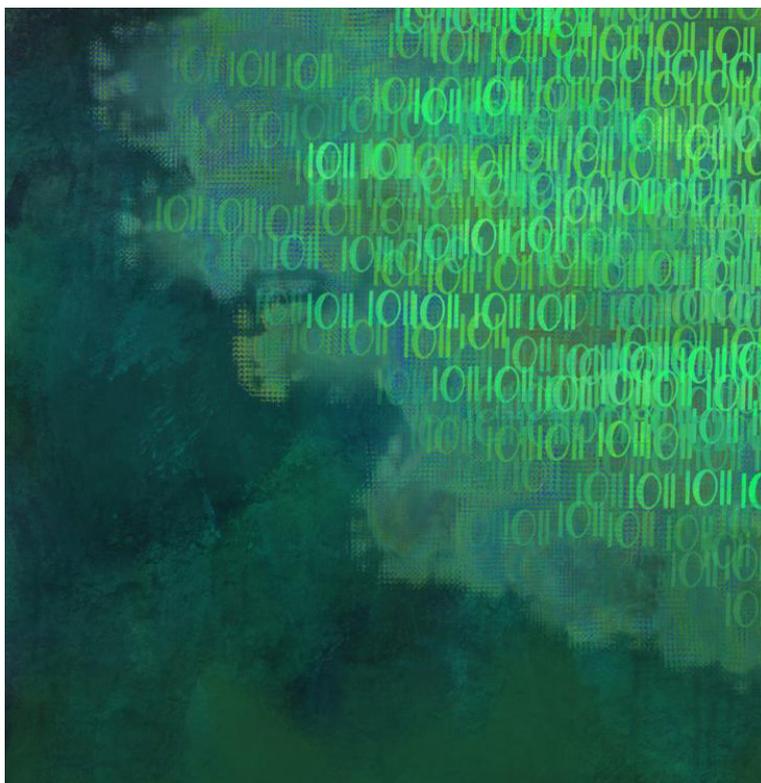


# La sostenibilità dell'innovazione digitale

a cura di

**Ilaria Garaci e Roberta Montinaro**



UniorPress







UNIVERSITÀ DI NAPOLI L'ORIENTALE  
DIPARTIMENTO DI SCIENZE UMANI E SOCIALI

# La sostenibilità dell'innovazione digitale

a cura di  
**Ilaria Garaci e Roberta Montinaro**



UniorPress  
Napoli 2023

*In copertina:* 0110, Indigo Picciano, 2023.

La sostenibilità della innovazione digitale  
a cura di Ilaria Garaci e Roberta Montinaro  
UniorPress, Napoli 2023. ISBN 978-88-6719-276-2



With the support of the  
Erasmus+ Programme  
of the European Union

Edizione digitale con licenza  
Creative Commons Attribution 4.0 International



**UniorPress** - Via Nuova Marina 59, 80133 - Napoli  
[www.uniorpress.unior.it](http://www.uniorpress.unior.it)

## INDICE

ROBERTA MONTINARO	
<i>La sostenibilità dell'innovazione digitale. Un'introduzione</i>	7
ENRICO CATERINI	
<i>Artificial intelligence, persona e soggetto</i>	23
MARCO FASCIGLIONE	
<i>I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale</i>	89
ILARIA GARACI	
<i>La valutazione d'impatto sui diritti fondamentali dei minori di età nell'ambiente digitale. Riflessioni a margine della proposta di direttiva relativa alla due diligence delle imprese ai fini della sostenibilità e del Digital Services Act</i>	113
FRANCESCO MEZZANOTTE	
<i>Rischio e responsabilità nei sistemi dell'Internet of Things</i>	137
ANTONINA ASTONE	
<i>Consenso ed intelligenza artificiale: limiti e prospettive</i>	187
ANTONELLA CORRENTI	
<i>Piattaforme tecnologiche: protezione ed educazione dell'utente all'utilizzo delle infrastrutture informatiche nei mercati a concorrenza imperfetta</i>	217
ROSARIO PETRUSO E GUIDO SMORTO	
<i>Trasformazione della filiera distributiva e responsabilità delle piattaforme del commercio elettronico nella proposta di direttiva "sulla responsabilità per danno da prodotti difettosi"</i>	245
ENRICO AL MUREDEN	
<i>Tutela della persona e limitazione dell'errore umano tra Advanced Driver Assistance Systems e guida automatizzata di livello 3</i>	299

MARCO CARLIZZI	
<i>Sostenibilità e innovazione nell'attività bancaria: il conto di base come soluzione per chi abbia ridotte capacità cognitive</i>	323
ETTORE BATTELLI	
<i>Gli smart-contract nel mercato delle assicurazioni: limiti e opportunità</i>	361
GIOVANNI BERTI DE MARINIS	
<i>L'algo-governance nelle imprese di assicurazione e l'integrazione dei fattori ESG</i>	405
SARA LANDINI	
<i>Sostenibilità e diritto dei privati. Il caso dei contratti sostenibili nel settore turistico</i>	431
INDICE DEGLI AUTORI IN ORDINE ALFABETICO	459

# I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale<sup>1</sup>

MARCO FASCIGLIONE

Sommario: 1. Introduzione. - 2. Algoritmi e nuove forme di potere. - 3. Nuove tecnologie, valori ed individuo. - 3.1. L'incidenza sulla formazione del consenso individuale e la comunicazione delle idee. - 3.2. L'incidenza sull'autonomia e della capacità di autodeterminarsi dell'individuo. - 3.3. L'incidenza sul valore della dignità umana. - 4. Responsabilità e diritti umani nella società degli algoritmi. - 5. Conclusioni.

## 1. Introduzione

Il *machine learning*, gli algoritmi e le altre applicazioni dell'intelligenza artificiale stanno influenzando in modo sempre più crescente ogni tipo di attività umana. Gli effetti derivanti dallo sviluppo di queste tecnologie sono ovunque e hanno dimostrato di comportare sia conseguenze positive sia il rischio di interferire negativamente sulla vita delle persone. Da un lato, esse hanno aperto la via a nuove opportunità di espansione della produttività, di sviluppo economico e di progresso in molteplici settori. Dall'altro lato, il loro sviluppo, celere e non regolamentato, e la loro capacità intrusiva nella società pongono rischi per gli individui e per la salvaguardia dei loro diritti umani. Sotto il primo aspetto, tali tecnologie possono essere utili alla salvaguardia dei diritti umani grazie all'impatto positivo che esse possono avere, tra le altre cose, sui diritti delle donne, sul diritto alla salute, sui diritti degli anziani. L'automazione di lavori pericolosi può migliorare significativamente la salute e la sicurezza sul lavoro. Allo stesso modo, l'uso delle tecnologie collegate all'intelligenza artificiale, lo sviluppo di c.d. '*smart cities*' e di dispositivi connes-

si può contribuire a ridurre le emissioni di gas serra e ad aiutare pertanto a mitigare l'impatto negativo derivante dai cambiamenti climatici. Sotto il secondo punto di vista, tuttavia, le potenzialità dell'intelligenza artificiale, basate sui *big data*, sugli algoritmi e sui calcoli predittivi, combinate con la pervasività dei dispositivi e dei sensori del c.d. *Internet of Things*, sono in grado di incidere nel governo delle funzioni fondamentali della società, dall'istruzione alla salute, dalla scienza all'economia fino alla sfera del diritto, della sicurezza e della difesa, del discorso politico e del processo decisionale democratico. Tutto ciò sta animando da diversi anni un profondo e vivace dibattito nell'opinione pubblica, e tra gli studiosi, circa l'impatto del progresso tecnologico sui valori fondanti delle società contemporanee: la democrazia, il rispetto dello stato di diritto e la *rule of law*, la garanzia dei diritti umani. Un dibattito quindi niente affatto nuovo ma che, proprio a causa della vertiginosa accelerazione del processo tecnologico è di stringente attualità<sup>2</sup>.

Queste brevi pagine perseguono, senza pretesa di esaustività, l'obiettivo di capire quale possa essere il ruolo del diritto internazionale dei diritti umani nella società dell'intelligenza artificiale e come prevenire conseguenze negative sui diritti umani di individui, comunità, eccetera, messi in pericolo da processi decisionali algoritmici. Ebbene, a giudizio di chi scrive le risposte a tale quesito richiedono l'utilizzo di tre chiavi di lettura. La prima attiene all'analisi del ruolo giocato dalle *nuove forme di potere* che si affacciano e agiscono nella contemporanea società degli algoritmi. La seconda chiave di lettura, riguarda l'analisi della capacità delle nuove tecnologie di incidere sui *valori* che si sono cristallizzati nell'ordinamento giuridico internazionale, ed in particolare negli strumenti internazionali di tutela dei diritti umani. La terza chiave di lettura, infine, attiene all'emersione di nuove *forme di responsabilità* dei diversi attori che operano nella contemporanea società degli algoritmi.

## 2. Algoritmi e nuove forme di potere

Partiamo dalla nozione di *potere*. Nella società degli algoritmi e dell'intelligenza artificiale emergono *nuove forme* di potere che possono mettere a rischio i diritti umani. Tali nuovi poteri si affiancano – o possono sostituirsi del tutto – ai tradizionali centri di esercizio del potere, sarebbe a dire gli Stati, intorno ai quali è si è tradizionalmente configurato il sistema internazionale di tutela dei diritti umani. Le imprese, tanto quelle del settore *High-tech* che sviluppano le tecnologie in esame, ma anche quelle che poi utilizzano tali tecnologie nei propri processi produttivi e commerciali, rappresentano una di queste nuove forme di potere, in grado di incidere sul godimento e sulla protezione dei diritti umani. Provo a spiegarmi con un esempio, quello delle c.d. *smart supply chains* in cui l'intelligenza artificiale può essere applicata in ottica di *capacity planning* come strumento per 'ottimizzare' le decisioni nell'organizzazione della catena del valore. Immaginiamo un'intelligenza artificiale che venga installata nei server di una grande azienda, ad es. una multinazionale dell'*automotive* che vende veicoli destinati al trasporto di beni e persone. Nei servizi e nei prodotti commercializzati da una tale ipotetica azienda possono rientrare: auto, furgoni, motrici, i pezzi di ricambio, le soluzioni energetiche (magari elettriche o ibride) che alimentano tali veicoli, le soluzioni finanziarie per il loro acquisto (e le relative banche e finanziarie gestite o partecipate dall'impresa) e tutta la filiera di fornitori e sub-fornitori situati in diverse aree del Pianeta. Immaginiamo che tale intelligenza artificiale sia 'autorizzata' dai suoi 'creatori' ad interagire sull'intera filiera dell'impresa allo scopo di migliorarne ed ottimizzarne la *value chain* per aumentare la produttività e massimizzare il profitto, e che nell'esercizio di tale compito le sia imposto come 'limite regolamentare' l'osservanza delle singole normative esistenti nei rispettivi or-

dinamenti nazionali interessati dalle attività dell'impresa. Quali le conseguenze? Essa potrà trovare soluzioni creative per raggiungere gli obiettivi dell'impresa: dalla creazione di sofisticate *shell companies* per sottoporsi a regimi fiscali più convenienti rispetto a quelli dove la multinazionale ha la propria sede, a strategie di acquisizione di risorse (materie prime, personale di ricerca, manodopera etc..) volte a contenere i costi attraverso l'impiego di processi di produzione che, seppur non illegali in quello specifico Stato, potrebbero sfociare in danni all'ambiente, alle persone e a comunità. In altri termini, quest'ipotetica intelligenza artificiale potrebbe sfruttare i *gap* regolamentari tra gli ordinamenti giuridici dei diversi Stati (ad es, le leggi nazionali giuslavoristiche, quelle sulla salvaguardia dell'ambiente) in modo tale che, pur rispettando le leggi dello Stato di origine, potrebbe ripianificare l'intera filiera spostando la produzione dove è 'più conveniente' per l'impresa. Il tutto per massimizzare il profitto! Non una novità per i modelli di business contemporanei in cui il principio della c.d. *shareholder primacy* obbliga le aziende a sfruttare l'opportunità concessa dai meccanismi di produzione lungo le catene di fornitura globali per ridurre i costi e massimizzare i profitti<sup>3</sup>, ma che un sistema di *machine learning* altamente evoluto può realizzare con migliore efficacia, spingendolo all'estremo con un potenziale 'effetto scalare' devastante per il pianeta e la società.

È esattamente in questa prospettiva di analisi che il dibattito sulle nuove tecnologie interseca quello sulle 'nuove forme di potere' ed in modo particolare quello sull'emersione di *nuovi attori* sulla scena internazionale che sempre più spesso contribuiscono, accanto agli Stati, alla formazione e all'attuazione delle norme di diritto internazionale. In un ambiente digitale globale le interferenze con il godimento dei diritti umani "non provengono solo dall'attuazione di tecnologie digitali da parte di attori pubblici, ma anche, e principalmente, dalla capacità

degli attori privati transnazionali di sviluppare e applicare standard privati in concorrenza con valori pubblici”<sup>4</sup>. In questa ottica, uno dei settori maggiormente in fermento riguarda il ruolo del settore privato nel sistema internazionale ed in modo particolare l’impatto delle attività delle *imprese* sui diritti umani con il processo di emersione di standard internazionali volti a disciplinare la condotta delle stesse in funzione di una loro “responsabilizzazione” in materia di diritti umani. Lo strumento internazionale di riferimento in materia è rappresentato dai Principi Guida ONU su imprese e diritti umani adottati nel 2011 dal Consiglio dei diritti umani delle Nazioni Unite<sup>5</sup>. Suddivisi in tre pilastri, il primo incentrato sull’obbligo statale di proteggere i diritti umani dalle violazioni riconducibili alle attività delle imprese, (il c.d. *State duty to protect*), il secondo relativo alla responsabilità delle imprese di rispettare i diritti umani (la c.d. *corporate responsibility to respect*), ed il terzo, infine, concernente il diritto di accesso ai rimedi per le vittime (c.d. *access to remedies*), i Principi Guida costituiscono il primo standard realmente ‘globale’ in materia. Nonostante essi non siano uno strumento vincolante hanno guadagnato un generale ed unanime consenso essendo diventati nel giro di pochi anni il principale standard internazionale in materia e sono stati riconosciuti da Stati, Organizzazioni internazionali, imprese, associazioni di categoria, ordini forensi, società civile e da tutti gli organismi onusiani che operano nel settore dei diritti umani<sup>6</sup>.

Il secondo pilastro dei Principi guida è particolarmente interessante ai fini della nostra analisi. In effetti esso fissa uno ‘standard di condotta attesa’ per le imprese che consiste nella responsabilità di evitare le violazioni dei diritti umani che esse possano *causare o contribuire a causare* e di prevenire l’impatto negativo sui diritti umani che deriva dalle attività di terze parti e che sia direttamente collegato alle loro operazioni, ai loro prodotti o servizi, in ragione di un rapporto commerciale con un

ente terzo<sup>7</sup>. Come è noto, il nucleo centrale di questa responsabilità si fonda su di uno standard di *due diligence* la c.d. *due diligence* aziendale sui diritti umani, che impone di cercare di prevenire l'impatto negativo sui diritti umani che può derivare dalle proprie operazioni economiche attraverso l'utilizzo di idonei processi volti a identificare, prevenire e rendere conto di come tali impatti vengono affrontati, nonché di porre loro rimedio<sup>8</sup>. Si tratta di un meccanismo di *risk-assessment* che si sostanzia in un processo continuativo di gestione del rischio che un'impresa ragionevole e prudente deve intraprendere, alla luce delle sue caratteristiche (settore di attività, contesto operativo, dimensioni e simili fattori) per far fronte alla sua responsabilità di rispettare i diritti umani<sup>9</sup>. Si tratta, insomma, di un approccio definibile come *human rights by design* all'impatto negativo delle attività di impresa sui diritti umani, che è applicabile anche alle imprese che sviluppano e/o utilizzano le moderne tecnologie digitali, basate sul *machine learning*, sull'intelligenza artificiale, ecc. Le imprese del settore tecnologico, infatti, già applicano un meccanismo, analogo ma più circoscritto, di valutazione del rischio di impatto negativo quando integrano le considerazioni in materia di tutela della *privacy* durante le fasi più importanti dello sviluppo di un prodotto (la c.d. *privacy by design*)<sup>10</sup>. In altre parole, la *due diligence* sui diritti umani si estende anche alle situazioni relative allo sviluppo e all'impiego di tali tecnologie, con le imprese che sono tenute a dimostrare di aver adottato tutte le misure appropriate per garantire la protezione dei diritti umani che potrebbero essere potenzialmente compromessi, in aggiunta e accanto alle questioni collegate alla tutela della *privacy*.

Se gli standard internazionali in materia di impresa e diritti umani già richiedono alle imprese di effettuare una *due diligence* generale sui diritti umani quando sviluppano e utilizzano tecnologie basate sugli algoritmi, stupisce allora che tale approccio regolamentare basato sull'adozione di misure preventive sia

assente dalla bozza di regolamento della Commissione europea del 2021 volta a fissare delle regole armonizzate in materia di intelligenza artificiale (il c.d. *Artificial intelligence Act*)<sup>11</sup>. La proposta di regolamento mira a garantire, tra le altre cose, che i sistemi di intelligenza artificiale immessi sul mercato dell'Unione e ivi utilizzati siano *sicuri* e rispettino la normativa vigente in materia di *diritti fondamentali* e i valori dell'Unione, nonché a garantire una migliore *governance* e che le autorità e i tribunali nazionali competenti possano indagare e affrontare più efficacemente eventuali violazioni degli obblighi in materia di diritti fondamentali in presenza di violazioni dei requisiti di sicurezza applicabili ai sistemi di intelligenza artificiale. Purtroppo, la proposta attualmente pendente non include alcun riferimento ai Principi Guida ONU, né all'adozione di una *due diligence* generale in materia di diritti umani per le imprese che si avvalgono di questa tecnologia, né ad altri analoghi standard internazionali in materia di imprese e diritti umani. Non può essere considerato espressione di uno *human rights by design* il riferimento, contenuto nell'articolo 54 della proposta di regolamento, che, in relazione alla raccolta e al trattamento di dati personali nel processo di sperimentazione e utilizzo di sistemi di intelligenza artificiale, rinvia, alla lettera c), alla necessità che esistano effettivi meccanismi di monitoraggio per identificare qualsiasi rischio elevato per i 'diritti fondamentali' delle persone interessate, nonché a meccanismi di 'risposta' (c.d. *response*) per mitigare prontamente tali rischi e, ove necessario, interrompere l'utilizzo di tali sistemi. Tantomeno ciò può valere per la formulazione dell'articolo 67 della proposta di regolamento che prevede che qualora il sistema di intelligenza artificiale presenti un rischio per la salute o la sicurezza delle persone, oppure per la conformità agli obblighi previsti dal diritto dell'Unione, o da quello nazionale, a tutela dei diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, l'autorità di vigilan-

za del mercato di uno Stato membro può chiedere all'operatore di adottare tutte le misure adeguate a far sì che il sistema in esame, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio o che sia, a seconda dei casi, ritirato dal mercato o richiamato entro un termine ragionevole, proporzionato alla natura del rischio. In entrambi i casi in effetti, la formulazione della proposta di regolamento non è allineata con le disposizioni del secondo pilastro dei Principi Guida ed il processo di *due diligence* aziendale sui diritti umani ivi disciplinati<sup>12</sup>. Siffatta mancanza è ancora più grave ove si consideri che il regolamento persegue l'obiettivo di assicurare la coerenza con il diritto dell'Unione ed in modo particolare con la Carta dei diritti fondamentali dell'UE e con le politiche dell'Unione in materia di dati ed in particolare con il regolamento generale sulla protezione dei dati 2016/679. Nulla si dice, né si rinvia in alcun modo al processo legislativo avviato dal legislatore europeo e destinato all'adozione di una direttiva della Commissione volta ad introdurre un obbligo per il settore privato europeo di *due diligence* in materia di diritti umani ed ambiente applicabile anche lungo le *supply chains* (la c.d. *corporate sustainability due diligence*)<sup>13</sup>. Insomma, armonizzare gli sforzi di questi due processi legislativi sarebbe stato, ed è tutt'ora, auspicabile.

### 3. Nuove tecnologie, valori ed individuo

Passiamo alla nozione di *valori*. Il *machine learning* e la tecnologia dell'intelligenza artificiale 'toccano' tre valori centrali della sfera personale dell'individuo: a) la formazione del *consenso* individuale e la comunicazione delle idee; b) l'autonomia e la capacità di *autodeterminarsi* dell'individuo; c) l'essenza dell'uomo, la sua *dignità*. Tutti e tre questi aspetti si trovano al centro del sistema di valori su cui si basano gli strumenti internazionali di tutela dei diritti umani.

### 3.1. L'incidenza sulla formazione del consenso individuale e la comunicazione delle idee

Per quanto riguarda il primo aspetto, le tecnologie in esame pongono complesse sfide alla formazione e alla comunicazione del *consenso individuale*, entrambe indispensabili per la rivendicazione e la protezione di qualsiasi diritto umano, sia esso civile, politico, economico, sociale o culturale. A ben vedere, la distorsione delle informazioni, la mancanza di processi trasparenti, il controllo sulle informazioni personali comportano in misura crescente la diluizione del nostro consenso individuale al punto tale da mettere in pericolo le stesse fondamenta del modo con cui affermiamo i nostri diritti umani e riteniamo che gli altri siano responsabili della loro violazione. Esempio plastico di quanto andiamo dicendo è rappresentato dallo scandalo *Facebook/Cambridge Analytica*. I fatti sono noti. Un ricercatore dell'Università di Cambridge aveva sviluppato un *App* da far girare in Facebook e che attraverso la somministrazione di un sondaggio riusciva a produrre profili psicologici e di previsione del comportamento degli utenti, basandosi sulle attività da questi svolte online. L'*App* fu scaricata da centinaia di migliaia di utenti di Facebook ed essa riuscì maliziosamente a memorizzare dati sensibili di vario tipo di circa 50 milioni di profili Facebook. Il ricercatore condivise (in violazione dei termini d'uso di Facebook) queste informazioni con *Cambridge Analytica* una società specializzata nel raccogliere dai social network dati sui loro utenti per creare profili di ogni utente da utilizzare attraverso un sistema di 'microtargeting comportamentale' sviluppato dall'impresa in questione. Un sistema, insomma, destinato a sviluppare messaggi pubblicitari altamente personalizzati per ogni singola persona ed in grado di far leva non solo sui gusti, ma anche sulle emozioni degli utenti. I dati raccolti erano in grado, pertanto, di creare profili psicologici dei titolari dei dati: questi profili abbinati al sistema di pubblicità

personale sarebbero stati utilizzati a scopi di propaganda politica per condizionare cento campagne elettorali in oltre trenta Stati<sup>14</sup>. Lo scandalo *Facebook/Cambridge Analytica*, con i rischi da esso palesati di distorsione dell'informazione di massa, di violazione della *privacy* per milioni di persone in tutto il mondo, mette in discussione il diritto dei cittadini a partecipare liberamente alla gestione degli affari pubblici e a votare in elezioni che garantiscano la libera espressione della volontà degli elettori così come garantito a livello universale dall'art. 25 del Patto sui diritti civili e politici, e a livello regionale europeo dall'art. 3 del Protocollo No. 1 della CEDU<sup>15</sup>.

Se le distorsioni dell'informazione, come quelle esaminate in relazione allo scandalo *Facebook/Cambridge Analytica*, mettono in discussione l'autentica natura e l'effettiva portata del consenso prestato dagli individui all'utilizzo di sistemi di *machine learning* e di intelligenza artificiale, l'altro lato della medaglia è rappresentato dal deficit di trasparenza circa come le imprese dell'*High-tech* utilizzano e condividono i dati degli utenti. In effetti nonostante il fatto che la comunicazione volontaria delle politiche in materia di trasparenza sia diventata uno standard del settore tecnologico<sup>16</sup>, tuttavia, continua a sussistere una diversità di approcci alla trasparenza in relazione all'utilizzo di algoritmi e di tecnologie di intelligenza artificiale, e continuano a sussistere differenze di tipo regolamentare e giurisdizionale nei diversi ordinamenti nazionali. Resta soprattutto aperta la questione relativa al se gli individui riescano a rilasciare effettivamente e realmente un consenso, consapevole, libero e informato all'utilizzo, condivisione o al trattamento dei loro dati da parte delle imprese del settore tecnologico quando si relazionano con le tecnologie digitali. A questo proposito l'Unione Europea sembra essere sempre più all'avanguardia a livello globale nel cercare di garantire siffatto consenso consapevole, informato e libero. Le *Ethics Guidelines for Trustworthy Artificial Intelligen-*

ce adottate nel 2019 dall'*High-Level Expert Group on Artificial Intelligence*<sup>17</sup>, infatti, individuano sette condizioni affinché le tecnologie fondate su algoritmi e simili possano definirsi 'affidabili' (*trustworthy*). Si tratta di assicurare 1) il controllo e supervisione da parte dell'uomo; 2) la solidità tecnica e sicurezza; 3) il rispetto della privacy e della *governance* dei dati; 4) la trasparenza; 5) la salvaguardia della diversità, della non discriminazione e dell'equità; 6) il benessere sociale e ambientale; 7) la responsabilità.

### 3.2. L'incidenza sull'autonomia e sulla capacità di autodeterminarsi dell'individuo

Per quanto attiene al secondo valore, quello dell'*autonomia* e della *capacità di autodeterminarsi* dell'uomo, tali valori costituiscono come evidenziato, in un recente scritto, dal Presidente della Corte europea dei diritti dell'uomo il "fondamento morale" della stessa nozione di *rule of law* in quanto funzionali all'esclusione di qualsiasi forma di arbitrio da parte dei governi e dei poteri, sia pubblici che privati<sup>18</sup>. Ebbene i fenomeni di c.d. *autoritarismo digitale*, in cui le tecnologie algoritmiche e di intelligenza artificiale vengono utilizzate come strumento di controllo sociale e di sorveglianza di polizia, in funzione di un 'rimodellamento delle forme di repressione'<sup>19</sup> non fanno altro che mettere in crisi l'autonomia personale e la capacità di autodeterminarsi dell'individuo e mettono quindi "sotto pressione" il funzionamento dello stesso principio di *rule of law*<sup>20</sup>. Il riferimento va ai sistemi di riconoscimento facciale, a quelli automatici di riconoscimento delle emozioni, alla sorveglianza digitalizzata, ma anche alle tecniche di disinformazione, all'utilizzo di *fake news*, cui tutti siamo chi in misura maggiore, chi in misura minore, esposti. È una prassi, questa passata in rassegna, che può costituire in assenza di meccanismi di bilanciamento e controllo, un pericoloso e subdolo

meccanismo di interferenza nei diritti fondamentali della persona umana.

È necessario, insomma, che le convenzioni e gli altri strumenti internazionali sui diritti umani – e gli obblighi che derivano da tali strumenti – guidino gli Stati e le loro azioni in materia di cooperazione digitale, e fare in modo che i diritti umani ricevano applicazione per garantire che le tecnologie digitali nuove ed emergenti non causino lacune di tutela. Il punto centrale è: in che modo fare ciò?

Ora, a noi sembra che superato, e da tempo, ogni dubbio relativamente al se il diritto internazionale dei diritti umani possa e debba ricevere applicazione all'era dell'intelligenza artificiale, la risposta alla domanda di cui sopra passa attraverso il riconoscimento che quando governi autocratici violano i diritti civili e politici attraverso misure di repressione digitale, oppure quando violano i diritti economici, sociali e culturali condizionando l'erogazione dei servizi pubblici (che si tratti del diritto al più alto livello raggiungibile di salute fisica e mentale, del diritto alla sicurezza sociale, del diritto all'istruzione, del diritto a partecipare alla vita culturale, del diritto a un adeguato tenore di vita) a meccanismi di controllo sociale non trasparenti e discriminatori, nulla di 'nuovo' emerge rispetto alle forme .. 'più tradizionali' di intrusione nella autonomia personale dell'individuo. Il problema va risolto, allora, nella logica della *responsabilità* dello Stato di *rispettare, proteggere e realizzare* i diritti umani sanciti nelle convenzioni internazionali<sup>21</sup>. Tale responsabilità scaturisce dal dovere degli Stati di regolamentare le attività degli enti economici privati – anche quelli che sviluppano e utilizzano tecnologie digitali – che si trovano sotto il loro controllo e/o giurisdizione anche quando queste attività dispieghino effetti in Paesi terzi. Con riferimento al settore dei diritti economici, sociali e culturali, questa impostazione è stata materialmente applicata dal Comitato per i diritti economici, sociali

e culturali nel Commento generale n. 24 dedicato specificamente agli obblighi che dal Patto del 1966 discendono sugli Stati contraenti in relazione alle attività delle imprese<sup>22</sup>. Il Comitato, in effetti, ha evidenziato come gli Stati contraenti siano obbligati ad adottare le misure necessarie per regolare le attività delle imprese che possono incidere negativamente sui diritti economici, sociali e culturali, e in particolare per evitare la discriminazione di lavoratori e migranti, quella sessuale, quella religiosa o razziale e le altre forme di discriminazione. Il Comitato ha sottolineato che l'obbligo di *rispettare* i diritti economici, sociali e culturali risulta violato "quando gli Stati parte attribuiscono priorità agli interessi commerciali delle imprese rispetto alle garanzie previste dal Patto senza alcuna giustificazione, o quando perseguono politiche che influiscono negativamente su tali diritti"<sup>23</sup>. L'obbligo di *proteggere*, invece, comporta secondo il Comitato che gli Stati contraenti "devono prevenire effettivamente qualsiasi violazione dei diritti economici, sociali e culturali che possa verificarsi nel quadro delle attività commerciali". Secondo il comitato, ciò richiede che gli Stati contraenti "adottino misure legislative, amministrative, educative e altre misure appropriate per garantire un'effettiva protezione contro le violazioni dei diritti del Patto collegate alle attività delle imprese e che forniscano alle vittime di tali violazioni l'accesso a delle vie di rimedio effettive"<sup>24</sup>. L'obbligo di realizzare, infine, impone agli Stati contraenti di adottare le misure necessarie, "nel massimo delle risorse disponibili, per facilitare e promuovere il godimento dei diritti sanciti dal Patto e, in alcuni casi, per fornire direttamente beni e servizi essenziali a tale godimento"<sup>25</sup>.

Di particolare rilevanza ai fini della nostra analisi è, inoltre, il fatto che il Comitato non abbia esitato a porre in evidenza come "gli obblighi degli Stati contraenti ai sensi del Patto non si fermano ai loro confini territoriali" e che essi sono tenuti ad "adottare le misure necessarie per prevenire le violazioni dei

diritti umani all'estero da parte di società domiciliate nel loro territorio e/o sottoposte alla loro giurisdizione (sia che sia costituite in base al loro diritto interno, sia che abbiano la loro sede legale, l'amministrazione centrale o il luogo principale di attività sul territorio nazionale), senza violare la sovranità o diminuire gli obblighi degli Stati ospitanti ai sensi del Patto<sup>26</sup>.

Nonostante questo crescente riconoscimento delle *responsabilità* degli Stati, resta il punto fondamentale di come garantire delle vie di rimedio effettive alle vittime che abbiano visto la propria autonomia personale e la propria capacità di autodeterminarsi essere 'comprese' da parte di regimi autocratici che usano le tecnologie digitali non solo contro i propri cittadini o le persone presenti sul proprio territorio, ma anche contro i presunti nemici dello Stato all'estero. Le vie di rimedio, in effetti, sono pur sempre ancorate all'ordinamento nazionale dello Stato in questione e, anche a causa della reticenza con cui normalmente i vari colossi del settore tecnologico affrontano le questioni di trasparenza ed il confronto con le autorità di regolamentazione di ordinamenti terzi, per le vittime di violazioni dei diritti umani causate dalle forme di repressione basata sull'utilizzo di tecnologie digitali, ottenere un ristoro resta molto spesso una chimera.

### 3.3. L'incidenza sul valore della dignità umana

Passiamo al terzo valore 'toccato' dal *machine learning* e dalle altre tecnologie digitali, il principio di *dignità umana*, principio considerato, come è noto, la *pietra angolare* della tutela internazionale dei diritti umani. Nella misura in cui l'impiego delle tecnologie digitali diventa un mezzo per *strumentalizzare* l'essere umano, esso rappresenta un'intrusione nel principio di dignità umana, intesa come l'uguale valore morale che deve essere riconosciuto ad *ogni* essere umano. Mi riferisco alla capacità, tipi-

camente inerente a siffatte tecnologie, di rimuovere, in misura più o meno maggiore, un certo grado di potestà decisionale dall'operatore umano, per attività che erano state fino ad oggi interamente realizzate e *controllate* dall'uomo, e a trasferirle a processi autonomizzati che sono in grado di funzionare senza un costante controllo umano<sup>27</sup>. Questo può rendere ridondanti – se non addirittura irrilevanti – le capacità cognitive e quelle di giudizio intrinsecamente connaturate all'uomo, come apprendere, parlare, valutare, ecc. La prassi ha già messo in luce i pericoli che dal punto di vista della protezione dei diritti umani sono collegati al venire meno delle competenze professionali dei lavoratori in specifici settori caratterizzati da alta automattizzazione (con l'enorme numero di disoccupati che questo processo potrà creare), oppure dall'utilizzo di piattaforme di lavoro digitali basate su algoritmi in grado di riprodurre pregiudizi sociali (con rischio di discriminazioni e *bias*.)<sup>28</sup>, o, infine, nell'esercizio di funzioni governative come l'amministrazione della giustizia<sup>29</sup>. Il rischio insomma è che tale processo di strumentalizzazione possa alterare il significato normalmente attribuito alla parola 'umanità' e la stessa valutazione circa il livello di tutela da attribuire alle dimensioni della dignità umana, 'intaccando' il mantra dell'*inviolabilità* di tale principio.

Insomma, ciò che si rende necessario è un approccio cauto al processo di sviluppo e utilizzo delle tecnologie digitali. Sebbene, esse siano in grado di sopravanzare l'effettiva capacità del diritto e delle autorità di regolamentazione di prevedere e anticipare i rischi per i diritti umani (piuttosto costringendo il diritto ad inseguire secondo una logica *reattiva* alla regolamentazione in tali materie), è opportuno, invece, che Stati e legislatori cerchino in via *preventiva* di esercitare le funzioni regolamentari ad essi spettanti mediante la previsione delle esternalità negative, come l'impatto sui diritti umani, che possono scaturire dal *machine learning*, dall'intelligenza artificiale e dalle altre tec-

nologie digitali che si intende disciplinare. Occorre, in altre parole, uno *human rights-based approach* che sia applicato attraverso il diritto in tutte le fasi di sviluppo e utilizzo delle tecnologie. La notizia positiva è che sul punto si sta consolidando, a mio giudizio, un consenso piuttosto diffuso come tra l'altro dimostrato da diversi documenti internazionali ed in modo particolare, con riferimento al contesto europeo, da quelli adottati in ambito di Unione europea<sup>30</sup> e di Consiglio d'Europa<sup>31</sup>.

#### 4. Responsabilità e diritti umani nella società degli algoritmi

La terza chiave di lettura, infine, attiene come anticipato poco più sopra all'allargamento dell'istituto della *responsabilità* nel diritto internazionale. Ci riferiamo in modo particolare all'emersione di nuove *forme di responsabilità* dei diversi attori che operano nella contemporanea società degli algoritmi. Si tratta di un tema su cui abbiamo altre volte avuto occasione di soffermarci e che non è possibile per motivi di spazio affrontare in modo approfondito in questa sede<sup>32</sup>. Basti qui solo sottolineare che l'avvento dei sistemi di *machine learning*, basati sulla tecnologia degli algoritmi e sull'intelligenza artificiale, può contribuire a modificare, e anzi sta già modificando, il modo con cui il diritto si forma, opera e viene applicato. Ciò vale, a nostro avviso, anche in relazione alla nozione di responsabilità applicata nel diritto internazionale, nel senso che, come suggerito dal processo di cristallizzazione di un sistema giuridico internazionale in materia di imprese e diritti umani, il riallineamento degli squilibri di *governance* (i c.d. *governance gaps*) che sempre più caratterizzano il sistema delle relazioni internazionali, non può più passare esclusivamente attraverso l'istituto della responsabilità internazionale dello Stato, ma deve altresì prendere necessariamente in considerazione anche le responsabilità 'complementari' e 'condivise'<sup>33</sup> degli altri attori che partecipano a

tali processi e contribuiscono a condizionare la protezione dei diritti umani, oppure a violarli apertamente. A nostro giudizio, insomma, accanto al regime sulla responsabilità internazionale dello Stato, che deve effettuare le sue scelte di *policy* in materia di tecnologie digitali senza rinunciare ad assicurare la protezione dei diritti umani degli individui sottoposti alla propria giurisdizione (con gli obblighi, collegati a tale responsabilità, di prevenzione, di informazione e di trasparenza), e accanto alla responsabilità dell'individuo applicata nell'ambito del diritto penale internazionale in relazione alle *gross violations* dei diritti umani, ... *tertium datur!* È in via di consolidamento un regime internazionale sulla *responsabilità delle imprese* in materia di diritti umani<sup>34</sup> che opera, accanto ai primi due regimi di responsabilità internazionale, e che impone alle imprese, con riferimento specifico alla salvaguardia di tali valori avvertiti come fondamentali per la comunità internazionale, di rispettarli e di adottare a tal fine processi di *due diligence* in materia di diritti umani per individuare, prevenire e mitigare i rischi di un impatto negativo sui diritti umani derivante dalle loro attività. Tale responsabilità delle imprese di rispettare i diritti umani si applica a tutti gli enti del settore privato e, per quanto attiene il tema del presente lavoro, si estende ovviamente anche alle imprese del settore tecnologico le cui operazioni economiche sono dedite allo sviluppo o all'utilizzo delle tecnologie digitali.

## 5. Conclusioni

L'utilizzo di tecnologie digitali, come l'impiego di algoritmi predittivi, l'intelligenza artificiale, il *machine learning*, le tecniche di riconoscimento facciale, è in costante aumento. La narrativa normalmente associata a questo fenomeno tende a mettere in luce il potenziale di queste tecnologie per la crescita economica, lo sviluppo, il benessere delle comunità di persone, ma non

sempre viene riposta sufficiente enfasi sul potenziale impatto negativo sulla società e sui principi che governano la società come la *rule of law* ed i diritti umani. Solo più recentemente, a causa delle pressioni provenienti da cittadini, dalla società civile e da altri gruppi vulnerabili, istituzioni di governo e Organizzazioni internazionali hanno iniziato a prendere in considerazione le sfide che tali tecnologie pongono per la tutela dei diritti umani. Ciò ha comportato uno spostamento dell'attenzione sulla questione volta a stabilire se e come regolamentarne l'utilizzo, e soprattutto quali attori debbano assumersi relativi doveri e responsabilità. A tal fine un crescente consenso si sta consolidando intorno alla necessità che il quadro normativo di riferimento per le tecnologie digitali richieda uno *human rights-based approach* e debba essere costruito intorno a due principi: quello della *centralità dell'uomo* e quello di *responsabilità*<sup>35</sup>. Per quanto riguarda il primo principio, la centralità dell'uomo rinvia alla necessità che sia assicurato un *controllo* effettivo sulle potenziali violazioni dei diritti umani derivanti dalle tecnologie digitali, il che implica che il loro utilizzo non deve violare i diritti fondamentali garantiti dalle Costituzioni e dagli standard internazionali. La centralità dell'uomo implica, insomma, che tali tecnologie debbano rimanere sotto il controllo umano, anche nelle circostanze in cui la digitalizzazione della tecnologia consenta di adottare decisioni indipendentemente da uno specifico intervento umano. Il criterio del controllo umano, si traduce pertanto, con riguardo alle imprese che sviluppano le tecnologie digitali oppure che ne fanno uso per i propri scopi commerciali, nella necessità di un approccio proattivo ai potenziali impatti negativi derivanti dall'utilizzo di questa tecnologia volto a prevenire le violazioni che possano scaturirne per la garanzia dei diritti umani. Tale approccio preventivo è perfettamente coerente con l'applicazione di processi di *due diligence* aziendale in materia di diritti umani.

Per quanto riguarda il secondo principio – quello di responsabilità – occorre garantire l'esistenza di sistemi di *accountability* efficaci per monitorare e, ove necessario, affrontare efficacemente qualsiasi impatto negativo sui diritti umani derivanti dalle tecnologie digitali. Ciò porta a considerare come oggigiorno le violazioni dei diritti umani si verificano sempre più frequentemente in un quadro caratterizzato da azioni *congiunte* e *coordinate*, piuttosto che indipendenti, da parte di diversi soggetti – pubblici e privati – che, attraverso i loro comportamenti, contribuiscono in vario modo ad assicurare, o meno, la tutela dei diritti umani. È esattamente in questa prospettiva di analisi che l'avvento della società dell'intelligenza artificiale non ha fatto altro che accelerare ulteriormente un processo già in atto e che sta originando “un cambiamento paradigmatico in cui il potere pubblico non è più l'unica fonte di preoccupazione per il rispetto dei diritti fondamentali e la tutela della democrazia”<sup>36</sup>.

Note di chiusura

<sup>1</sup> Il presente lavoro è pubblicato grazie al supporto del progetto SERICS (SEcurity and RIghts in the CyberSpace - PE00000014) realizzato nell'ambito del Piano Nazionale di Ripresa e resilienza del MUR, finanziato dal programma NextGenerationEU dell'UE.

<sup>2</sup> Basti pensare alla letteratura addensatasi negli anni '70 del secolo trascorso intorno ad uno dei primi studi circa i rapporti tra sviluppo scientifico-tecnologico e strutture economico-sociali, il c.d. Rapporto Richta dal nome del suo autore (cfr. R. RICHTA, *Civiltà al bivio: le conseguenze umane e sociali della rivoluzione scientifica e tecnologica*, Milano, 1972). Nella prospettiva dei diritti fondamentali ci limitiamo a segnalare, in una letteratura praticamente sconfinata, M. CARTABIA, *In tema di "nuovi" diritti*, in *Scritti in onore di F. Modugno*, Napoli, 2011, I, 643; S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet*, Hart Publishing, Oxford, 2021.

<sup>3</sup> Cfr. T. Van Ho, *COVID-19 Symposium: A Time to Kill 'Business as Usual' - Centring Human Rights in a Frustrated Economy (Part 1)*, in *Opinio Juris*, 2 aprile 2020.

<sup>4</sup> Cfr. O. POLLICINO, *Costituzionalismo, privacy e neurodiritti*, in *Medialaws*, 2021, pp. 9-16, in part. p. 11.

<sup>5</sup> Cfr. Consiglio dei diritti umani, *Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN Doc. A/HRC/17/31 del 21 marzo 2011.

<sup>6</sup> Non è possibile una analisi puntuale del contenuto dei Principi Guida. Ci limitiamo a rinviare a R. MARES (ed.), *The UN Guiding principles on business and human rights: foundations and implementations*, Leiden, 2012; F. MARRELLA, *I Principi Guida dell'ONU sulle imprese e i diritti umani del 2011 e l'accesso ai rimedi tramite gli strumenti di diritto internazionale privato europeo: una valutazione critica*, in (a cura di) M. CASTELLANETA, F. VESSIA, *La responsabilità sociale d'impresa tra diritto societario e diritto internazionale*, Napoli, 2019, pp. 315-337. Sia consentito anche il rinvio a M. FASCIGLIONE, *I Principi guida ONU su impresa e diritti umani e il consolidamento del regime internazionale in materia di settant'anni dalla Dichiarazione universale*, in (a cura di) G. CATALDI, *I diritti umani a settant'anni dalla Dichiarazione universale delle Nazioni Unite*, Napoli, 2019, pp. 93-128; ID., *Per uno studio dei Principi Guida ONU su imprese e diritti umani*, in (a cura di) M. FASCIGLIONE, *I Principi Guida su Imprese e Diritti Umani*, Roma, 2020, pp. 35-58.

<sup>7</sup> Cfr. i Principi 13 e 17.

<sup>8</sup> Cfr. Principio 15.

<sup>9</sup> Cfr. Alto commissariato sui diritti umani, *The Corporate Responsibility to Respect Human Rights: An Interpretative Guide*, Ginevra, 2012, p. 4.

<sup>10</sup> In Europa, la *privacy by design* e la *privacy by default* sono elementi fondamentali del regime giuridico di protezione dei dati dall'art. 25 del GDPR (Regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE). In base a tale disposizione, i responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate e le garanzie necessarie, volte ad attuare i principi di protezione dei dati in modo efficace e a tutelare i diritti e le libertà degli interessati (cfr. anche *European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adottato il 13 novembre 2019, par. 12 e seguenti). In materia v. A.E. WALDMAN, *Data Protection by Design? A Critique of Article 25 of the GDPR*, in *Cornell International Law Journal*, 2020, Vol. 53, No. 1, p. 147-167.

<sup>11</sup> Cfr. 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, COM(2021) 206 final, del 21 aprile 2021.

<sup>12</sup> Abbiamo avuto modo di analizzare maggiormente in dettaglio tale aspetto in M. FASCIGLIONE, *Business and Human Rights in the Age of Artificial Intelligence*, in *Federalismi.it*, 2/2022, pp. 164-183, p. 177 ss.

<sup>13</sup> Cfr. Commissione europea, *Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937*, COM(2022)71 final, del 23 febbraio 2022.

<sup>14</sup> Cfr. <https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked>.

<sup>15</sup> Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Roma, 1950. In materia v. M. STARITA, *Art. 3*, in (a cura di) S. BARTOLE, P. DE SENA, V. ZAGREBELSKI, *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, pp. 832-857.

<sup>16</sup> Ruolo pionieristico è stato svolto da Google quando, nel 2010, essa ha pubblicato il suo *Transparency Report*, in cui ha reso note le sue restrizioni circa i contenuti e le misure relative alla sicurezza e alla privacy (cfr. <https://transparencyreport.google.com/about>).

## I diritti umani nell'era degli algoritmi e dell'intelligenza artificiale

<sup>17</sup> Cfr. High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 2019, consultabile al sito <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

<sup>18</sup> R. SPANO, *The rule of law as the lodestar of the European Convention on Human Rights: The Strasbourg Court and the independence of the judiciary*, in *European Law Journal*, 2021.

<sup>19</sup> Cfr. S. FELDSTEIN, *How Artificial Intelligence Is Reshaping Repression*, in *Journal of Democracy*, 2019, Volume 30, n. 1, pp. 40-52.

<sup>20</sup> Cfr. O. POLLICINO, *Costituzionalismo, privacy e neurodiritti*, cit., p. 10.

<sup>21</sup> Come noto la tripartizione degli obblighi scaturenti dalle norme sui diritti umani in obblighi di rispettare, proteggere e realizzare, è stata proposta in dottrina da H. SHUE, *Basic Rights: Subsistence, Affluence, and US Foreign Policy*, Princeton, 1980, p. 52, ripresa da A. EIDE, *The International Human Rights System*, in (Eds) A. Eide et al, *Food as a Human Rights*, Tokyo, 1984, p. 152 ss, e materialmente recepita dal Comitato sui diritti economici, sociali e culturali nella sua, oramai consolidata, prassi.

<sup>22</sup> Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, UN Doc. E/C.12/GC/24, del 10 agosto 2017.

<sup>23</sup> Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 12.

<sup>24</sup> Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 14.

<sup>25</sup> Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 23.

<sup>26</sup> Comitato sui diritti economici, sociali e culturali, *General comment No. 24 (2017)*, cit. par. 26.

<sup>27</sup> Per una analisi in materia sia pure in una prospettiva differente v. P. DE SENA, *Dignità umana in senso oggettivo e diritto internazionale*, in *Dir. um. e dir. int.*, 2017, pp. 573-586, che si sofferma sul ruolo della dignità umana in senso oggettivo come *ratio* dell'indisponibilità del corpo umano, a fini commerciali, in ambito europeo.

<sup>28</sup> Si consideri ad esempio il caso dell'algoritmo utilizzato dalla società *Deliveroo Italia* per gestire il sistema di prenotazione digitale delle sessioni di lavoro dei *rider* impiegati dall'azienda. L'algoritmo, infatti, che doveva stabilire

la priorità in base alla quale ai *rider* venivano assegnati i turni di lavoro, era stato concepito in modo da penalizzare i lavoratori che si assentavano ingiustificatamente dalle sessioni di lavoro assegnate, ma non effettuava alcuna differenziazione per le situazioni di astensione legittima, come l'esercizio del diritto di sciopero! Il caso ha originato quindi una vicenda giudiziaria con il Tribunale di Bologna che ha condannato la società per condotta discriminatoria in relazione al funzionamento dell'algoritmo nella piattaforma digitale (cfr. Trib. di Bologna, *Filcams Cgil Bologna, Nidil Cgil Bologna, Filt Cgil Bologna c. Deliveroo Italia S.r.l.*, ord. 31 dicembre 2020).

<sup>29</sup> In materia, con riferimento all'indipendenza dei giudici cfr. G.M. RUOTOLO, *The End of Dormancy. Judicial Independence through Data-Driven Knowledge, Open Data and Artificial Intelligence from an International and European Law Perspective*, in (eds.) S. SHETREET, H. CHODOSH, E. HELLAND, *Challenged Justice. In pursuit of Judicial Independence*, Leiden/Boston, 2021, p. 59 ss.

<sup>30</sup> Sul punto, si veda, *inter alia*: Consiglio europeo, *Presidency conclusions. The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, del 21 ottobre 2020, par. 10 e ss., che enfatizza la necessità di “[a] fundamental rights-based approach to AI”; Commissione europea, *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, del 19 febbraio 2020, p. 2, secondo cui “qualsiasi quadro regolamentare per l'IA deve essere fondato sui valori fondamentali dell'Unione” incluso il rispetto per i diritti umani. Il tema è poi ampiamente trattato negli studi compiuti dall'Agenzia per i diritti fondamentali dell'Unione europea (v. FRA, *Getting the future right – Artificial intelligence and fundamental rights*, del 14 dicembre 2020; FRA, *Fundamental Rights Report 2022*, 8 giugno 2022p. 17 e ss.).

<sup>31</sup> Il tema di uno *human rights-based approach* allo sviluppo e utilizzo delle tecnologie digitali è presente in tutti i documenti prodotti dall'*Ad hoc Committee on Artificial Intelligence* del Consiglio d'Europa e che sono consultabili al sito web [www.coe.int/en/web/artificial-intelligence/cahai](http://www.coe.int/en/web/artificial-intelligence/cahai).

<sup>32</sup> V. ad es, M. FASCIGLIONE, *L'emergenza COVID-19 e l'attuazione della responsabilità delle imprese di rispettare i diritti umani nel diritto internazionale*, in *Quaderni di SIDIBlog*, 2020 (2021), pp. 25-45.

<sup>33</sup> Le implicazioni teoriche e pratiche delle *shared responsibilities* di imprese e di Stati nel diritto internazionale sono analizzate da: A. NOLLKAEMPER, D. JACOBS, *Shared Responsibility in International Law: A Conceptual Framework*, in *Michigan Journal of International Law*, 2013, p. 359 ss.; M. KARAVIAS, *Shared Responsibility and Multinational Enterprises*, in *Netherlands International Law Review*, 2015, p. 91 ss.

<sup>34</sup> I segnali del consolidamento di un siffatto regime sono, a nostro giudizio, molteplici. Non si tratta solo dell'affermazione di standard internazionali non vincolanti in materia di imprese e diritti umani, come ad es. i menzionati Principi guida onusiani del 2011, e gli altri standard internazionali esistenti in materia, ma anche del processo di emersione di regimi normativi che, tanto a livello di ordinamenti nazionali degli Stati, quanto a livello di ordinamenti regionali (come quello europeo), sono volti a fissare obblighi di *due diligence* in materia di diritti umani per le imprese.

<sup>35</sup> Entrambi i principi sono stati più volte evocati dalle istituzioni internazionali e da altri organismi di regolamentazione. Si veda, tra gli altri, FRA, *Getting the future right*, cit., pp. 8-10.

<sup>36</sup> O. POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, in *MediaLaws*, 11 novembre 2020.

## **Indice degli autori**

### **ENRICO AL MUREDEN**

Professore ordinario di diritto privato presso l'Università di Bologna

**ANTONINA ASTONE** Professoressa associata di diritto privato presso l'Università degli Studi di Messina

### **ETTORE BATTELLI**

Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

### **GIOVANNI BERTI DE MARINIS**

Professore associato di diritto dell'economia presso l'Università degli Studi di Perugia

### **MARCO CARLIZZI**

Avvocato del Foro di Roma, dottore di ricerca in diritto commerciale – Università di Roma “Tor Vergata”

### **ENRICO CATERINI**

Professore ordinario di diritto privato presso l'Università della Calabria

**ANTONELLA CORRENTI** Assegnista di diritto privato comparato presso l'Università degli Studi di Messina

### **MARCO FASCIGLIONE**

Ricercatore di Diritto internazionale e di Tutela dei diritti umani, CNR-IRISS

**ILARIA GARACI**

Professoressa associata di diritto privato presso l'Università Europea di Roma

**SARA LANDINI**

Professoressa ordinaria di diritto dell'economia presso l'Università degli Studi di Firenze

**FRANCESCO MEZZANOTTE**

Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

**ROBERTA MONTINARO**

Professoressa ordinaria di diritto privato presso l'Università di Napoli L'Orientale

**ROSARIO PETRUSO**

Professore associato di diritto privato comparato presso l'Università degli Studi di Palermo

**GUIDO SMORTO**

Professore ordinario di diritto privato comparato presso l'Università degli Studi di Palermo



IL TORCOLIERE • Officine Grafico-Editoriali d'Ateneo  
Università di Napoli L'Orientale  
stampato nel mese di giugno 2023



**UNIVERSITÀ DI NAPOLI  
L'ORIENTALE**

Dipartimento di Scienze Umane e Sociali

Il libro esamina le questioni giuridiche più rilevanti legate all'evoluzione delle tecnologie digitali e, in particolare, allo sviluppo di sistemi intelligenti, al loro impatto sui diritti umani e alla imputazione delle responsabilità.

Gli autori esplorano le soluzioni in grado di promuovere e garantire la sostenibilità dell'innovazione, attraverso azioni preventive e la protezione *by design*. Del resto, le tecnologie digitali contribuiscono a migliorare la valutazione dei rischi, a promuovere la trasparenza e l'efficienza dei servizi digitali, nel rispetto degli obiettivi dello sviluppo sostenibile. Specifica attenzione è rivolta ai settori assicurativo, bancario e turistico.

ILARIA GARACI - Professore associato di Diritto privato nell'Università Europea di Roma, dove insegna Diritto privato ed Elements of Italian Private Law. È membro del Collegio dei docenti nel Corso di Dottorato in "Persona, benessere e innovazione", presso l'Università Europea di Roma. Relatrice in seminari e conferenze nazionali e internazionali, è autrice di due lavori monografici e di diversi contributi in materia di beni immateriali e tutela della persona, tutela del consumatore, responsabilità civile, rimedi restitutori, diritti dei minori di età.

ROBERTA MONTINARO - Professore ordinario di Diritto Privato, insegna Diritto privato e Diritto privato dell'economia digitale presso il Dipartimento di Scienze Umanistiche e Sociali dell'Università di Napoli L'Orientale. È coordinatore scientifico del Modulo Jean Monnet "DiCIT - Digital Citizenship in the European Union" e membro del collegio dei docenti del Dottorato Nazionale in Intelligenza Artificiale. È stata relatrice e coordinatrice scientifica di seminari e conferenze nazionali e internazionali. Autrice di monografie, ha pubblicato anche articoli e saggi in libri e riviste scientifiche, in italiano e in inglese. I suoi principali interessi di ricerca riguardano il diritto dei trust, la responsabilità civile, il diritto dei consumatori e il diritto delle tecnologie digitali.

ISBN 978-88-6719-276-2