodotto richiede dati forniti da terze parti o raccolti dall'ambiente e dipende dai processi di autoapprendimento e dalla personalizzazione delle impostazioni scelte dall'utente. Ciò diluisce il ruolo tradizionale di un produttore, quando una moltitudine di attori contribuisce alla progettazione, al funzionamento e all'uso del prodotto / sistema di intelligenza artificiale.

Ciò è collegato ad un'altra limitazione di responsabilità: la maggior parte degli Stati membri ha adottato la cosiddetta difesa dal rischio di sviluppo, che consente al produttore di evitare la responsabilità se lo stato delle conoscenze scientifiche e tecniche al momento in cui ha messo in circolazione il prodotto non era tale per consentire di scoprire l'esistenza del difetto (articolo 7 lit. e PLD). La difesa può diventare molto più importante praticamente per quanto riguarda i sofisticati prodotti basati sull'intelligenza artificiale.

È stato menzionato che il regime PLD protegge la vita, la salute e la proprietà dei consumatori.

Per quanto riguarda quest'ultimo, non è chiaro se copre danni ai dati, dal momento che i dati potrebbero non essere un "oggetto di proprietà" ai sensi dell'articolo 9 lit. b PLD.

Condotta contributiva: Mentre il bilanciamento della responsabilità alla luce della condotta della vittima che contribuisce al loro danno non solleva nuovi problemi nell'era delle tecnologie digitali emergenti, si dovrebbe tenere presente che tutte le sfide sopra elencate in relazione al torturatore si applicano corrispondentemente alla vittima.

Ciò è particolarmente vero se la vittima è stata coinvolta o ha in qualche modo beneficiato del funzionamento di alcuni sistemi intelligenti o altri dispositivi digitalizzati interconnessi, ad es. installando (o non installando) gli aggiornamenti, modificando le impostazioni di sistema predefinite o aggiungendo il proprio contenuto digitale. Oltre alle collisioni di veicoli autonomi, altri esempi evidenti includono il proprietario della casa che non riesce a installare correttamente e combinare più componenti di un sistema di casa intelligente nonostante le istruzioni adeguate. Nel primo caso, si incontrano due rischi simili, mentre nel secondo i rischi di una tecnologia digitale emergente devono essere ponderati rispetto al mancato rispetto degli standard di cura previsti.

Prescrizione: Sebbene vi sia una certa tendenza in tutta Europa a riformare le leggi in materia di prescrizione di richieste di risarcimento per illecito, non è problematico applicare queste regole a scenari che coinvolgono tecnologie digitali emergenti. Tuttavia, si dovrebbe essere consapevoli del fatto che, in particolare nelle giurisdizioni in cui il periodo di prescrizione è relativamente breve, le complessità di queste tecnologie, che possono ritardare il processo di accertamento dei fatti, possono essere contrarie agli interessi della vittima tagliando prematuramente il reclamo, prima la tecnologia potrebbe essere identificata come la fonte del suo danno.

Sfide procedurali: Oltre ai problemi del diritto illecito sostanziale già indicato, l'applicazione dei quadri di responsabilità nella pratica è anche interessata da sfide nel campo del diritto procedurale. Considerando la tendenza dell'esperienza della giurisprudenza in alcuni Stati membri ad alleviare l'onere di provare il nesso di causalità in determinate questioni complesse (come la negligenza medica), si potrebbe facilmente prevedere che i tribunali potrebbero sostenere allo stesso modo le vittime di tecnologie digitali emergenti che hanno difficoltà dimostrando che la tecnologia in questione era la vera causa del loro danno. Tuttavia, è probabile che ciò differisca da caso a caso e sicuramente da uno Stato membro all'altro. Per quanto riguarda le questioni puramente procedurali, potrebbero esserci anche problemi, poiché concetti di diritto procedurale ben consolidati come prove prima facie possono essere difficili da applicare a situazioni che coinvolgono sviluppi tecnologici emergenti.

Le conseguenti differenze nell'esito dei casi derivanti da differenze nelle legislazioni procedurali degli Stati membri possono essere alleviate almeno in parte armonizzando le norme sull'onere della prova.

Assicurazione: Un regime assicurativo obbligatorio per alcune categorie di AI / robot è stato proposto come possibile soluzione al problema di allocazione della responsabilità per danni causati da tali sistemi (talvolta combinato con fondi di compensazione per danni non coperti da polizze assicurative obbligatorie).

Tuttavia, un regime assicurativo obbligatorio non può essere considerato l'unica risposta al problema di come assegnare la responsabilità e non può sostituire completamente le regole di responsabilità chiare ed eque. Le compagnie di assicurazione fanno parte dell'intero ecosistema sociale e hanno bisogno di regole di responsabilità per proteggere i propri interessi in relazione ad altre entità (diritti di ricorso). Inoltre, al fine di mantenere le tecnologie digitali emergenti il più sicure possibile e, quindi, degne di fiducia, l'assicurazione dovrebbe essere influenzata il meno possibile. Allo stesso tempo, tuttavia, è necessario assicurare casi di rischio molto elevato o catastrofico al fine di garantire un risarcimento per danni potenzialmente gravi.

Quindi, la domanda riguarda se un'assicurazione di prima o terza parte, o una combinazione di entrambi, dovrebbe essere richiesta o almeno raccomandata e in quali casi.

Attualmente, il diritto dell'UE richiede un'assicurazione di responsabilità obbligatoria (di terzi) ad es. per l'uso di autoveicoli, vettori aerei e operatori aerei o vettori di passeggeri via mare.

Le leggi degli Stati membri richiedono un'assicurazione obbligatoria di responsabilità civile in vari altri casi, per lo più abbinata a regimi di responsabilità rigorosa o all'esercizio di determinate professioni.

Nuove polizze assicurative opzionali (ad es. Cyber-insurance) sono offerte a coloro che sono interessati a coprire i rischi sia di prima che di terzi. Nel complesso, il mercato assicurativo è piuttosto eterogeneo e può adattarsi alle esigenze di tutte le parti interessate. Tuttavia, questa eterogeneità, combinata con una molteplicità di attori coinvolti in una domanda di risarcimento assicurativo, può comportare costi amministrativi elevati sia da parte delle compagnie assicurative che dei potenziali imputati, il lungo trattamento dei crediti assicurativi e l'imprevedibilità del risultato finale per le parti coinvolti.

Gli assicuratori utilizzano tradizionalmente i dati storici sui sinistri per valutare la frequenza e la gravità del rischio. In futuro, guadagneranno terreno sistemi più complessi, che utilizzano profili di rischio altamente granulari basati sull'analisi dei dati, anche mediante l'analisi dei dati registrati o trasmessi in streaming in tempo reale. Alla luce di ciò, la questione dell'accesso ai dati per le compagnie di assicurazione è molto pertinente.

Anche l'efficienza in termini di costi del processo di reclamo è una considerazione importante.

Prospettive di responsabilità per le tecnologie digitali emergenti:

La promessa di benefici e notevoli opportunità per la società rese possibili da una moltitudine di usi e applicazioni delle tecnologie digitali emergenti è incontestabile. Nonostante questi indiscutibili guadagni, l'uso pervasivo di sistemi e combinazioni di tecnologie sempre più sofisticati, in molteplici settori economici e contesti sociali, crea rischi e può causare perdite. L'adeguatezza degli attuali regimi giuridici di responsabilità in Europa per compensare completamente i danni causati da queste tecnologie è tuttavia discutibile.

A tal fine, alcuni concetti chiave alla base dei regimi di responsabilità classici richiedono un chiarimento giuridico. Inoltre, per far fronte ad alcune situazioni, potrebbe essere necessaria la formulazione di regole, principi e concetti specifici per adeguare i regimi di responsabilità legale alle nuove realtà.

Sfide delle tecnologie digitali emergenti per la legge sulla responsabilità ([1] - [2] VEDI SOPRA):

La digitalizzazione è cambiata e sta ancora cambiando il mondo. La legge sulla responsabilità nelle giurisdizioni europee si è evoluta nel corso di molti secoli ed è già sopravvissuta a molti sviluppi dirompenti. Non sorprende quindi che, in linea di principio, la legge sulla responsabilità è in grado di far fronte anche alle tecnologie digitali emergenti. Tuttavia, ci sono alcuni cambiamenti fondamentali, ognuno dei quali può essere solo di natura graduale, ma la cui dimensione e l'effetto combinato si traducono in perturbazioni***.***

a) ***Complessità:*** l'hardware moderno può essere un composto di più parti la cui interazione richiede un alto livello di sofisticazione tecnica. Combinandolo con una percentuale crescente di componenti digitali, compresa l'intelligenza artificiale, rende tale tecnologia ancora più complessa e la sposta lontano dagli archetipi di fonti potenzialmente dannose su cui si basano le norme di responsabilità esistenti. Laddove, ad esempio, un AV interagisce con altri AV, un'infrastruttura stradale connessa e vari servizi cloud, può essere sempre più difficile scoprire da dove provenga un problema e cosa alla fine abbia causato un incidente. La pluralità di attori negli ecosistemi digitali rende sempre più difficile scoprire chi potrebbe essere responsabile del danno causato.
   Un'altra dimensione di questa complessità è la complessità interna degli algoritmi coinvolti.
b) ***Opacità:*** più le tecnologie digitali emergenti diventano più complesse, meno coloro che traggono vantaggio dalle loro funzioni o che sono esposte a esse possono comprendere i processi che

potrebbero aver causato danni a sé stessi o agli altri. Gli algoritmi spesso non arrivano più come codice più o meno facilmente leggibile, ma come una scatola nera che si è evoluta attraverso l'autoapprendimento e che potremmo essere in grado di testare sui suoi effetti, ma non tanto da capire. È quindi sempre più difficile per le vittime identificare tali tecnologie come una possibile fonte di danno, per non parlare del motivo per cui l'hanno causato. Una volta che una vittima ha reclamato con successo i danni di un torturatore, il torturatore potrebbe avere difficoltà simili a livello di riparazione.

c) ***Apertura:*** le tecnologie digitali emergenti non vengono completate una volta messe in circolazione, ma per loro natura dipendono da input successivi, in particolare aggiornamenti o upgrade più o meno frequenti. Spesso devono interagire con altri sistemi o fonti di dati per funzionare correttamente. Pertanto, devono rimanere aperti in base alla progettazione, ovvero consentire l'ingresso esterno tramite una spina hardware o tramite una connessione wireless e diventare combinazioni ibride di hardware, software, aggiornamenti software continui e vari servizi continui. Questo passaggio dalla nozione classica di prodotto completato in un determinato momento alla fusione di prodotti e servizi in corso ha un impatto considerevole, tra l'altro, sulla responsabilità del prodotto.
d) ***Autonomia:*** le nuove tecnologie emergenti svolgono sempre più compiti con meno, o completamente senza, controllo o supervisione umana. Sono essi stessi in grado di alterare gli algoritmi iniziali a causa delle capacità di autoapprendimento che elaborano i dati esterni raccolti nel corso dell'operazione. La scelta di tali dati e il grado di impatto che ha sul risultato è costantemente adattato dagli stessi algoritmi in evoluzione.
e) ***Prevedibilità:*** molti sistemi sono progettati non solo per rispondere a stimoli predefiniti, ma per identificarne e classificarne di nuovi e collegarli a una reazione corrispondente auto-scelta che non è stata pre-programmata come tale. Più sistemi di dati esterni sono in grado di elaborare e più sono dotati di un'IA sempre più sofisticata, più è difficile prevedere l'impatto preciso che avranno una volta in funzione.
f) ***Determinazione dei dati (Data – Driveness):*** le tecnologie digitali emergenti dipendono sempre più da informazioni esterne che non sono preinstallate, ma generate da sensori integrati o comunicate dall'esterno, da fonti di dati regolari o da fornitori ad hoc. I dati necessari per il loro corretto funzionamento possono, tuttavia, essere imperfetti o mancanti del tutto, a causa di errori di comunicazione o problemi della fonte di dati esterna, a causa di difetti dei sensori interni o degli algoritmi integrati progettati per analizzare, verificare ed elaborare tali dati.
g) ***Vulnerabilità:*** le tecnologie digitali emergenti sono generalmente soggette ad aggiornamenti più o meno frequenti e operano in interazione più o meno costante con informazioni esterne. Le funzionalità integrate che consentono l'accesso a tali input rendono queste tecnologie particolarmente vulnerabili alle violazioni della sicurezza informatica. Ciò può causare il malfunzionamento del sistema stesso e / o modificarne le caratteristiche in modo tale da causare danni.

Impatto di queste sfide e necessità di intervento ([3] - [4] VEDI SOPRA):

I regimi di responsabilità esistenti in tutti gli Stati membri già adesso forniscono risposte alla domanda se la vittima di qualsiasi rischio che si materializza possa chiedere un risarcimento da un altro, ea quali condizioni.

Tuttavia, queste risposte potrebbero non essere sempre soddisfacenti quando il danno è causato dalle tecnologie digitali emergenti date le sfide e per vari motivi.

Uno dei motivi per cui le norme esistenti in materia di responsabilità possono produrre risultati insoddisfacenti è che la perdita derivante dalle tecnologie digitali emergenti non è assegnata alla parte che è la più appropriata per sopportarla. Come regola generale, la perdita ricade normalmente sulla vittima stessa (casum sentit dominus) a meno che non vi sia una ragione convincente per trasferirla a un'altra parte alla quale la perdita può essere attribuita. I motivi per l'attribuzione della perdita a un'altra parte variano a

seconda del tipo di responsabilità in gioco. Sotto la responsabilità fondata sulla colpa, il punto cruciale è che il comportamento discutibile ed evitabile del torturatore ha causato il danno, che a sua volta si traduce sia in un argomento di giustizia correttiva che in un argomento sul fornire i giusti incentivi per evitare danni.

In molti regimi di responsabilità oggettiva, i punti cardine sono beneficio e controllo, vale a dire che la persona responsabile espone gli altri ai rischi di un'attività di cui la persona responsabile ha beneficiato e che era sotto il suo controllo. Ciò si traduce nuovamente in argomenti sia sulla giustizia correttiva che sui giusti incentivi. L'analisi economica ha ridefinito questi elementi ponendo l'accento sull'evitatore del costo più economico o sull'assicuratore più economico dell'assicurazione, con l'evitatore del costo più economico che di solito è proprio la persona che potrebbe semplicemente desistere da un comportamento discutibile o che controlla un rischio e la sua entità.

> ***Illustrazione 2.*** *Per i veicoli stradali tradizionali, era il singolo proprietario (O) che era la persona più adatta a essere responsabile, in cui i danni erano causati dall'operazione del veicolo. Indipendentemente dal fatto che il danno sia stato causato o meno dall'intenzione o dalla negligenza di O, è stato sicuramente O a beneficiare dell'operazione in generale, che ha avuto il grado elevato di controllo del rischio decidendo quando, dove e come utilizzare, mantenere e riparare il veicolo, e quindi anche il più economico evitatore e beneficiario dell'assicurazione. Laddove i moderni veicoli autonomi (AV) sono di proprietà privata, è ancora il singolo proprietario che decide quando utilizzare l'AV e inserisce la destinazione nel sistema, ma tutte le altre decisioni (percorso, velocità ecc.) Sono prese da algoritmi forniti dal produttore (P) dell'AV o un terzo che agisce per conto di P. P è anche responsabile della manutenzione del veicolo. P può quindi essere la persona molto più appropriata ad essere responsabile di O.*

Le norme esistenti in materia di responsabilità possono anche portare a risultati inappropriati per motivi legati più alla coerenza e alla coerenza, in particolare tenendo conto del principio di equivalenza funzionale, come ad esempio quando un risarcimento viene negato in una situazione che coinvolge tecnologie digitali emergenti quando vi sarebbe un risarcimento in un situazione funzionalmente equivalente che coinvolge condotta umana e tecnologia convenzionale.

> ***Illustrazione 3.*** *L'ospedale H utilizza un robot chirurgico basato sull'intelligenza artificiale. Nonostante il fatto che H e il suo personale abbiano assolto tutti i possibili doveri di cura, il paziente è danneggiato a causa di un malfunzionamento del robot che nessuno avrebbe potuto prevedere e che non è correlato alla condizione in cui il robot è stato spedito. Se P non fosse indennizzato per il danno che ne deriva, ciò sarebbe incompatibile con l'esito della situazione funzionalmente equivalente in cui H ha assunto un medico umano ed è responsabile della sua condotta comparabile secondo le norme nazionali sulla responsabilità vicaria (vedi C.8).*

L'applicazione delle tradizionali regole di responsabilità può anche portare a risultati insoddisfacenti perché, mentre teoricamente la vittima potrebbe ricevere un risarcimento, le controversie sarebbero indebitamente onerose e costose, lasciandole senza un effettivo accesso alla giustizia. Questo può accadere se i requisiti di responsabilità che dovrebbero dimostrare o sono del tutto inadatti al rischio rappresentato dalle tecnologie digitali emergenti o troppo difficili da stabilire. Lasciare la vittima incompensata o non compensata in tali casi può essere indesiderabile, in quanto può privare efficacemente la vittima della protezione di base per quanto riguarda i suoi significativi interessi legalmente protetti (come la vita, la salute, l'integrità fisica e la proprietà o altri diritti importanti).

In molte situazioni, un risultato particolare non è soddisfacente per due o più dei motivi sopra indicati.

È chiaro fin dall'inizio che nessuna soluzione unica può essere (o dovrebbe) essere offerta. Invece, è necessario considerare una gamma di opzioni, con la scelta all'interno di quella gamma da determinare da vari fattori. Vari argomenti politici hanno dimostrato che la responsabilità rigorosa dell'operatore di alcune tecnologie digitali emergenti può essere giustificata, dati gli interessi in competizione tra detto operatore e la vittima, nonché le alternative della vittima all'ottenimento di un risarcimento ([9] - [12]) . Nel caso di un difetto del prodotto, il produttore di quel prodotto può essere il destinatario appropriato di reclami derivanti da tali difetti ([13] - [15]). Tuttavia, adattando la nozione di responsabilità per colpa specificando ulteriori obblighi di diligenza ([16] - [17]) o spostando l'onere della prova della colpa ([22] (b), [24] (b), [27]), ad esempio, potrebbe già risolvere gli effetti dirompenti delle tecnologie digitali emergenti nel campo del diritto illecito, se necessario e del tutto opportuno. Le lacune rimanenti possono spesso essere colmate estendendo la responsabilità vicaria all'uso della tecnologia autonoma al posto degli ausiliari umani ([18]). Se ci sono difficoltà pratiche sistemiche nel dimostrare la causalità e altri fattori, potrebbe essere necessario apportare alcune modifiche al riguardo ([22], [24], [25] - [26], [29] - [30]). In alcuni casi può essere necessario un obbligo di assicurazione per garantire che le vittime ottengano un risarcimento ([33]). Anche i fondi di compensazione possono svolgere un ruolo complementare ([34]).

Basi di responsabilità ([5] - [7]): Nella maggior parte dei casi, anche con le tecnologie digitali emergenti, può essere invocata più di una base di responsabilità se i rischi che ne derivano si materializzano. Queste basi di responsabilità possono essere disponibili in tutto o in parte alla vittima immediata o alle varie parti coinvolte. Ciò solleva la questione se la prima persona che ha pagato il risarcimento alla vittima possa recuperare almeno una parte del pagamento del risarcimento da un'altra parte.

> ***Illustrazione 4***. *Ad esempio, se l'operatore di un veicolo autonomo (O) è ritenuto responsabile per eventuali perdite causate dal suo funzionamento, ma anche il produttore del veicolo autonomo (P) è responsabile perché l'incidente è stato causato da un difetto del prodotto , O può trasferire parte o tutto quel rischio a livello di ricorso a P, se è O, o l'assicuratore di O, che ha pagato i danni alla vittima in primo luogo.*

Tracciare il confine tra responsabilità civile e responsabilità contrattuale è spesso difficile. Ciò diventa tanto più importante nelle giurisdizioni che non consentono richieste simultanee in entrambi i regimi, come la Francia.

Le giurisdizioni che consentono richieste simultanee tendono a superare le carenze del diritto illecito spostando i casi illeciti nel regno della responsabilità contrattuale, ad esempio creando obbligazioni quasi-contrattuali con l'obiettivo primario di consentire ai beneficiari di tali obblighi di avvalersi dei benefici di un richiedente contrattuale.

Tuttavia, esiste sempre un gruppo limitato di vittime che beneficiano di tali teorie contrattuali e le vittime che esulano dal campo di applicazione possono ancora incontrare gravi difficoltà.

Nella misura in cui le vittime delle tecnologie digitali emergenti hanno già pretese in base a tali teorie contrattuali, il divario di responsabilità creato dagli effetti dirompenti di queste tecnologie può essere ridotto o addirittura inesistente, almeno per quanto riguarda le vittime immediate dei rischi del tecnologie in questione. Tuttavia, coloro che pagano loro un risarcimento in base alla responsabilità contrattuale possono comunque voler ricorrere contro, ad esempio, il produttore del prodotto che hanno venduto, causando danni ai propri clienti o utenti.

La disponibilità di un reclamo contrattuale di ricorso contro un'altra parte può anche entrare in gioco nel decidere se la parte in questione possa essere o meno il destinatario appropriato della domanda di risarcimento per illecito della vittima.

In alcuni scenari di danno, come l'assistenza sanitaria, potrebbero esistere altri sistemi per proteggere le vittime immediate. Questo deve essere preso in considerazione quando si determina in che misura (e dove esattamente) le tecnologie digitali emergenti pongono sfide ai regimi di responsabilità esistenti.

Personalità giuridica ([8] VEDI SOPRA):

Nel corso degli anni, ci sono state molte proposte per estendere un qualche tipo di personalità giuridica alle tecnologie digitali emergenti, alcune addirittura risalenti al secolo scorso.

In tempi recenti, il rapporto del PE su "Norme di diritto civile sulla robotica" ha invitato la Commissione a creare uno strumento legislativo per affrontare la responsabilità causata dai robot. Ha inoltre chiesto alla Commissione di considerare "uno status giuridico specifico per i robot", "eventualmente l'applicazione della personalità elettronica", come una soluzione di responsabilità.

Anche in una forma così provvisoria, questa proposta si è rivelata molto controversa.

La personalità giuridica si presenta in molte forme, anche per le persone fisiche, come i bambini, che possono essere trattate diversamente dagli adulti. La classe più nota di persone diverse dalle persone fisiche, corporazioni, ha a lungo goduto solo di una serie limitata di diritti e obbligazioni che consente loro di fare causa e essere citati in giudizio, stipulare contratti, incorrere in debiti, proprietà proprie ed essere condannati per crimini . Dare una personalità giuridica ai robot o all'intelligenza artificiale non richiederebbe l'inserimento di tutti i diritti delle persone fisiche o delle società. Teoricamente, una personalità giuridica potrebbe consistere esclusivamente in obblighi.

Una soluzione del genere, tuttavia, non sarebbe praticamente utile, poiché la responsabilità civile è una responsabilità patrimoniale, che richiede al suo portatore di avere beni.

Tuttavia, gli esperti ritengono che attualmente non sia necessario dare una personalità giuridica alle tecnologie digitali emergenti. I danni causati da tecnologie anche completamente autonome sono generalmente riducibili ai rischi attribuibili a persone fisiche o categorie di persone giuridiche esistenti e, in caso contrario, le nuove leggi rivolte alle persone fisiche sono una risposta migliore rispetto alla creazione di una nuova categoria di persona giuridica.

Qualsiasi tipo di personalità giuridica per le tecnologie digitali emergenti può sollevare una serie di questioni etiche. Ancora più importante, avrebbe senso percorrere questa strada solo se aiutasse i sistemi legali ad affrontare le sfide delle tecnologie digitali emergenti.

Ogni ulteriore personalità dovrebbe andare di pari passo con i fondi assegnati a tali persone elettroniche, in modo che i reclami possano essere effettivamente promossi nei loro confronti. Ciò equivarrebbe a mettere un limite alla responsabilità e - come ha dimostrato l'esperienza con le società - i successivi tentativi di aggirare tali restrizioni perseguendo pretese nei confronti di persone fisiche o giuridiche alle quali è possibile attribuire persone elettroniche, "perforando efficacemente il velo elettronico".

Inoltre, al fine di dare una dimensione reale alla responsabilità, gli agenti elettronici dovrebbero essere in grado di acquisire attività da soli.

Ciò richiederebbe la risoluzione di numerosi problemi legislativi relativi alla loro capacità giuridica e al modo in cui agiscono quando effettuano transazioni legali.

> ***Illustrazione 5.*** *Immagina che la responsabilità di un'auto completamente autonoma fosse sull'auto anziché sul suo operatore. Le vittime di incidenti riceveranno un risarcimento solo se viene stipulata un'assicurazione per l'auto e qualcuno (chi?) Paga i premi, o se qualcuno (chi?) Fornisce all'auto beni con i quali si potrebbero risarcire i danni. Se tali beni non fossero sufficienti per compensare completamente le vittime di un incidente, le vittime avrebbero un*

forte incentivo a chiedere un risarcimento alla persona che beneficia del funzionamento dell'auto. Se le attività dell'auto fossero sufficienti a pagare lo stesso livello di indennizzo previsto dai regimi di responsabilità e assicurazioni esistenti, non ci sarebbe motivo di discussione, ma in tal caso, dare alla macchina una personalità giuridica sarebbe una mera formalità e non cambierebbe realmente la situazione.

Gli esperti desiderano tuttavia sottolineare che guardano solo al lato della responsabilità delle cose e non assumono alcun tipo di posizione sul futuro sviluppo del diritto societario, ad esempio se un'intelligenza artificiale possa agire come membro di un consiglio di amministrazione.

Responsabilità rigorosa dell'operatore ([9] - [12] VEDI SOPRA):

Le rigide norme di responsabilità esistenti negli Stati membri possono già applicarsi alle tecnologie digitali emergenti.

Il miglior esempio di ciò sono i regimi di responsabilità per i veicoli a motore che molto probabilmente si applicheranno già alle auto autonome o agli aeromobili (che potrebbero già includere almeno alcuni droni). Tuttavia, la situazione in Europa varia ancora molto. Alcune giurisdizioni hanno clausole generali più o meno generose, o almeno consentono l'analogia con i regimi legali esistenti, mentre altre fanno a meno dei requisiti di colpa solo in pochissime situazioni strettamente definite, ma spesso espandono la nozione di colpa. La responsabilità rigorosa si applica in genere solo in caso di danni fisici a persone o cose, ma non per pura perdita economica. Anche nella stessa giurisdizione, ci possono essere differenze considerevoli tra i vari regimi di responsabilità rigorosa, come dimostrato dalla vasta gamma di difese disponibili per la persona responsabile o dalla scelta del legislatore a favore o contro i limiti.

Il semplice fatto che la tecnologia sia nuova non è una giustificazione sufficiente per introdurre una responsabilità rigorosa.

Tuttavia, anche le tecnologie digitali emergenti che in genere possono causare danni significativi comparabili ai rischi già soggetti a responsabilità oggettiva dovrebbero essere soggette a responsabilità oggettiva.

Questo perché le vittime dovrebbero essere trattate allo stesso modo se sono esposte e alla fine danneggiate da pericoli simili.

Per il momento, questo vale principalmente per le tecnologie digitali emergenti che si muovono negli spazi pubblici, come veicoli, droni o simili. Gli elettrodomestici intelligenti non saranno in genere candidati idonei per la responsabilità oggettiva. Sono in particolare gli oggetti di un certo peso minimo, mossi ad una certa velocità minima, che sono candidati per basi aggiuntive di responsabilità oggettiva, come i robot di consegna o di pulizia guidati dall'intelligenza artificiale, almeno se sono operati in aree dove altri potrebbero essere esposto a rischio. Una responsabilità rigorosa potrebbe non essere appropriata per i robot puramente fissi (ad es. Robot chirurgici o industriali), anche se guidati dall'intelligenza artificiale, che sono impiegati esclusivamente in un ambiente ristretto, con una ristretta gamma di persone esposte al rischio, che inoltre sono protette da un diverso - incluso il contratto - regime (nelle figure seguenti, pazienti protetti da responsabilità contrattuale o personale di fabbrica coperto da schemi di indennizzo degli operai).

Illustrazione 6. *I sensori che controllano il percorso di un robot guidato dall'intelligenza artificiale che trasporta componenti pesanti in caso di malfunzionamento della Fabbrica F, facendo sì che il robot lasci il percorso previsto, esce dalla fabbrica e si imbatte in passante P per strada. Anche se in questo caso potrebbero non essere applicabili le norme vigenti in materia di responsabilità oggettiva dei veicoli a motore, P dovrebbe comunque essere in grado di chiedere un risarcimento a F senza dover dimostrare che F o uno dei suoi dipendenti sono in errore.*

Se viene raggiunta la soglia di rischio pertinente per una tecnologia digitale emergente e sembra pertanto opportuno subordinare il funzionamento di questa tecnologia a un regime di responsabilità rigoroso, detto regime dovrebbe condividere le stesse caratteristiche di altre passività senza colpa per rischi comparabili.

Ciò vale anche per la questione di quali perdite siano recuperabili in quale misura, incluso se si debbano introdurre limiti e se il danno non pecuniario è recuperabile.

L'introduzione di una responsabilità oggettiva dovrebbe offrire alle vittime un accesso più facile al risarcimento, senza ovviamente escludere una richiesta di responsabilità in caso di colpa parallela se i suoi requisiti sono soddisfatti.

Inoltre, mentre la responsabilità rigorosa in genere incanalerà la responsabilità sulla persona responsabile (ad esempio, l'operatore della tecnologia), questa persona si riserva il diritto di ricorrere a terzi che contribuiscono al rischio, come il produttore.

Gli esperti hanno ampiamente discusso se la responsabilità rigorosa per le tecnologie digitali emergenti dovrebbe piuttosto essere a carico del proprietario / utente / custode della tecnologia piuttosto che del suo produttore. È stato sottolineato, in particolare nel contesto delle auto autonome, che mentre la stragrande maggioranza degli incidenti era causata da errori umani in passato, la maggior parte degli incidenti sarà causata dal malfunzionamento della tecnologia in futuro (anche se non necessariamente dell'auto autonoma stessa).

Ciò a sua volta potrebbe significare che in primo luogo non sarebbe appropriato ritenere il proprietario / utente / custode strettamente responsabile, poiché è il produttore il più economico a evitare i costi e che è principalmente in grado di controllare il rischio di incidenti . D'altra parte, è ancora il proprietario / utente / custode che decide quando, dove e per quali scopi viene utilizzata la tecnologia e che beneficia direttamente del suo utilizzo. Inoltre, se la responsabilità rigida per il funzionamento della tecnologia (oltre alla responsabilità del prodotto) fosse a carico del produttore, il costo dell'assicurazione verrebbe comunque trasferito ai proprietari attraverso il meccanismo dei prezzi.

A conti fatti, l'NTF del gruppo di esperti non considera utili i concetti tradizionali di proprietario / utente / custode nel contesto delle tecnologie digitali emergenti. Preferiscono piuttosto il concetto più neutro e flessibile di "operatore", che si riferisce alla persona che ha il controllo del rischio connesso al funzionamento delle tecnologie digitali emergenti e che beneficia del successo. Il "controllo" è un concetto variabile, tuttavia, che va dalla semplice attivazione della tecnologia, esponendo così i terzi ai suoi potenziali rischi, alla determinazione dell'output o del risultato (come l'inserimento della destinazione di un veicolo o la definizione delle attività successive di un robot) e possono includere ulteriori passaggi tra loro, che influiscono sui dettagli dell'operazione dall'inizio alla fine. Tuttavia, più un sistema è sofisticato e autonomo, meno qualcuno esercita un effettivo "controllo" sui dettagli dell'operazione e la definizione e l'influenza degli algoritmi, ad esempio mediante aggiornamenti continui, può avere un impatto maggiore rispetto all'avvio del sistema.

Con le tecnologie digitali emergenti, spesso c'è più di una sola persona che può, in modo significativo, essere considerata "operativa" la tecnologia. Il proprietario / utente / custode può utilizzare la tecnologia sul front-end, ma spesso esiste anche un fornitore di back-end centrale che, su base continua, definisce le caratteristiche della tecnologia e fornisce servizi di supporto back-end essenziali. Questo operatore di back-end può avere un alto grado di controllo sui rischi operativi a cui sono esposti gli altri. Da un punto di vista economico, anche l'operatore backend beneficia dell'operazione, poiché tale operatore beneficia dei dati generati dall'operazione o la remunerazione dell'operatore è calcolata direttamente sulla base della durata, della natura continua o dell'intensità dell'operazione, oppure perché un pagamento una tantum ricevuto da questo operatore di backend riflette la durata complessiva stimata, la natura continua e l'intensità dell'operazione.

Illustrazione 7. *Un AV può essere di proprietà privata di una persona che decide se utilizzare l'AV per lo shopping o per un viaggio di lavoro e con quale frequenza, quando e dove. Questo individuo è l'operatore frontend. Anche il produttore dell'AV o di un altro fornitore di servizi controlla continuamente l'AV, ad es. fornendo continuamente servizi di navigazione nel cloud, aggiornando continuamente i dati delle mappe o il software AV a seguito dell'apprendimento automatico della flotta controllata e decidendo quando l'AV ha bisogno di quale tipo di manutenzione. Questa persona è l'operatore back-end. Naturalmente l'operatore frontend e backend può anche essere la stessa persona, ad esempio in uno schema di "mobilità come servizio" (MaaS), in cui un AV è gestito da un operatore di flotta che è anche l'operatore backend.*

Laddove vi sia più di un operatore, come un frontend e un operatore di backend, gli esperti ritengono che la responsabilità rigorosa debba incombere su chi ha maggiore controllo sui rischi posti dall'operazione. Mentre sia il controllo che i benefici sono decisivi per qualificare una persona come operatore, il beneficio è spesso molto difficile da quantificare, quindi fare affidamento solo sui benefici in quanto il fattore decisivo per decidere chi, su due operatori, dovrebbe essere responsabile, porterebbe a incertezza.

Molto spesso, l'operatore frontend avrà un maggiore controllo, ma laddove le tecnologie digitali emergenti si focalizzeranno maggiormente sul backend, potrebbero esserci casi in cui un tale controllo continuo sulla tecnologia rimane con l'operatore backend che - nonostante il fatto che la tecnologia sia venduta a singoli proprietari: è più convincente ritenere responsabile l'operatore di back-end in quanto persona principalmente in grado di controllare, ridurre e assicurare i rischi associati all'uso della tecnologia.

Idealmente, al fine di evitare incertezze, il legislatore dovrebbe definire quale operatore è responsabile in quali circostanze e tutte le altre questioni che devono essere regolamentate (ad esempio in materia di assicurazioni). Ad esempio, il legislatore potrebbe decidere che per gli AV con un livello di automazione di 4 o 5, è il fornitore che gestisce il sistema e che entra nell'AV nel registro nazionale che è responsabile. Questo fornitore pertanto stipulerebbe anche un'assicurazione e potrebbe trasferire i premi attraverso le tasse pagate per i suoi servizi. Laddove diversi provider svolgono la funzione di operatori di backend, uno di essi dovrebbe essere designato come operatore responsabile per ogni AV.

Ciò che è stato detto finora può, nella maggior parte degli Stati membri, essere ampiamente attuato mediante una semplice estensione dei sistemi esistenti di responsabilità oggettiva. Tuttavia, poiché tali sistemi sono oggi presenti in molti Stati membri, includono una serie di difese, eccezioni ed esclusioni che potrebbero non essere appropriate per le tecnologie digitali emergenti, poiché riflettono, ad esempio, un focus sul controllo continuo da parte dell'uomo.

Illustrazione 8. *Diversi schemi nazionali di responsabilità del traffico si concentrano sull'esistenza di un conducente o consentono una difesa in caso di un evento inevitabile o nozioni simili. Questi concetti non si traducono correttamente in scenari di rischio che coinvolgono tecnologie digitali emergenti perché il conducente di un AV assomiglia di più a un passeggero e perché la responsabilità (o l'esclusione di esso) non può più essere collegata al controllo umano, che in genere manca del tutto, almeno con AV di livello 5.*

Responsabilità rigorosa del produttore ([13] - [15] VEDI SOPRA):

Secondo l'opinione dell'NTF del gruppo di esperti, il principio della responsabilità del produttore, adottato in relazione ai prodotti tradizionali, dovrebbe applicarsi anche alle tecnologie digitali emergenti. I motivi alla base, come un'equa distribuzione dei rischi e dei benefici associati alla produzione commerciale, la diffusione dei costi dei danni individuali a tutti gli acquirenti di un determinato tipo di prodotto e la prevenzione, sono pienamente validi anche se il prodotto o uno dei suoi componenti essenziali è in forma digitale.

È in linea con il principio di equivalenza funzionale (vedi [3] (b)), che i danni causati da contenuti digitali difettosi dovrebbero innescare la responsabilità del produttore perché il contenuto digitale svolge molte delle funzioni materiali mobili tangibili utilizzate per adempiere quando il PLD era redatto e approvato. Ciò è tanto più vero per gli elementi digitali difettosi di altri prodotti, alcuni dei quali provengono separatamente dall'elemento tangibile (ad esempio, come app di controllo da scaricare suLLo smartphone dell'utente) o come aggiornamenti over-the-air dopo che il prodotto è stato messo in circolazione (ad esempio aggiornamenti di sicurezza) o come servizi digitali forniti su base continua durante il periodo di utilizzo del prodotto (ad esempio navigazione servizi cloud).

Quando il difetto si è manifestato a causa dell'interferenza del produttore con il prodotto già messo in circolazione (ad esempio tramite un aggiornamento del software) o per la mancata interferenza del produttore, dovrebbe essere considerato come un difetto del prodotto per il quale il produttore è responsabile.

Il momento in cui un prodotto viene immesso sul mercato non dovrebbe fissare un limite rigoroso alla responsabilità del produttore per i difetti in cui, dopo quel momento, il produttore o un terzo che agisce per conto del produttore rimane incaricato di fornire aggiornamenti o servizi digitali. Il produttore dovrebbe pertanto rimanere responsabile qualora il difetto abbia origine (i) in un componente digitale difettoso o in una parte ausiliaria digitale o in altri contenuti o servizi digitali forniti per il prodotto con il consenso del produttore dopo che il prodotto è stato messo in circolazione; o (ii) in assenza di un aggiornamento di contenuti digitali o della fornitura di un servizio digitale che sarebbe stato necessario per mantenere il livello di sicurezza previsto entro il periodo di tempo per il quale Il produttore è tenuto a fornire tali aggiornamenti.

Solo di recente, l'UE ha confermato nella direttiva (UE) 2019/771 sulla vendita di beni che un venditore è anche responsabile del fatto che tali elementi digitali siano conformi al contratto, compresi gli aggiornamenti previsti per il periodo che il consumatore può si aspettano ragionevolmente e la Direttiva (UE 2019/770 stabilisce un regime simile per i contenuti digitali e i servizi digitali. Le caratteristiche proposte della rigida responsabilità di un produttore sono molto simili e seguono molto la stessa logica, anche se per motivi diversi.

Come indicato sopra, le tecnologie digitali emergenti sono caratterizzate da una prevedibilità limitata.

Questo fenomeno si intensificherà con la diffusione dell'apprendimento automatico. L'interconnessione dei dispositivi, nonché le minacce alla sicurezza informatica, contribuiscono anche a difficoltà nel prevedere le prestazioni del prodotto. Un difetto nel contenuto digitale o in un prodotto con elementi digitali può quindi derivare dall'impatto dell'ambiente in cui il prodotto opera o dall'evoluzione del prodotto, per il quale il produttore ha creato solo un quadro generale ma che non ha progettato in dettaglio. In considerazione della necessità di condividere benefici e rischi in modo efficiente ed equo, la difesa dal rischio di sviluppo, che consente al produttore di evitare la responsabilità per difetti imprevedibili, non dovrebbe essere disponibile nei casi in cui era prevedibile che potesse verificarsi uno sviluppo imprevisto.

Le caratteristiche delle tecnologie digitali emergenti, come l'opacità, l'apertura, l'autonomia e la prevedibilità limitata (vedi [1]), possono spesso comportare difficoltà o costi irragionevoli per la vittima per stabilire sia la sicurezza che un utente medio ha il diritto di aspettarsi, sia il fallimento per raggiungere questo livello di sicurezza. Allo stesso tempo, può essere significativamente più facile per il produttore dimostrare fatti pertinenti. Questa asimmetria giustifica l'inversione dell'onere della prova.

La vittima dovrebbe inoltre beneficiare di una riduzione dell'onere probatorio per quanto riguarda la relazione causale tra un difetto e il danno (vedere [26]).

La responsabilità rigorosa dei produttori per i prodotti difettosi dovrebbe essere integrata con la responsabilità basata sui guasti per il mancato adempimento dei compiti di monitoraggio (vedere [17] (b)).

Responsabilità da difetto e doveri di diligenza ([16] - [17] VEDI SOPRA):

Per l'uso di tecnologie più tradizionali, è già riconosciuto che i loro operatori devono assolvere una serie di compiti di cura. Si riferiscono alla scelta della tecnologia, in particolare alla luce dei compiti da svolgere e delle capacità e capacità dell'operatore; il quadro organizzativo fornito, in particolare per quanto riguarda un adeguato monitoraggio; e manutenzione, compresi eventuali controlli di sicurezza e riparazione. La mancata osservanza di tali doveri può comportare la responsabilità per colpa indipendentemente dal fatto che l'operatore possa anche essere strettamente responsabile per il rischio creato dalla tecnologia.

> ***Illustrazione 9.*** *Nonostante le avverse condizioni meteorologiche dovute a una forte tempesta, del tutto prevedibile, il rivenditore (R) continua a impiegare droni per consegnare merci ai clienti.*
> *Uno dei droni è colpito da un forte vento, cade a terra e ferisce gravemente un passante.*
> *R potrebbe non solo essere strettamente responsabile per i rischi inerenti al funzionamento dei droni, ma anche per la sua incapacità di interrompere l'uso di tali droni durante la tempesta.*

In molti sistemi giuridici nazionali, i tribunali hanno elevato il dovere di diligenza in questione al punto in cui è difficile tracciare il confine tra responsabilità per colpa e responsabilità oggettiva. Con le tecnologie digitali emergenti, tali doveri di cura - nonostante tutte le nuove opportunità e le tecnologie che migliorano la sicurezza di cui questi sistemi possono presentare - sono spesso ingranditi ancora di più.

> ***Illustrazione 10****. La compagnia aerea A acquista un aereo dal produttore P. Un nuovo elemento AI dell'autopilota può, in circostanze molto eccezionali, causare l'incidente dell'aereo se il software non viene disabilitato manualmente dal pilota. La compagnia aerea A ha il dovere di prendersi familiarità con la nuova funzionalità, monitorare l'aereo e assicurarsi che i piloti ricevano l'adeguata formazione e scambino informazioni e esperienze relative all'utilizzo del nuovo software.*
> *Se A viola questo obbligo, A può essere ritenuta responsabile sotto la responsabilità per colpa (fatti salvi gli strumenti legali internazionali esistenti che possono limitare la responsabilità di A).*

Più tecnologie avanzate diventano, più è difficile per gli operatori sviluppare le giuste competenze e svolgere tutti i compiti. Mentre il rischio di competenze insufficienti dovrebbe essere ancora a carico degli operatori, sarebbe ingiusto lasciare i produttori completamente fuori dall'equazione. Piuttosto, i produttori devono progettare, descrivere e commercializzare i prodotti in modo efficace per consentire agli operatori di adempiere alle proprie funzioni.

> ***Illustrazione 11****. Nell'illustrazione 10, è principalmente P che deve avvisare i propri clienti (A) delle caratteristiche e dei rischi particolari del software in questione, e possibilmente offrire i corsi di formazione necessari e monitorare il sistema una volta acceso il mercato.*

In molte giurisdizioni nazionali, un obbligo generale di monitoraggio del prodotto da parte dei produttori è già stato sviluppato ai fini del diritto illecito. Alla luce delle caratteristiche delle tecnologie digitali emergenti, in particolare della loro apertura e dipendenza dall'ambiente digitale generale, compresa l'emergere di nuovi malware, tale compito di monitoraggio sarebbe di fondamentale importanza.

Responsabilità vicaria per sistemi autonomi ([18] - [19] VEDI SOPRA):

Un'opzione proposta per affrontare i rischi della tecnologia digitale emergente è la potenziale espansione della nozione di responsabilità vicaria, lasciando intatto il rispettivo regime nazionale di responsabilità per gli altri, ma espandendolo (direttamente o tramite analogia) a situazioni funzionalmente equivalenti in cui si fa uso di tecnologia autonoma invece di utilizzare un ausiliario umano.

Ciò può integrare la responsabilità oggettiva ai sensi di [9] - [12] e la responsabilità per colpa basata sulla nozione di doveri di cura rafforzati ai sensi di [16].

> ***Illustrazione 12.*** *Un ospedale utilizza un robot chirurgico guidato dall'intelligenza artificiale. Nonostante il fatto che l'ospedale abbia adempiuto a tutti i possibili doveri di cura, un paziente viene danneggiato perché il robot non funziona in modo che nessuno avrebbe potuto prevedere. L'ospedale dovrebbe essere responsabile in ogni caso, secondo il principio delineato in [18].*

La portata e le condizioni per l'applicazione della responsabilità vicaria variano da un paese all'altro, a causa dei diversi modi in cui i sistemi giuridici nazionali si sono sviluppati e il conseguente ambito di applicazione più ampio o più stretto della responsabilità rigorosa che hanno adottato. Tuttavia, lo sviluppo di tecnologie digitali emergenti, in particolare sistemi con un elevato grado di autonomia decisionale, richiede il rispetto dei requisiti di equivalenza (vedere 2 [3] (b)).

Laddove l'uso di un ausiliario umano comporterebbe la responsabilità di un preponente, l'uso di uno strumento di tecnologia digitale non dovrebbe invece consentire al preside di evitare la responsabilità. Piuttosto, dovrebbe comportare tale responsabilità nella stessa misura.

Tuttavia, poiché le leggi si trovano in molte giurisdizioni, la nozione di responsabilità vicaria al momento richiede che il sistema ausiliario si sia comportato male (sebbene valutato secondo gli standard applicabili al preponente). Nel caso di una macchina o tecnologia, questo fa scattare la domanda in base a quali parametri di riferimento tale "condotta" dovrebbe essere valutata. Gli esperti ne hanno discusso in modo approfondito, ma non sono giunti a una conclusione definitiva. Tuttavia, la risposta più convincente sembra essere che il punto di riferimento per la valutazione delle prestazioni con la tecnologia autonoma dovrebbe essere principalmente il punto di riferimento accettato per gli ausiliari umani, ma una volta che la tecnologia autonoma supera gli ausiliari umani in termini di prevenzione del danno, il punto di riferimento dovrebbe essere determinato dalle prestazioni di tecnologia comparabile disponibile sul mercato.

Poiché di solito esiste una vasta gamma di tecnologie disponibili, che possono presentare parametri di sicurezza molto diversi, nella scelta del punto di confronto appropriato, si dovrebbero applicare gli stessi principi delle tecnologie tradizionali (come macchine a raggi X o altre apparecchiature), ovvero riferimento dovrebbe essere tenuto al dovere di diligenza dell'operatore per quanto riguarda la scelta del sistema (vedere [16] (a)).

> ***Illustrazione 13.*** *Nell'esempio del robot chirurgico (Figura 12), non è difficile stabilire una condotta scorretta pertinente in cui, ad esempio, il taglio effettuato dal robot è il doppio di quello che avrebbe fatto un chirurgo umano. Se il taglio fosse più lungo di quello che avrebbero fatto i migliori robot sul mercato, ma comunque più corto di quello di un chirurgo umano, si deve rispondere alla domanda se l'ospedale avrebbe dovuto acquistare un robot migliore con gli stessi principi della domanda di sé un ospedale avrebbe dovuto acquistare una macchina a raggi X migliore o impiegare medici extra.*

Registrazione per progettazione ([20] - [23] VEDI SOPRA):

Le tecnologie digitali emergenti non solo danno origine a complessità e opacità senza precedenti.

Offrono anche possibilità senza precedenti di documentazione affidabile e dettagliata degli eventi che possono consentire l'identificazione tra l'altro di ciò che ha causato un incidente. Questo di solito può essere fatto utilizzando i file di registro, motivo per cui sembra desiderabile imporre, in determinate circostanze, il dovere di fornire una registrazione adeguata e di divulgare i dati alla vittima in un formato leggibile.

Eventuali requisiti devono essere sicuramente idonei al conseguimento e alla proporzione degli obiettivi, tenendo conto, in particolare, della fattibilità tecnica e dei costi della registrazione, dei valori in gioco, dell'entità del rischio e di eventuali conseguenze negative per i diritti degli altri . La registrazione dovrebbe essere effettuata in modo tale che nessuna parte interessata possa manipolare i dati e che la vittima e / o la persona che risarcisce la vittima in primo luogo, ad esempio un fornitore di assicurazioni, abbia accesso ad essi. Inoltre, è ovvio che la registrazione deve essere effettuata in conformità con la legge altrimenti applicabile, in particolare per quanto riguarda la protezione dei dati e la protezione dei segreti commerciali.

> ***Illustrazione 14.*** *Nel caso degli AV ci sarebbe un obbligo di registrazione. Gli incidenti stradali si verificano piuttosto frequentemente e spesso causano gravi danni alla vita e alla salute delle persone. I veicoli a motore sono comunque molto sofisticati e costosi, quindi l'aggiunta della tecnologia di registrazione non dovrebbe aumentare significativamente i costi di produzione. Esistono molti dati che possono essere ragionevolmente registrati e serviranno a ricostruire eventi e catene causali che sono entrambi essenziali per allocare la responsabilità (ad esempio scoprendo quale AV ha causato l'incidente non rispondendo a un segnale inviato dall'altro AV) e difficilmente potrebbe essere ricostruito diversamente.*
>
> ***Illustrazione 15****. La registrazione non sarebbe consigliabile, tuttavia, nel caso di una bambola dotata di AI per bambini. I rischi associati alla bambola non sono del tipo in cui la registrazione sarebbe una risposta adeguata. Per quanto riguarda il rischio di merchandising nascosto, il che significa che la bambola manipola la mente del bambino citando e ripetendo alcuni marchi di prodotti, le implicazioni negative della registrazione (che dovrebbe includere, in una certa misura, la registrazione delle conversazioni) per la protezione dei dati supererebbe ogni possibile beneficio. Per quanto riguarda il rischio di un estraneo che si intromette nella bambola, la risposta corretta è più sicurezza informatica per impedirlo, non un obbligo di registrazione.*

Il mancato rispetto di un obbligo di registrazione e divulgazione dovrebbe comportare una presunzione confutabile che le informazioni, se registrate e divulgate, avrebbero rivelato che il relativo elemento di responsabilità è soddisfatto.

> ***Illustrazione 16.*** *Prendi l'esempio di un incidente tra l'AV di A e l'AV di B, ferendo B. La situazione del traffico era quella in cui, normalmente, i due AV scambiavano dati e "negoziavano" quale AV entrava per prima nella corsia. Quando è stato citato in giudizio da B, A si rifiuta di divulgare i dati registrati nelle registrazioni del suo AV. Si presume quindi che il suo AV abbia inviato un segnale che dice all'AV di B di entrare per prima nella corsia, ma è comunque andato per primo da solo.*

Se un prodotto utilizzato dall'operatore non contiene un'opzione di registrazione (ad esempio, in violazione dei requisiti normativi obbligatori o in contrasto con altri prodotti di questo tipo) e l'operatore è, per questo motivo, esposto a responsabilità, l'operatore dovrebbe essere in grado di trasferire la perdita derivante dalla sua incapacità di rispettare l'obbligo di divulgare i dati registrati alla vittima (che di solito comporta la responsabilità dell'operatore nei confronti della vittima) al produttore. Ciò può essere ottenuto in vari modi, anche consentendo una domanda separata o mediante surrogazione.

> ***Illustrazione 17.*** *Immagina che, nell'illustrazione 16, A non abbia rifiutato di divulgare i dati, ma che l'AV di A non abbia registrato il tipo di dati in questione. Se A dovesse pagare danni a B solo per questo motivo, dovrebbe anche poter fare causa al produttore.*

Regole di sicurezza ([24] VEDI SOPRA):

Con maggiore complessità, apertura e vulnerabilità, aumenta la necessità di introdurre nuove norme di sicurezza. La sicurezza del prodotto digitale differisce dalla sicurezza del prodotto in termini tradizionali in vari modi, anche tenendo conto degli effetti che un prodotto può avere sull'ambiente digitale dell'utente. Ancora più importante, la sicurezza informatica è diventata essenziale.

Per quanto riguarda le conseguenze della conformità o non conformità a tali regole, gli esperti hanno preso in considerazione due diverse soluzioni. Una soluzione era che il mancato rispetto delle norme può comportare un'inversione dell'onere della prova riguardante elementi chiave di responsabilità, inclusi causalità e colpa. L'altra soluzione era che il rispetto delle regole porta alla presunzione dell'assenza di causalità o colpa. Gli esperti hanno deciso a favore della prima soluzione, perché è più adatta ad affrontare le difficoltà delle vittime quando si tratta di dimostrare gli elementi di responsabilità in contesti che coinvolgono le tecnologie digitali emergenti. In particolare, è il ritmo con cui queste tecnologie si stanno evolvendo e la necessità di imporre ai fornitori l'obbligo di monitorare il mercato e reagire più rapidamente alle nuove minacce di quanto potrebbe fare qualsiasi governante, che ha reso inappropriato avere una presunzione dell'assenza di causalità o colpa se un fornitore ha rispettato le regole.

> ***Illustrazione 18.*** *Immagina che ci sia una nuova regola sulla sicurezza informatica delle apparecchiature domestiche IoT, progettata per prevenire l'hacking e il danno che ne deriva. Il Wi-Fi privato della vittima viene violato in un modo tipico delle lacune di sicurezza informatica nelle apparecchiature IoT. Laddove la vittima può dimostrare che un bollitore prodotto da P non ha rispettato lo standard di sicurezza in base alle norme di sicurezza adottate, la vittima potrebbe citare in giudizio P e l'onere sarebbe su P per dimostrare che il danno era stato causato da un dispositivo diverso.*

Va sottolineato che ciò si riferisce solo alle regole adottate dal legislatore, come quelle adottate nell'ambito del "Nuovo approccio normativo", e non a semplici standard tecnici che si stanno sviluppando nella pratica.

L'inversione dell'onere della prova discusso qui è essenziale nell'ambito della responsabilità fondata sui guasti.

Nel caso della responsabilità del produttore, un principio simile è già applicato in molte giurisdizioni nel contesto delle implementazioni PLD nazionali. Si presume che il mancato rispetto di uno standard di sicurezza significhi che il prodotto non fornisce il livello di sicurezza che il consumatore ha il diritto di aspettarsi. Ragionamenti simili dovrebbero applicarsi alla responsabilità del produttore di una tecnologia digitale emergente ([13] - [15]).

Onere della prova del nesso di causalità ([25] - [26] VEDI SOPRA):

Come è già la norma standard in tutte le giurisdizioni, chiunque richieda un risarcimento da un altro dovrebbe in generale dimostrare tutti i requisiti necessari per tale richiesta, incluso in particolare il nesso causale tra il danno da risarcire da un lato e le attività o i rischi all'interno del sfera del destinatario del reclamo può innescare la responsabilità di quest'ultimo sull'altro.

Questo principio generale è supportato, tra l'altro, dalle preoccupazioni di equità e risulta dalla necessità di considerare ed equilibrare gli interessi di entrambe le parti.

Tuttavia, date le implicazioni pratiche della complessità e dell'opacità delle tecnologie digitali emergenti in particolare, le vittime potrebbero trovarsi in una posizione più debole per stabilire il nesso di causalità rispetto ad altri casi illeciti, in cui gli eventi che portano al danno possono essere analizzati più facilmente a posteriori, anche dal punto di vista della vittima.

Come è vero in tutte le giurisdizioni, in passato i tribunali hanno già trovato il modo di alleviare l'onere di provare il nesso di causalità se la posizione del richiedente è considerata più debole rispetto ai casi tipici.

Ciò include opzioni procedurali come consentire prove prima facie, applicare la teoria della res ipsa loquitur o abbassare lo standard di prova in determinate categorie di casi.

Alcune giurisdizioni sono anche disposte a spostare completamente l'onere della prova del nesso di causalità se la base per ritenere il convenuto responsabile può essere dimostrata particolarmente forte dal richiedente (come grave colpa del convenuto), ma il nesso causale tra tale comportamento difettoso e il danno del richiedente è semplicemente sospettato, ma non provato, dalle prove disponibili per il richiedente.

Un altro metodo per aiutare il richiedente a provare la causa del danno consiste nel concentrarsi su chiunque abbia il controllo delle prove chiave ma non riesce a produrle, ad esempio, se l'imputato è o dovrebbe essere in grado di presentare prove interne come progetti di progettazione, competenza interna, file di registro o altre registrazioni, ma non produce tali prove in tribunale, né strategicamente né perché le prove sono state perse o mai generate.

La promozione di misure specifiche rischierebbe in particolare di interferire con le norme procedurali nazionali. Tuttavia, al fine di offrire una guida per l'ulteriore sviluppo e ravvicinamento delle legislazioni e per consentire un ragionamento più coerente e comparabile, gli esperti ritengono che abbassare l'asticella per il richiedente di dimostrare il nesso di causalità possa essere consigliabile per le vittime di tecnologie digitali emergenti se sono in gioco i seguenti fattori.

- In primo luogo, è possibile che la stessa tecnologia abbia alcune caratteristiche potenzialmente dannose, che potrebbero essere prese in considerazione anche se non è (ancora) dimostrato che tali rischi si siano effettivamente materializzati. Se il richiedente può dimostrare che c'era un difetto in un prodotto che incorporava tecnologie digitali emergenti, creando così un rischio straordinario in aggiunta a quelli comunemente associati a prodotti impeccabili, ma - ancora una volta - il danno causato non può essere (completamente) rintracciato in detto difetto , questo potrebbe ancora essere preso in considerazione nella valutazione generale di come attuare l'onere della prova del nesso di causalità.
- Se ci sono più possibili cause e non è chiaro cosa abbia innescato esattamente il danno (o quale combinazione di potenziali cause con quale percentuale di probabilità), ma se la probabilità di tutte le possibili cause combinate, che sono attribuibili a una parte (ad esempio l'operatore) supera una determinata soglia (ad es. 50% o più), ciò può anche contribuire a porre l'onere di produrre prove che confutano tali impressioni di prima mano su quella parte.

  Illustrazione 19. *Un piccolo robot di consegna gestito dal rivenditore R ferisce un pedone per strada. Non è chiaro quale delle seguenti possibili cause abbia provocato l'incidente: il robot potrebbe essere stato difettoso dall'inizio; R potrebbe non aver installato un aggiornamento necessario che avrebbe impedito l'incidente; Il dipendente E di R potrebbe aver sovraccaricato il robot; l'hacker H potrebbe aver intenzionalmente manipolato il robot; alcuni adolescenti potrebbero essere saltati sul robot per divertimento; una tegola potrebbe essere caduta da un edificio vicino e così via.*
  Se la probabilità di tutte le possibili cause attribuibili a R supera significativamente la probabilità di tutte le altre possibili cause, l'onere dovrebbe essere su R per dimostrare che nessuna delle cause all'interno della propria sfera ha innescato l'incidente.

- Considerando ulteriori aspetti che si riferiscono all'analisi degli eventi causali e che sono (o dovrebbero essere) prevalentemente in controllo dell'esperienza e delle prove che contribuiscono a tale analisi, si potrebbe considerare l'asimmetria informativa tipicamente trovata tra coloro che sviluppano e producono tecnologie digitali emergenti su da una parte e le vittime di terze parti

dall'altra parte come un altro argomento nella valutazione complessiva di chi dovrebbe sopportare l'onere di provare il nesso di causalità e in che misura. Ciò include la tecnologia stessa, ma anche potenziali prove generate da tale tecnologia in occasione dell'evento dannoso.
Quest'ultimo non solo considera chi può recuperare tali dati, ma anche chi può leggerli e interpretarli (in particolare se sono crittografati o intelligibili solo con specifiche conoscenze specialistiche). Un aspetto specifico in questo contesto è se un articolo coinvolto nell'evento dannoso avesse (o secondo gli standard del settore) un dispositivo di registrazione installato, che avrebbe potuto raccogliere informazioni in grado di far luce su ciò che è realmente accaduto.

- Infine, come è già comunemente usato come argomento pesante nell'equilibrio generale degli interessi nei casi illeciti, il tipo e l'entità del danno possono anche contribuire a decidere fino a che punto dovrebbe essere ancora la vittima a provare la causa del suo danno.

Onere della prova difettosa ([27] VEDI SOPRA):

Quando il danno deriva da un'attività in cui le tecnologie digitali emergenti svolgono un ruolo, la vittima può incontrare notevoli difficoltà a provare fatti che confermano la sua richiesta di risarcimento danni basata su negligenza o colpa. Ciò giustifica il ripensamento dell'approccio tradizionale per dimostrare queste condizioni di responsabilità.

L'adozione di qualsiasi norma relativa alla distribuzione dell'onere della prova in errore richiede in primo luogo la spiegazione dell'errore. Vi è una varietà di significati associati a questa parola in vari sistemi giuridici, che vanno dall'equare la colpa con l'erroneità della condotta alla comprensione della colpa come colpa puramente individuale e soggettiva. Pertanto la responsabilità basata sui guasti richiede:

a) sempre una violazione di un determinato obbligo di diligenza (standard di condotta);
b) in alcune (probabilmente la maggior parte) giurisdizioni, l'intenzione di violare questo dovere di diligenza o negligenza nel farlo;
c) in alcune (probabilmente la minoranza di) giurisdizioni, una valutazione etica negativa della condotta del torturatore come soggettivamente riprovevole.

Lo standard di condotta può essere stabilito dallo statuto o altrimenti prescritto normalmente sotto forma di misure regolamentari o standard e norme emanati dalle autorità competenti. Però, può anche essere stabilito ex post dal tribunale, sulla base di criteri generali quali ragionevolezza, diligenza, ecc.

Le tecnologie digitali emergenti, in particolare la presenza di AI, cambiano la struttura della responsabilità basata sui guasti. I due esempi più importanti dell'applicazione della responsabilità per colpa ai danni correlati all'intelligenza artificiale sono la responsabilità del produttore per i danni causati dal prodotto da lui prodotto, che avrebbe dovuto monitorare, ecc. (Responsabilità al di fuori dell'ambito di un regime di responsabilità rigoroso come quello previsto in [13] - [15] sopra) e la responsabilità dell'utente (operatore) per i danni da lui causati durante l'utilizzo di uno strumento basato sull'intelligenza artificiale.

Nel caso della responsabilità del produttore (al di fuori della rigorosa responsabilità del prodotto), la causa diretta del danno è un prodotto, ma le caratteristiche dannose del prodotto sono l'effetto della negligenza del produttore nella progettazione, fabbricazione, commercializzazione, monitoraggio, ecc. Prodotto. Pertanto, per dimostrare la colpa è necessario dimostrare che il prodotto non era della qualità richiesta e che il produttore ha violato intenzionalmente o negligentemente uno standard di condotta applicabile nei confronti di questo prodotto. L'avanzata delle tecnologie digitali emergenti aumenta le difficoltà evidenti in relazione a:

- i requisiti di qualità del prodotto e i dettagli del suo funzionamento effettivo che ha portato al danno;
- violazione di un obbligo di diligenza da parte del produttore nei confronti del prodotto (incluso lo standard di condotta applicabile);

- fatti che consentano al tribunale di stabilire che la violazione dell'obbligo di diligenza era intenzionale o negligente.

Per quanto riguarda la responsabilità dell'utente, la struttura generale della responsabilità per le azioni eseguite utilizzando gli strumenti è la seguente:

un attore + l'uso di uno strumento [ingiustizia / colpa] → Causa → Vittima di un danno [interesse protetto]

La sfida dell'analisi dei difetti nel modello tradizionale è la valutazione del comportamento dell'attore in relazione a:

(i) la sua decisione di agire;
(ii) la sua decisione di utilizzare uno strumento,
(iii) la sua scelta dello strumento,
(iv) il suo modo di utilizzarlo o di controllarne o monitorarne il funzionamento.

Pertanto l'attore è in colpa se:

(i) la sua decisione sull'azione stessa è sbagliata e vi è intenzione o negligenza nel prendere questa decisione, o
(ii) la sua decisione sull'uso di uno strumento nell'azione invece di eseguirlo da sola è sbagliata e vi è intenzione o negligenza nel prendere questa decisione, oppure
(iii) la sua scelta dello strumento è errata (sceglie il tipo di strumento che non è adatto al compito o lo strumento giusto che ha scelto successivamente malfunzionamenti) e vi è stata intenzione o negligenza nel fare questa scelta, oppure
(iv) usa il suo strumento o controlla / monitora il suo funzionamento in modo errato e vi è intenzione o negligenza in questo comportamento.

Secondo la regola generale di responsabilità, l'onere della prova sia della violazione di un dovere di diligenza che dell'intenzione o della negligenza incombe alla vittima.

Nel modello tradizionale, il corretto funzionamento dello strumento e il risultato atteso del suo funzionamento sono noti e facili da stabilire e i dettagli delle prestazioni effettive dello strumento di solito non sono troppo difficili da esaminare. A causa del loro rapido sviluppo e delle loro caratteristiche, descritte sopra (opacità, apertura, autonomia e prevedibilità limitata), le tecnologie digitali emergenti utilizzate come strumenti aggiungono ulteriori livelli di complessità al modello di responsabilità basato sui guasti, sfidando il funzionamento delle regole di responsabilità basate sui guasti su due livelli:

a) un livello strutturale: l'autonomia e la capacità di autoapprendimento della tecnologia possono essere viste come una rottura del nesso causale tra la condotta dell'attore e il danno - questo è il problema dell'attribuzione dell'operazione e del suo risultato a una persona, che dovrebbe essere risolto attribuendo legalmente tutte le azioni della tecnologia digitale emergente e i loro effetti all'operatore della tecnologia (cfr. [18]).
b) un livello pratico di accertamento dei fatti: i fatti da cui dipende la responsabilità possono essere difficili da scoprire e comunicare al tribunale. La difficoltà può essere:
    - scoprire e spiegare a un'altra persona in che modo un determinato insieme di dati di input ha determinato l'esito del processo gestito dall'IA e che ciò ha comportato una carenza del sistema;

- mostrare che il torturatore ha violato uno standard (livello) di cura nel decidere di utilizzare questa particolare tecnologia digitale emergente in questa situazione concreta, o nel gestirla / monitorarla;
- stabilire che la violazione di questo standard è stata intenzionale o negligente.

In teoria, il richiedente deve dimostrare che l'imputato ha violato uno standard (livello) di assistenza applicabile e lo ha fatto intenzionalmente o negligentemente. In pratica, tuttavia, se lo standard di cura non è stato prescritto normalmente (da uno statuto o altro), l'onere del richiedente si estende a dimostrare (o persuadere) quale livello di assistenza dovrebbe applicare al comportamento del convenuto. La mancanza di uno standard chiaro pone quindi la parte con l'onere di provare l'esistenza dello standard, o la sua violazione, in svantaggio.

La questione è quindi se tutte queste difficoltà probatorie debbano rimanere con la vittima o tutte o parte di esse, in tutto o in circostanze specifiche, debbano colpire l'imputato.

Elementi di prova, l'onere per il quale normalmente è a carico del richiedente, ma che potrebbero essere assegnati al convenuto sono:

- violazione di un dovere di diligenza da parte del convenuto (il produttore, per quanto riguarda la progettazione, la fabbricazione, il monitoraggio, ecc., E l'utente per quanto riguarda la scelta della tecnologia e il funzionamento / monitoraggio),
- intenzione o negligenza del convenuto,
- qualità scadenti della tecnologia,
- funzionamento errato della tecnologia.

In vari ordinamenti giuridici, sono riconosciuti vari fattori che giustificano la modifica dell'onere della prova a favore del richiedente, in particolare:

a) elevata probabilità di colpa,
b) la capacità pratica delle parti di dimostrare la propria colpa,
c) violazione dell'obbligo legale da parte del convenuto,
d) particolare pericolosità dell'attività del convenuto che ha provocato danni,
e) natura e portata del danno.

Esistono anche varie tecniche legali per farlo, dall'inversione legale dell'onere della prova a tutti i tipi di strumenti procedurali come prove prima facie, presunzioni di fatto, inferenza negativa e così via.

Le caratteristiche delle tecnologie digitali emergenti come l'opacità, l'apertura, l'autonomia e la prevedibilità limitata possono spesso comportare difficoltà o costi irragionevoli per l'attore a dimostrare i fatti necessari per l'accertamento della colpa. Allo stesso tempo, la prova dei fatti rilevanti può essere molto più semplice per l'imputato (produttore o operatore della tecnologia). Questa asimmetria giustifica l'inversione dell'onere della prova. Mentre, come accennato in precedenza, in molti casi i tribunali possono ottenere risultati simili con varie disposizioni procedurali, l'introduzione di una norma chiara garantirà la convergenza e la prevedibilità desiderate nell'applicazione della legge.

Cause all'interno della sfera della vittima ([28] VEDI SOPRA):

Mentre le giurisdizioni in tutta Europa già ora riconoscono che la condotta o qualche altro rischio all'interno della sfera della vittima può ridurre o addirittura escludere la sua richiesta di risarcimento nei confronti di un'altra, sembra importante affermare che qualunque cosa la NTF del gruppo di esperti proponga di migliorare le norme sulla responsabilità per le tecnologie digitali emergenti dovrebbero applicarsi di conseguenza se tali tecnologie sono utilizzate all'interno della sfera della vittima. Ciò è in linea con la cosiddetta regola "immagine speculare" della condotta contributiva.

Pertanto, se due AV si scontrano, ad esempio, i criteri di cui sopra per l'identificazione dell'operatore responsabile ([10] - [11]) dovrebbero applicarsi di conseguenza per determinare quale effetto ha sull'impatto del proprio veicolo della vittima sulla sua perdita sulla responsabilità dell'altro operatore AV.

Unità commerciali e tecnologiche ([29] - [30] VEDI SOPRA):

Tra le molte sfide per le vittime delle tecnologie digitali emergenti c'è la sfida di mostrare quale parte di un complesso ecosistema digitale ha causato il danno. Ciò può essere particolarmente difficile laddove diversi elementi siano stati forniti da parti diverse, creando un rischio significativo per la vittima di citare in giudizio la parte sbagliata e finire senza alcun risarcimento e costi di contenzioso. È pertanto giustificato disporre di regole speciali per le situazioni in cui due o più parti cooperano su base contrattuale o simile nella fornitura di elementi diversi di uno stesso ecosistema digitale, formando un'unità commerciale e tecnologica. In queste situazioni, tutti i potenziali torturatori dovrebbero essere responsabili in solido nei confronti della vittima, laddove la vittima possa dimostrare che almeno un elemento ha causato il danno in modo da innescare la responsabilità, ma non quale elemento.

> ***Illustrazione 20.*** *Un sistema di allarme intelligente prodotto dal produttore A è stato aggiunto a un ambiente di casa intelligente prodotto da B e installato e installato da C. Questo hub di casa intelligente funziona su un ecosistema sviluppato dal fornitore D. Si verifica un furto con scasso, ma la polizia è non debitamente avvisato dal sistema di allarme, quindi vengono causati danni significativi.*
> *A, B e D sono collegati da sofisticati accordi contrattuali riguardanti l'interoperabilità dei componenti pertinenti che ciascuno di essi fornisce e qualsiasi marketing correlato. Se si può dimostrare che il malfunzionamento non è stato causato da C (o da una causa esterna), ma se non è chiaro quale sia la situazione tra A, B e D, il proprietario della casa dovrebbe essere in grado di citare in giudizio A, B e D congiuntamente . Ognuno di loro è libero di dimostrare nei procedimenti che non è stata l'unità commerciale e tecnologica a causare il malfunzionamento, ma in caso contrario, il proprietario della casa può essere ritenuto responsabile in solido.*

La logica alla base di ciò è, da un lato, che potrebbe esserci una grave sotto-compensazione delle vittime in uno scenario di tecnologie digitali emergenti rispetto alla situazione funzionalmente equivalente del passato quando i sistemi di allarme erano fabbricati da un produttore chiaramente identificabile (e qualsiasi la responsabilità da parte dei fornitori di componenti si sarebbe aggiunta a questo) senza alcuna interazione significativa con gli altri componenti di un ecosistema.

Ciò può persino creare falsi incentivi, poiché i fornitori potrebbero essere tentati di dividere artificialmente gli ecosistemi che forniscono in componenti indipendenti, oscurando così i collegamenti causali e diluendo la responsabilità. In ogni caso, non dovrebbe essere la vittima a sopportare il rischio di una particolare struttura interna da parte del fornitore in una situazione in cui avrebbe potuto esserci un solo fornitore. In questi casi è anche più efficace ritenere responsabili tutti i potenziali infortuni, in quanto i diversi fornitori sono nella posizione migliore per controllare i rischi di interazione e interoperabilità e concordare anticipatamente la distribuzione dei costi degli incidenti.

Può essere difficile, in casi limite, definire ciò che si qualifica ancora come unità commerciale e tecnologica. I fattori da prendere in considerazione saranno, in primo luogo, qualsiasi commercializzazione congiunta o coordinata degli elementi, ma anche il grado di interdipendenza tecnica e di interoperabilità tra gli elementi e il grado di specificità o esclusività della loro combinazione.

> ***Illustrazione 21***. *Immagina che, nell'illustrazione 20, anche il provider di rete E avrebbe potuto causare il problema a causa di una temporanea interruzione della connessione Internet. Tuttavia, le apparecchiature per la casa intelligente normalmente necessitano solo della connettività di rete, ma non della connettività di rete di un determinato fornitore, e una maggiore cooperazione tra A, B e D da un lato e dall'altro non può essere attesa dal consumatore. Le cose potrebbero essere diverse nel caso piuttosto eccezionale che questo sia stato effettivamente offerto come pacchetto, con E marketing i suoi servizi sulla base del loro essere particolarmente affidabili come base per questo tipo di ecosistema di casa intelligente.*

Le unità commerciali e tecnologiche possono anche diventare rilevanti nella fase di ricorso tra i torturatori multipli, indipendentemente dal fatto che la vittima abbia già invocato la nozione di unità commerciali e tecnologiche (cfr. [31]).

Ricorso tra più torturatori ([31] VEDI SOPRA):

Uno dei problemi più urgenti per le vittime nei moderni ecosistemi digitali è che, a causa della maggiore complessità e opacità, spesso non sono in grado di scoprire e dimostrare quale dei vari elementi abbia effettivamente causato un incidente (il classico scenario di causalità alternativo).

> ***Illustrazione 22.*** *L'arteria di un paziente viene tagliata da un robot chirurgico guidato dall'intelligenza artificiale a causa di un guasto del chirurgo che utilizza il robot o a causa di un'esecuzione errata dei movimenti del chirurgo da parte del robot. In tal caso, nessuna delle due potenziali cause soddisfa la condizione condizionale sine qua non test ("ma per" test), perché se una di esse viene ignorata ipoteticamente, il danno potrebbe essere stato causato dal restante rispettivo altro evento . La conseguenza sarebbe che nessuna di queste sospette ragioni per cui la vittima è stata danneggiata potrebbe innescare la responsabilità, quindi la vittima potrebbe - almeno in alcuni sistemi giuridici - finire senza una richiesta di risarcimento, nonostante la certezza nota che una delle due o più eventi erano davvero la causa del danno.*

I sistemi giuridici negli Stati membri reagiscono in modo molto diverso a tali scenari e ogni soluzione presenta i suoi svantaggi.

Laddove una persona abbia causato un danno alla vittima e lo stesso danno sia imputabile a un'altra persona, la responsabilità di più torturatori (tortureasors) è normalmente una responsabilità congiunta, vale a dire che la vittima può richiedere il pagamento dell'intero importo o parte della somma da uno qualsiasi dei torturatori multipli, a discrezione della vittima, ma la somma totale richiesta non può superare la somma totale dovuta. Ci possono essere eccezionalmente situazioni in cui esiste una base ragionevole per attribuire solo una parte del danno a ciascuno dei criminali, nel qual caso la responsabilità può anche essere considerata.

Nella fase di ricorso, la responsabilità di altri torturatori nei confronti del torturatore che ha pagato i danni alla vittima è normalmente diversa, vale a dire che altri torturatori sono responsabili solo della loro parte individuale di responsabilità per il danno.

Non vi è motivo di discostarsi da questi principi nel contesto delle tecnologie digitali emergenti, ed è per questo che [31] suggerisce come regola generale diverse responsabilità nella fase di ricorso.

Tuttavia, la complessità e l'opacità delle emergenti impostazioni della tecnologia digitale che rendono già difficile per la vittima ottenere sollievo in primo luogo, rendono anche difficile per il torturatore pagante identificare le azioni e cercare un risarcimento dagli altri torturatori. Tuttavia, nonostante la complessità e l'opacità, è spesso possibile identificare due o più torturatori che formano un'unità commerciale e / o tecnologica (vedere [29] - [30]). Ciò dovrebbe essere rilevante anche nella fase di ricorso, vale a dire che i

membri di quell'unità dovrebbero essere responsabili congiuntamente di risarcire un altro malfattore che non è un membro dell'unità e ha pagato danni alla vittima che eccedono la sua quota.

> ***Illustrazione 23.*** *Il produttore di hardware ha un contratto con un fornitore di software e un altro con il fornitore di numerosi servizi cloud, che hanno causato il danno e che collaborano tutti su base contrattuale. Laddove un altro torturatore abbia versato un risarcimento alla vittima e chieda riparazione, le tre parti possono essere viste come un'unità commerciale e il torturatore pagatore dovrebbe essere in grado di richiedere il pagamento dell'intera quota cumulativa a una delle tre parti.*

Come è stato spiegato nel contesto di [29] - [30]), ciò è anche nell'interesse dell'efficienza, in quanto le parti sono incentivate a prendere accordi contrattuali per le richieste di risarcimento.

Danno ai dati ([32] VEDI SOPRA):

In termini di danni causati, l'emergere di tecnologie digitali ha comportato alcuni cambiamenti graduali, ma solo un piccolo cambiamento dirompente. Esiste un'eccezione, che a rigor di termini è anche un cambiamento graduale, ma la cui dimensione è tale da poter essere considerata dirompente: il significato del danno ai dati, come la cancellazione, il deterioramento, la contaminazione, la crittografia, l'alterazione o la soppressione dei dati . Con gran parte della nostra vita e la nostra "proprietà" che diventa digitale, non è più appropriato limitare la responsabilità al mondo tangibile. Tuttavia, non è neppure appropriato equiparare semplicemente i dati a beni materiali ai fini della responsabilità.

La maggior parte dei sistemi legali non presenta molti problemi quando si tratta di responsabilità contrattuale, in particolare in caso di negligenza del partner contrattuale.

> ***Illustrazione 24.*** *A archivia tutti i suoi file nello spazio cloud fornito dal fornitore dello spazio cloud C sulla base di un contratto. C non è riuscito a proteggere correttamente lo spazio cloud, motivo per cui un hacker sconosciuto elimina tutte le foto di A. C sarà normalmente responsabile nei confronti di A per un contratto. La responsabilità sarebbe in ogni caso per la perdita economica, ad es. eventuali costi che A deve sostenere per il ripristino dei file. Il fatto che A riceva o meno un risarcimento per la perdita non economica associata alla perdita della memoria familiare dipenderà dal sistema giuridico nazionale in questione.*

Le cose sono meno ovvie per la responsabilità per illecito, almeno in un certo numero di giurisdizioni. Per molto tempo, alcune giurisdizioni hanno risolto il problema considerando il danno ai dati come danno al supporto fisico su cui sono stati archiviati. Questo dovrebbe essere ancora possibile.

> ***Illustrazione 25.*** *Immagina che A abbia archiviato tutti i suoi file sul disco rigido del suo personal computer a casa. Il vicino B danneggia negativamente il computer, rendendo i file illeggibili.*
> *Indipendentemente dalla qualificazione del danno ai dati, questo era in ogni caso un danno illegale alla proprietà materiale di A (il disco rigido), e già per questo motivo B sarebbe responsabile.*

Tuttavia, questo approccio non porta a risultati soddisfacenti in cui il proprietario del supporto non è identico alla persona che ha un interesse legale protetto nei dati.

La domanda più difficile è ciò che equivale a un interesse legale protetto sufficientemente simile alla proprietà. L'NTF del gruppo di esperti ha discusso in modo approfondito se vi fossero anche responsabilità in caso di illecito laddove i dati pertinenti fossero protetti dalla legge sulla proprietà intellettuale o da un regime simile, come la protezione del database o la protezione del segreto commerciale. Tuttavia, in fin dei conti non sembra logico concentrarsi sulla protezione della proprietà intellettuale, poiché i motivi per cui il

legislatore introduce i diritti di proprietà intellettuale per i risultati intellettuali hanno poco a che fare con i motivi per cui una copia particolare su un determinato supporto dovrebbe essere protetta.

> ***Illustrazione 26.*** *A ha tutti i suoi file memorizzati nello spazio cloud fornito da C. Senza alcuna negligenza da parte di C, B danneggia negligentemente i server di C e tutti i file di A vengono eliminati. Esso non è chiaro il motivo per cui dovrebbe fare la differenza nella responsabilità di B se*
>
> *a) i file contenevano testo o foto di cui A deteneva il copyright,*
> *b) i file contenevano testo o foto di cui terzi detenevano il copyright, oppure*
> *c) i file contenevano dati macchina di grande valore economico, ai quali nessuno detiene alcun diritto d'autore o altri diritti di proprietà intellettuale.*

A seconda del sistema legale applicabile, tuttavia, potrebbero esserci altri interessi legali protetti con effetto di terze parti (non solo contro una parte contraente o altra parte particolare), come il possesso.

I dati sufficientemente affini alla proprietà sono solo una delle giustificazioni per riconoscere la responsabilità civile in caso di danni. In alternativa, dovrebbe esserci la responsabilità laddove il danno sia stato causato da un comportamento equivalente a un atto criminale, in particolare un'attività illegale ai sensi del diritto internazionale come la Convenzione di Budapest sulla criminalità informatica o in cui abbia violato altre norme relative alla condotta come legislazione sulla sicurezza dei prodotti il cui scopo è evitare tali danni.

> ***Illustrazione 27.*** *Se B nell'illustrazione 26 compromette lo spazio nella nuvola ed elimina i file di A, questo normalmente si qualifica come condotta criminale e B dovrebbe essere responsabile.*

Questo scopo dovrebbe idealmente essere espresso dalla lingua di tale legislazione. Un esempio, dove è stato chiarito molto, è il regolamento generale sulla protezione dei dati (GDPR). L'articolo 82 afferma esplicitamente che esiste una responsabilità in caso di danni causati dalla violazione dei requisiti del GDPR.

Nel definire tali norme relative alla condotta, la legge dovrebbe tenere in debita considerazione, in particolare, l'ubiquità dei dati e il suo significato come attività. Mentre sarebbe teoricamente possibile introdurre, ad esempio, uno standard che afferma in modo molto ampio che è generalmente vietato accedere, modificare ecc. Qualsiasi dato controllato da un'altra persona e di allegare la responsabilità in caso di violazione di questo standard, ciò potrebbe comportare una responsabilità eccessiva rischi perché tutti noi, in un modo o nell'altro, accediamo e modifichiamo costantemente i dati controllati da altri.

Ultimo ma non meno importante, la maggior parte delle giurisdizioni concorderebbe sul fatto che il danneggiamento dei dati dovrebbe comportare la responsabilità laddove il torturatore agisse con l'intenzione di causare danni.

Assicurazione ([33] VEDI SOPRA):

In particolare, i regimi di responsabilità rigorosa previsti dalla legge comportano spesso l'obbligo per la persona a cui è attribuibile il rischio di stipulare una copertura assicurativa contro il suo rischio di responsabilità. Ciò è in genere spiegato con la necessità di proteggere le future vittime dal rischio di insolvenza della persona responsabile. Tuttavia, dal punto di vista dell'analisi economica, il requisito assicurativo favorisce piuttosto l'internalizzazione dei costi delle attività che la persona responsabile (lecitamente) persegue.

In ogni caso, l'assicurazione obbligatoria di responsabilità civile non dovrebbe essere introdotta senza un'attenta analisi della sua effettiva necessità, piuttosto che essere automaticamente collegata a una

determinata attività. Dopotutto, il torturatore potrebbe essere in grado di compensare le vittime delle sue attività con i propri fondi se le perdite complessive prevedibili possono essere coperte anche senza assicurazione. Inoltre, il mercato potrebbe semplicemente non offrire una copertura assicurativa per un certo rischio, in particolare se è difficile da calcolare a causa della mancanza di esperienza, il che è abbastanza probabile con le nuove tecnologie (e quindi potrebbe anche essere un problema con le tecnologie digitali emergenti). Richiedere un'assicurazione in quest'ultima situazione può effettivamente impedire l'implementazione della tecnologia, se ciò richiede una prova dell'assicurazione nonostante il fatto che nessuno sul mercato sia disposto a sostenere rischi così ancora sconosciuti.

Ciò può in parte essere risolto limitando la responsabilità per determinati rischi ad un importo predeterminato (sebbene regolarmente adeguato), come spesso accade con i regimi di responsabilità rigorosi previsti dalla legge. Si potrebbe anche immaginare un requisito meno specifico per fornire copertura (quindi non necessariamente stipulando un'assicurazione, ma anche altri titoli finanziari).

Tuttavia, come dimostrato dall'esperienza in almeno alcuni settori (principalmente il traffico motorizzato), l'assicurazione di responsabilità civile obbligatoria può funzionare bene ed è effettivamente appropriata a determinate condizioni.

Dal punto di vista assicurativo, alcuni settori sono i più adatti ai regimi assicurativi obbligatori, compresi i trasporti, le industrie con un alto potenziale di lesioni personali e / o danni ambientali, attività pericolose e alcuni settori professionali.

Pertanto, potrebbe essere consigliabile rendere obbligatoria la copertura assicurativa di responsabilità civile per alcune tecnologie digitali emergenti. Ciò è particolarmente vero per i rischi altamente significativi (che possono portare a danni sostanziali e / o causare perdite frequenti), dove sembra improbabile che i potenziali feriti siano in grado di compensare tutte le vittime stesse (con fondi propri, con l'aiuto di titoli finanziari alternativi o mediante autoassicurazione volontaria).

Se viene introdotta un'assicurazione di responsabilità civile obbligatoria, l'assicuratore dovrebbe presentare una domanda di ricorso nei confronti del torturatore. In scenari di rischio paragonabili a quelli del traffico motorizzato, un'azione diretta delle vittime contro l'assicuratore può anche essere consigliabile.

Fondi di compensazione ([34] VEDI SOPRA):

Se i regimi di responsabilità sopra descritti (responsabilità rigorosa del produttore e dell'operatore e responsabilità basata sulla colpa) funzionano correttamente, non è necessario istituire nuovi tipi di fondi di compensazione, finanziati e gestiti dallo Stato o da altre istituzioni e con l'obiettivo di risarcire le vittime per le perdite subite come risultato del funzionamento di tecnologie digitali emergenti. Si consiglia, tuttavia, di garantire che nelle aree in cui è stata introdotta un'assicurazione di responsabilità civile obbligatoria sia presente un fondo di compensazione per riparare i danni causati da una tecnologia non identificata o non assicurata.

L'articolo 10 della direttiva assicurazione autoveicoli può fungere da modello per tale regime.

Poiché l'hacking costituisce una seria minaccia per gli utenti delle tecnologie basate su software e le norme tradizionali in materia di illecito civile possono spesso rivelarsi insufficienti a causa dell'incapacità della vittima di identificare il malfattore, può essere consigliabile introdurre un sistema di indennizzo per colpa non equivalente a quello applicabile alle vittime di crimini violenti, se e nella misura in cui un crimine informatico costituisce un reato equivalente a quest'ultimo. Le persone che hanno subito gravi lesioni

personali a causa del crimine informatico potrebbero quindi essere trattate allo stesso modo delle vittime di reati violenti.