GIUSTIZIA INSIEME

Diritto e innovazione" class="voce">

Machina delinquere non potest

di Costanza Corridori

19 maggio 2022

Machina delinquere non potest*

di Costanza Corridori

Quarta rivoluzione industriale: il dominio della digitalizzazione e dell'automazione. L'intelligenza artificiale entra nelle nostre vite e nei vari ambiti della società: che impatti può avere nel mondo del diritto penale?

Cosa significa intelligenza? Esiste una differenza tra un cervello elettronico e uno umano? Cosa accadrebbe qualora un robot causasse la morte di un individuo? L'algoritmo può commettere illeciti? Chi ne risponderebbe penalmente?

Questi sono solo alcuni degli interrogativi che tale articolo mira a sottolineare. Nonostante la rapidità del progresso tecnologico ci permetta oggi di affrontare tematiche come le auto a guida autonoma, i robot chirurghi e le chatbot, il diritto (soprattutto in ambito penale) non è ancora riuscito ad adattarsi al cambiamento culturale: non esistono normative idonee a disciplinare la responsabilità penale in caso di reati commessi dall'intelligenza artificiale.

I rischi sono molti, soprattutto per i diritti fondamentali degli esseri umani: per questo, l'articolo mira a fornire un'informazione generale sull'evoluzione storico-tecnologica realizzatasi fino ad oggi in tema di intelligenza artificiale, per poi passare alla trattazione della tesi di Gabriel Hallevy, che ha come obiettivo l'introduzione di una terza categoria giuridica (la personalità elettronica) da affiancare alla persona fisica e giuridica. Infine, si affronterà specificamente il problema della

interazione tra l'intelligenza artificiale e il diritto penale, principalmente in tema di responsabilità stradale, di responsabilità medica e di cybercrime "in senso ampio".

Lo scopo dell'articolo non è quello di fornire una risposta univoca ai quesiti che, inevitabilmente, si pongono in relazione all'intelligenza artificiale. L'obiettivo è far riflettere il lettore e fornire un quadro di analisi chiaro per spingere il giurista verso un futuro non molto lontano in cui esseri umani e tecnologia collaboreranno allo scopo di migliorare la vita degli individui.

Sommario: 1. "Le macchine sono in grado di pensare?" – 2. Tra scienza e dato normativo: la problematica definizione dell'intelligenza artificiale – 3. La personalità elettronica: un terzo genus*?* – 4. *Machina delinquere non potest* – 5. I reati "robotici" – 5.1 Le *self-driving cars* e i reati di omicidio e lesioni stradali – 5.2 L'uso dell'intelligenza artificiale in ambito sanitario e la responsabilità colposa del medico in caso di errore – 5.3 I *cybercrime* in senso ampio realizzati attraverso l'intelligenza artificiale – 6. Il diritto penale della società del rischio

1. "*Le macchine sono in grado di pensare?*"[1]

Si tratta di una delle frasi più celebri di Alan Turing: il padre dell'informatica. Siamo giunti in quella che viene comunemente denominata la quarta rivoluzione industriale, dominata da *robot* e macchine pensanti. Tali apparecchi informatici ed elettronici ci supportano e aiutano nella quotidianità, dagli assistenti vocali come *Alexa* o *Siri*, agli elettrodomestici che comunicano tra di loro, passando per le vetture dotate di guida autonoma.

Se di punto in bianco tutti i sistemi dotati della cosiddetta intelligenza artificiale dovessero sparire, la società rimarrebbe paralizzata. Molte attività, prima tipicamente manuali, sono state ora interamente automatizzate. Le macchine hanno sostituito gli esseri umani nel mondo del lavoro ma, al contempo, la tecnologia ha generato una richiesta continua di personale altamente specializzato che si possa occupare di realizzare ed educare l'algoritmo di *machine learning* contenuto all'interno di un *software* di intelligenza artificiale.

2. *Tra scienza e dato normativo: la problematica definizione dell'intelligenza artificiale*

Di recente capita sempre più spesso di assistere a conferenze di giuristi in cui si sente parlare di algoritmi, di digitalizzazione, di *software* e di automatizzazione, in cui si tratta di giudici *robot*, della integrale sostituzione degli avvocati con dei sistemi per il *computer*, ovvero di *cybercrime*, di *chatbot* e di *deep-fake*. Il mondo dell'informatica sta entrando nelle varie branche del diritto e non solo: in ambito sanitario si possono osservare *robot* che operano i pazienti sotto la supervisione del chirurgo[2] e algoritmi che possono suggerire al medico la migliore diagnosi e

cura per il singolo soggetto. [3]

Sembra la descrizione di un mondo idilliaco in cui macchine intelligenti e esseri umani possono convivere supportandosi a vicenda.

Ma cosa succede se un veicolo autonomo dotato di intelligenza artificiale investe un pedone? Chi risponde se il *robot* chirurgo sbaglia l'approccio medico? E se una *chatbot* inizia a diffamare un utente su una piattaforma *social*?

Non stiamo parlando di film fantascientifici, ma di realtà attuali che presto il legislatore dovrà affrontare al fine di adottare una disciplina di diritto penale che sia idonea a tutelare i vari interessi in gioco.

La prima difficoltà riscontrabile dal legislatore e dai giuristi in generale risulta essere l'assenza di una definizione scientifica universalmente accettata di cosa sia l'intelligenza artificiale che comporta di conseguenza difficoltà di definizione normativa.

La data di nascita (convenzionale) dell'intelligenza artificiale è il 1955 quando il matematico John McCarthy introdusse tale concetto al convegno al *Dartmounth College* di Hanover, New Hamphsire,[4] e affidandoci alla definizione fornitaci dal matematico statunitense Marvin Minsky, anch'esso presente al convegno: l'intelligenza artificiale è *"la scienza di far fare alle macchine cose che richiederebbero intelligenza se fatte dall'uomo."*[5] In realtà, l'evoluzione scientifica iniziò secoli prima, dall'abaco del 400 a.C., e proseguì oltre, fino ad arrivare al *robot* umanoide che forse verrà lanciato quest'anno da Elon Musk[6].

La straordinarietà dell'intelligenza artificiale è dovuta al fatto che tali sistemi hanno la capacità di interagire con il mondo esterno grazie ad un *software* basato su un algoritmo di autoapprendimento che trasforma gli *input* appresi dall'esterno in *output* permettendo alla macchina di migliorarsi autonomamente imparando dall'esperienza potendosi quindi discostare, in modo non sempre prevedibile, da quanto programmato dal suo creatore. L'oscurità dell'algoritmo gli garantisce la definizione di *black box algorithm.*

Nel mondo del diritto, queste difficoltà si riflettono a cascata, infatti, ad oggi, l'unica parvenza di testo vincolante risulta essere la Proposta di Regolamento del Parlamento Europeo del 21 aprile 2021[7] che ha come obiettivo la correttezza, la sicurezza e la trasparenza dell'intelligenza artificiale dividendola in base a due livelli di rischio: intollerabile (e vietato), perché in contrasto con i valori dell'Unione Europea e ad alto rischio, permessa nel rispetto di alcuni requisiti necessari allo scopo di garantire la sicurezza nell'uso. La Proposta, però, inoltre, non tratta di

aspetti di diritto penale afferenti all'intelligenza artificiale che ad oggi non viene disciplinata da nessuna norma specifica nonostante la stessa si stia facendo sempre più spazio in ambito processuale e sostanziale. Infatti, in fase di indagini, nelle operazioni polizia predittiva e di intercettazioni, l'intelligenza artificiale ricopre un ruolo di fondamentale ausilio per le operazioni di prevenzione degli illeciti e di raccoglimento delle prove; in fase di giudizio, l'intelligenza artificiale viene utilizzata (soprattutto negli Stati Uniti d'America[8] e in Cina) come sostegno e come sostituto del giudice nelle sue decisioni attraverso l'utilizzo di algoritmi per la valutazione della pericolosità sociale (non ancora ammessi in Italia per i limiti costituzionali dovuti al rischio di oscurità della motivazione e della non trasparenza della decisione); in sede di digitalizzazione della giustizia, l'intelligenza artificiale risulta risolutiva per lo scopo di velocizzare la ricerca di documenti e di facilitare l'accesso alle fonti; infine, in ambito di diritto penale sostanziale, l'intelligenza artificiale può rilevare come strumento, vittima o autore del reato (nel caso in cui venisse accettata la possibilità di riconoscere ai *robot* la personalità elettronica, di cui tratteremo a breve).

L'evoluzione porta con sé aspetti fortemente positivi ma al contempo, i rischi sono sempre dietro l'angolo. Proprio per questo, parlando di automazione è importante trattare del rapporto tra gli illeciti e l'intelligenza artificiale per comprendere chi debba essere considerato come penalmente responsabile per i reati commessi da tale tecnologia.

3. *La personalità elettronica: un terzo genus?*

Alla base di tale argomento sussiste una semplice e al contempo complessa domanda apparentemente estranea alle questioni giuridiche: cosa significa essere intelligenti? Le macchine possono realmente essere considerate tali? O si tratta di una mera razionalità connotata da un'assenza di libero arbitrio?

Le teorie di Gabriel Hallevy[9], un giurista israeliano, connesse all'ipotesi di istituire una personalità elettronica per i *robot* da affiancare alle comuni categorie dei soggetti di diritto (persona fisica e giuridica) al fine di affermare la sussistenza di una responsabilità penale in capo ai sistemi di intelligenza artificiale, vengono criticate[10] da questioni fondate essenzialmente sulla impraticabilità dell'analogia tra la mente umana e quella robotica, sul concetto di libero arbitrio e sull'effettiva coscienza e volontà di movimento posseduta da un sistema intelligente.

Secondo Hallevy le azioni poste in essere dall'intelligenza artificiale possono essere paragonate a quelle umane in quanto i *robot* sono dotati di una fisicità che gli permette di muoversi nello

spazio e di modificare l'ambiente circostante e, inoltre, essi sono mossi verso un obiettivo; dunque, i *robot* sono dotati di autonomia e razionalità che gli consente di rappresentarsi e di volere un determinato risultato, In tal modo si va a riconoscere la soddisfazione dei requisiti oggettivi e soggettivi del reato. Considerando tale teoria positiva, sarebbe così possibile far rispondere direttamente l'intelligenza artificiale dotata di personalità elettronica delle azioni illecite che va a realizzare.

In realtà, per quanto l'algoritmo si basi sul *machine learning* (che permette al sistema di apprendere dall'ambiente e di modificare il proprio comportamento esteriore), allo stato attuale della tecnica, i *robot* sono fortemente vincolati all'algoritmo che li domina, non hanno possibilità di decidere in modo pienamente autonomo e cosciente le azioni da intraprendere. Risultano dunque entità determinate, e quindi l'elemento soggettivo riscontrato è solo apparente: comportarsi come un essere umano non significa essere un essere umano.

4. *Machina delinquere non potest*

Dunque, risulta veritiero il brocardo "*machina delinquere non potest*" (formulato sulla falsa riga di quello prima applicabile alle società)?**[11]** Può un sistema intelligente essere considerato responsabile per gli illeciti che realizza?

Ad oggi sembra possibile dare una risposta affermativa al primo quesito: i sistemi intelligenti non sono ancora abbastanza autonomi da poter essere considerati come responsabili delle proprie azioni. Questo non può però affermarsi come certezza per il futuro, infatti, vista la rapidità di evoluzione della tecnologia, non è possibile escludere che in pochi anni l'abilità delle macchine e la loro autonomia superi o equivalga quella dell'essere umano.

Nell'attesa, per i reati commessi dai *robot* intelligenti, che non possono essere considerati come titolari di diritti e di doveri e che dunque non possono essere soggetti al diritto penale, siamo chiamati a valutare le possibili forme di responsabilità in capo a soggetti umani e quindi in base agli attuali canoni normativi in tema di responsabilità penale: la sussistenza di una posizione di garanzia in capo ad un soggetto specifico, un nesso causale tra l'azione della persona fisica e l'evento realizzato dalla macchina e soprattutto, l'esistenza di un elemento soggettivo, almeno al livello della colpa, al fine di evitare di ricadere in forme di responsabilità oggettiva.

Ipotizzare una responsabilità in capo al programmatore o utilizzatore, se si procede sulla scorta di automatismi, sconta il rischio di violare il principio di personalità e colpevolezza della responsabilità penale, come sancito dall'articolo 27 della Costituzione, ricadendo in inammissibili ipotesi di responsabilità oggettiva che il diritto penale non ammette. Dunque,

risulta necessario analizzare le azioni del *robot*, i cui meccanismi sono spesso oscuri (come una *black box*), per valutare se le persone fisiche che lavorano e agiscono intorno, tramite e attraverso i sistemi intelligenti, possano nel caso concreto prevedere a priori la realizzazione dell'evento lesivo.

Sarà configurabile, ovviamente, una responsabilità di tipo doloso in capo al soggetto utilizzatore o programmatore che utilizzi o programmi il sistema intelligente allo scopo di commettere illeciti.

Più complesso il tema della responsabilità colposa dell'operatore, in quanto, al fine di evitare di ricadere in forme di responsabilità oggettiva, sarà necessario valutare la sussistenza di un controllo significativo del programmatore sull'operato della macchina. Infatti, in base all'articolo 41 co.2 c.p., l'azione autonoma dell'intelligenza artificiale rientra nel concetto di causa sopravvenuta che rompe il nesso di causalità tra l'azione di programmazione posta in essere dal creatore dell'algoritmo e l'evento lesivo realizzato dal *robot*. Dunque, la persona fisica risponderà solo se possiede, in concreto, il potere e il dovere di evitare l'evento (articolo 40 cpv. c.p.).

In generale, invece, nel caso di responsabilità colposa del programmatore e del produttore, qualora gli stessi abbiano messo in commercio un *robot* intelligente consapevoli dei suoi rischi senza fare nulla per impedirli, si applicheranno, non sempre in modo chiaro e lineare, i criteri mutuati dalla responsabilità da prodotto difettoso (Direttiva 85/374/CEE)**[12]**. Allo stesso modo, non risulta semplice individuare un unico soggetto direttamente responsabile, in quanto, alla realizzazione di ogni singolo sistema intelligente collaboreranno un numero consistente di programmatori, ingegneri, scienziati, produttori e società.

5. *I reati "robotici"*

Tali disquisizioni possono risultare apparentemente solo teoriche e senza risvolti pratici. Proprio per questo è auspicabile, adesso, entrare nel vivo dei reati e del diritto penale così da comprendere a pieno che impatto l'intelligenza artificiale possa avere nella vita degli esseri umani.

Focalizzando, quindi, la nostra attenzione solo su tre tipologie di reati "robotici" (l'omicidio e le lesioni colpose stradali, la responsabilità medica e i *cybercrime* in senso ampio) è già possibile astrattamente immaginare le ricadute imponenti che l'intelligenza artificiale può avere sui diritti fondamentali degli individui e sui beni giuridici tutelati dall'ordinamento.

5.1. *Le self-driving cars e i reati di omicidio e lesioni stradali*

Infatti, con i veicoli autonomi i dubbi relativi alla responsabilità per i danni arrecati da un'autovettura non guidata da un essere umano, risultano notevoli: la possibilità di un controllo *ex ante* ed uno realizzato dal "guidatore-passeggero" persona fisica, l'ipotesi di realizzazione di un algoritmo del rischio che scelga lui discrezionalmente quale bene giuridico tutelare maggiormente e il tema dell'affidabilità dei sistemi intelligenti (connesso alla fiducia che la collettività può dargli). Difatti le autovetture autonome possono essere suddivise in sei livelli di automazione (da "zero" a "cinque").[13] Fino al livello "due" non si riscontrano particolari problematiche relative all'individuazione del soggetto responsabile per i reati di cui agli articoli 589 *bis* e 590 *bis* c.p. perché non sussiste alcuna sostituzione del guidatore da parte dell'intelligenza artificiale. Ciò perché, finché è presente un guidatore effettivo sul veicolo sarà lui il titolare dell'obbligo di prudenza, di controllo del veicolo e di rispetto del codice della strada e di conseguenza sarà lui a dover essere considerato come penalmente responsabile delle azioni di omicidio o lesioni gravi o gravissime dovute alla violazione del codice della strada. Le problematiche si iniziano a scorgere a partire dal livello "tre", ossia le vetture semi autonome in cui parte delle attività normalmente poste in essere dal guidatore, vengono delegate all'intelligenza artificiale. In tal caso, il guidatore continua ad essere presente sul veicolo e di conseguenza sarà lui a dover essere considerato come responsabile ma risulta complesso valutare l'effettivo controllo sull'autovettura che il soggetto possa esercitare: si rischia infatti di ricadere in una mera *fictio iuris*. Al livello "quattro" si può finalmente parlare di *self-driving car* in quanto il guidatore interviene solo eventualmente in situazioni di rischio, tutto il resto è delegato all'intelligenza artificiale. A tale livello, considerare il guidatore come il soggetto responsabile comporterebbe un passaggio da una condotta attiva (di guida non conforme) a una condotta passiva (di omesso controllo sul veicolo autonomo). Infine, nelle autovetture di livello "cinque", la figura del guidatore scompare del tutto, trasformandosi in un mero passeggero. Di conseguenza, qualora dovessimo giungere a tale livello di automazione, il legislatore dovrà necessariamente valutare nuove ipotesi di responsabilità o adattare le attuali norme sulla scorta, ad esempio, della responsabilità del produttore in caso di difetto del prodotto.

5.2. *L'uso dell'intelligenza artificiale in ambito sanitario e la responsabilità colposa del medico in caso di errore*

Passando all'ambito medico e sanitario, le scoperte tecnologiche permettono ai pazienti di riprendere la mobilità di arti paralizzati[14], di controllare il tremore del *Parkinson* e di mantenere sotto controllo i parametri vitali del soggetto al fine di somministrargli correttamente

i farmaci. Inoltre, gli algoritmi intelligenti supportano il medico nelle sue decisioni e diagnosi. Ma in caso di errore? Le vigenti fattispecie criminose risultano idonee ad affrontare anche tali situazioni?

Infatti, i rischi di *bias* dovuti a dati discriminatori che si ripercuotono sulla salute dei pazienti sono notevoli e questi possono andare ad influenzare le decisioni del medico ledendo dunque i diritti fondamentali dei soggetti.

In caso di errori sanitari, basandoci sull'articolo 590 *sexies* c.p., per come interpretato dalla Sentenza della Cassazione Penale a Sezioni Unite n. 8770 del 22 febbraio 2018**[15]**, l'operatore sanitario sarà esonerato da responsabilità nel caso di imperizia lieve in fase esecutiva nonostante il rispetto delle linee guida pubblicate ai sensi di legge e delle buone pratiche clinico assistenziali adeguate al caso concreto. **[16]**

La domanda da porsi è quindi se esistano linee guida idonee a regolare l'utilizzo dell'intelligenza artificiale in ambito sanitario. Purtroppo, ad oggi non sono presenti e infatti, l'Organizzazione Mondiale della Sanità, nel giugno del 2021 ha realizzato un *report* intitolato "*Ethics and Governance of Artificial Intelligence for Health*" **[17]** in cui spinge gli Stati ad adottare delle linee guida mirate per tali situazioni andando ad elencare i principi da dover rispettare al fine di tutelare i vari interessi in gioco. All'interno del documento, suddiviso in nove sezioni, viene fornita una definizione, di intelligenza artificiale e di *big data* sanitari, utile per individuare le principali applicazioni di tale tecnologia in medicina (come la ricerca, la gestione dei sistemi sanitari e il monitoraggio della salute pubblica). Vengono poi trattate le leggi e i principi (tutela dei diritti fondamentali, protezione dei dati personali, norme sull'utilizzo dei dati sanitari), anche di stampo etico, da dover rispettare nell'utilizzo della tecnologia innovativa. Infine, il *report* fornisce linee guida pratiche che dovrebbero essere seguite da parte di programmatori, ministeri della salute e operatori sanitari.

A seguito di tale analisi, l'OMS, nel rispondere alle domande sulla responsabilità del medico che si sia affidato al suggerimento proposto dal dispositivo intelligente, successivamente tradottosi in un errore, sottolinea le problematiche relative sia all'eccessiva limitazione sia all'eccessiva liberalizzazione dell'utilizzo dei sistemi intelligenti. Infatti, qualora si dovesse penalizzare il medico a causa di un errore dovuto all'essersi affidato al dispositivo intelligente, si limiterebbe fortemente l'evoluzione scientifica e tecnologica in abito sanitario che frenerebbe lo sviluppo di tali tecnologie in campo medico. Al contempo, qualora si giustificasse sempre il medico che pone in essere un'azione lesiva sul paziente, per il solo fatto di essersi affidato all'intelligenza

artificiale, si causerebbe un'eccessiva automatizzazione delle scelte mediche.

Sarebbe dunque opportuno realizzare delle linee guida accreditate specifiche per l'intelligenza artificiale per far si che il medico possa affidarsi ad esse potendosi così muovere all'interno di binari stabiliti e certi per non rischiare di ricadere in responsabilità dovendosi affidare a linee guida e buone pratiche clinico-assistenziali frammentarie e non aggiornate. Allo stato attuale sembra non esserci spazio per un'esenzione della responsabilità dell'operatore sanitario dovuta ad errore del sistema intelligente, in quanto non è possibile imputarla al *robot* essendo effettivamente un mero strumento nelle mani del medico; salvo, naturalmente, ipotesi di responsabilità da prodotto difettoso nel caso in cui i danni siano dovuti ad un difetto del *software* .

In tali due tipologie di reati (omicidio e lesioni personali stradali e responsabilità medica), il soggetto (guidatore o medico) non agisce con lo scopo di commettere un reato, ma l'evento lesivo si realizza comunque: bisognerà quindi valutare, per il guidatore, l'osservanza delle disposizioni dettate in materia di circolazione stradale, e per il medico, il rispetto delle linee guida e delle buone pratiche clinico-assistenziale. Solo nel caso in cui tali norme cautelari non vengano rispettate allora potrà essere ipotizzata una responsabilità colposa di tali soggetti.

5.3. *I cybercrime in senso ampio realizzati attraverso l'intelligenza artificiale*

Da ultimo, il tema dei reati informatici. La diffamazione e le *fake-news* rischiano di essere automatizzate tramite *chatbot* intelligenti che comunicano con gli utenti sui *social network* e imparano dai loro atteggiamenti: come avvenne nel 2016 con la *chatbot* "*Tay – Thinking About You*"[18] che attraverso il sistema di *machine learning* imparò dagli utenti della piattaforma "*Twitter*" a diffondere messaggi di odio e di discriminazione e per questo nell'arco di pochi giorni fu tolta dal mercato.[19] Inoltre, un fenomeno alquanto preoccupante riguarda il *deep-fake*, l'abilità di alcuni sistemi intelligenti di realizzare video falsi raffiguranti persone vere: possono consistere in falsi discorsi politici o in falsi video pornografici andando così a "spogliare" virtualmente un soggetto non consenziente. [20] È abbastanza evidente l'impatto che questo potrebbe avere sull'informazione e sulla vita personale delle vittime: una nuova frontiera del *revenge porn*. Difatti, il *deep-fake* è considerabile come una *dual-use technology*, in quanto può essere utilizzato sia per scopi leciti (come la realizzazione di film o videogiochi) che per scopi illeciti potendo rientrare in differenti fattispecie penali. Analizzando, però, attentamente l'articolo 612 *ter* c.p. punisce la diffusione di immagini o video sessualmente espliciti senza il consenso del soggetto raffigurato, è facile rendersi conto di come la norma non faccia alcun

riferimento ai contenuti non reali e dunque, nel rispetto del principio di tassatività della legge penale, le azioni di diffusione di immagini sessualmente esplicite senza il consenso della vittima ma realizzate attraverso la tecnica del *deep-fake,* nonostante siano comunque fortemente lesive della sfera intima del soggetto offeso, non potrebbero rientrare all'interno di tale fattispecie di reato. [21] Diametralmente opposta è invece la situazione relativa all'articolo 600 *quater* 1 c.p. che punisce la pornografia virtuale intesa come la realizzazione di video falsi raffiguranti minori andando ad anticipare la tutela della loro libertà sessuale. Infatti, tale fattispecie contempla la tecnica del *deep-fake* in quanto per video falsi si intendono anche le manipolazioni delle immagini e i fotomontaggi.

Dunque, sarebbe auspicabile un intervento legislativo che possa tutelare maggiormente le vittime di tali azioni lesive commesse con dolo (a differenza della responsabilità medica o per omicidio e lesioni stradali).

6. *Il diritto penale della società del rischio*

Concludendo, quando si sente parlare di tali sistemi, sembra sempre che riguardino un mondo lontano, futuro e inaccessibile. Invece, non è così. Il futuro è adesso ed è bene che si inizi ad affrontarlo. Il mondo dei reati robotici è già reale. Il diritto (come sempre) arriva in ritardo (e il penale in particolar modo): è normale, esso disciplina le situazioni concrete che di volta in volta si vanno a realizzare e non può ipotizzare situazioni future. Il legislatore rincorre i fenomeni che avvengono nella quotidianità e la funzione stessa del diritto penale impone che sia così, non essendo ammissibile in una democrazia occidentale avanzata l'utilizzo del sistema penale per "correggere" e "indirizzare" le condotte dei consociati verso scopi superindividuali. Il diritto penale, e quello punitivo latamente inteso, deve rimanere l'*ultima ratio*.

Infatti, per quanto possiamo girare la testa dall'altra parte e non pensare alle conseguenze (positive e negative) dell'evoluzione tecnologica, queste ci coinvolgono da vicino. Ed è necessario effettuare un bilanciamento in modo tale da non frenare lo sviluppo tecnologico e al contempo tutelare i diritti degli individui. Dunque, è prospettabile ipotizzare una legislazione penale basata sul principio della società del rischio.[22] Si tratta di un passaggio da una prospettiva *ex post* del diritto penale ad una prospettiva *ex ante* grazie all'individuazione di norme cautelari che devono essere rispettate dagli operatori che risulteranno in tal caso esenti da responsabilità perché si rientrerebbe in un'area di rischio consentito, tutelando così il progresso scientifico e l'essere umano.

*Cfr. in questa *Rivista* sul medesimo tema ***Algoritmi e intelligenza artificiale alla ricerca di una definizione: l'esegesi del Consiglio di Stato, alla luce dell'AI Act*** di Federica Paolucci dell'8 aprile 2022; ***La tecnologia amica del processo: dall'eredità dell'emergenza pandemica ai sistemi di giustizia predittiva*** di Roberto Natoli e Pierluigi Vigneri del 16 marzo 2022; e ***Il draft di regolamento europeo sull'intelligenza artificiale*** di Antonello Soro del 6 maggio 2021.

[1] A. M. Turing, "*Computing Machinery and Intelligence*," *Mind* 59, no. 236, 1950 (pag. 433–460).

[2] L. Mischitelli, "*Così i robot aiutano i chirurghi a operare meglio: progressi e prospettive della tecnologia*", in *Agendadigitale.eu*, 4 giugno 2021: **https://www.agendadigitale.eu/sanita/cosi-i-robot-aiutano-i-chirurghi-a-operare-meglio-progressi-e-prospettive-della-tecnologia/**

[3] M. Moruzzi, "*Robot sanitari alla sfida autonomia: la svolta «quinta dimensione»*", in *Agendadigitale.eu*, 21 ottobre 2020: **https://www.agendadigitale.eu/sanita/robot-sanitari-alla-sfida-autonomia-la-svolta-quinta-dimensione/**

[4]J. McCarthy, M. L. Minsky, N. Rochester e C.E. Shannon, "*A proposal for the Dartmouth summer research project on artificial intelligence*", Dartmouth College, Hanover, New Hamphsire, 1955: **http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf** .

[5] M.L. Minsky, "*Semantic information processing*", Cambridge, 1969.

[6]S. Campanelli, "*2022 anno del Tesla Bot, il robot umanoide da lavoro di Elon Musk*", Huffpost, 20/08/2021: **https://www.huffingtonpost.it/entry/tesla-bot-il-robot-umanoide-metallico-di-elon-musk_it_611f881ae4b0e8ac791d153d**.

[7] Commissione Europea, "*Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*", COM2021/206 final, Bruxelles 21/04/2021: **https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex:52021pc0206**

[8] State v. Loomis, 881 N.W.2d 749 (2016) 754 (USA).

[9] G. Hallevy, "*The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*", Akron Intellectual Property Journal: Vol. 4: Iss. 2, Article 1: **https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1**

[10] C. Piergallini, "*Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*" Rivista Italiana di Diritto e Procedura Penale, fasc.4, 1 dicembre 2020, pag. 1745; Paragrafo 4.1 "Machina artificialis

delinquere et puniri potest? Grundlinien di un (improbabile) diritto penale 'robotico'".

A. Cappellini, "*Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale",* in Criminalia: Annuario di scienze penalistiche, Edizioni ETS, 2018, Pisa: **https://discrimen.it/wp-content/uploads/Cappellini-Machina-delinquere-non-potest.pdf**

M.B. Magro, "*Decisione umana e decisione robotica un'ipotesi di responsabilità da procreazione robotica",* in La Legislazione penale, Giustizia Penale e nuove tecnologie, 2020, Dipartimento di Giurisprudenza, Università degli Studi di Torino, Torino: **http://www.lalegislazionepenale.eu/wp-content/uploads/2020/05/Magro-Giustizia-penale-e-nuove-tecnologie.pdf**

[11] A. Cappellini, "*Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale",* in Criminalia: Annuario di scienze penalistiche, Edizioni ETS, 2018, Pisa: **https://discrimen.it/wp-content/uploads/Cappellini-Machina-delinquere-non-potest.pdf**

[12]Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al "*Ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi*": **https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31985L0374&from=IT**

[13] A. Cappellini, "*Profili penalistici delle self-driving cars*" (pag. 325 – 353) in "*Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione*", IX Corso di formazione interdottorale di Diritto e Procedura penale "Giuliano Vassalli" per dottorandi e dottori di ricerca. AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre – 1 dicembre 2018. In Diritto penale Contemporaneo, Rivista trimestrale 2/2019. Paragrafo 2 (pag. 327 – 328) "Dalle auto semi-autonome a quelle totalmente *self-driving*: i "livelli" di automazione".

I. Salvadori, "*Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*", Rivista Italiana di Diritto e Procedura Penale, fasc.1, 1 marzo 2021, pag. 83; Paragrafo 3, "Dall'automazione all'autonomia: classificazione degli agenti artificiali".

[14] M. B. Magro, "*Biorobotica, robotica e diritto penale*", in D. Provolo, S. Riondato, F. Yenisey (a cura di), Genetics, Robotics, Law, Punishment, Padova University Press, 2014, pp. 510 s.

[15] Sentenza della Cassazione Penale, Sezioni Unite, n. 8770 del 22 febbraio 2018: **https://www.biodiritto.org/ocmultibinary/download/3259/31842/8/ba374071a4619dfb28edf5d0587fb31pen-sez-un-2018-8770.pdf**

[16] F. Cembrani, "*Irresponsabilità penale del medico e qualità metodologica del sapere scientifico codificato medical and methodological quality of the scientific code*", Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario), fasc.2, 1 aprile 2019.

[17] WHO, World Health Organization, "*Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*", *Ginevra, 2021:* **https://www.who.int/publications/i/item/9789240029200**

[18] E. Hunt, "*Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter*", The Guardian, 24/03/2016: **https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter**

[19]E. Capone, "*Le intelligenze artificiali fra razzismo e questione etica*", 06/04/2021, IT Italian.Tech, Parte del gruppo GEDI e la Repubblica: **https://www.italian.tech/2021/04/06/news/le-intelligenze-artificiali-fra-razzismo-e-questione-etica-299491573/**

[20] F.M.R. Livelli, "*Deepfake e revenge porn, combatterli con la cultura digitale: ecco come*", in Network Digital 360 – Cybersecurity 360, 8 febbraio 2021: **https://www.cybersecurity360.it/nuove-minacce/deepfake-e-revenge-porn-combatterli-con-la-cultura-digitale-ecco-come/**

[21] N. Amore, "*La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612 ter c.p.*", in Legislazione penale, 20 gennaio 2020: **http://www.lalegislazionepenale.eu/wp-content/uploads/2020/01/N.-Amore-Approfondimenti-1.pdf**

[22] S. Arcieri, "*Percezione del rischio e attribuzione di responsabilità*", in Diritto Penale e Uomo (DPU) – Criminal Law and Human Condition, Fascicolo 10/2020, 28 ottobre 2020, Milano: **https://dirittopenaleuomo.org/wp-content/uploads/2020/10/douglas_DPU.pdf**.