CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

BREVI RIFLESSIONI IN MERITO AL POSSIBILE IMPATTO DELL´INTELLIGENZA ARTIFICIALE SUI DIRITTI UMANI

Il con tributo fornisce una breve analisi del possibile impatto che l´Intelligenza artificiale può avere sui diritti e le libertà fondamentali della persona.

di **Riccardo Samperi**
IUS/08 - DIRITTO COSTITUZIONALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Giovedì 29 Luglio 2021

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The Paper provides a brief analysis of the possible impact that Artificial Intelligence may have on Human Rights and Fundamental Freedoms of the Person.

Sommario: 1. Definizione di Artificial Intelligence; 2. «Machine learning», «deep learning» e «speech recognition»; 3. I nuovi rischi determinati dall'AI; 4. Il possibile impatto dell'AI sui diritti umani: in particolare, sul diritto ad un giusto processo e sulla libertà personale; 5. Il diritto alla privacy e la protezione dei dati personali; 6. La libertà di circolazione; 7. Le libertà di espressione, pensiero, religione, riunione e associazione; 8. La libertà di autodeterminazione nelle scelte politiche e il divieto di propaganda; 9. Considerazioni conclusive: possibili strategie per conciliare lo sviluppo tecnologico e la salvaguardia dei diritti umani.

1. Definizione di Artificial Intelligence

L'intelligenza artificiale sta attraversando una fase di considerevole sviluppo, che si accompagna ad una sempre maggiore capacità di "affect", cioè di incidere, sui diritti fondamentali della persona, di gran lunga superiore a quella che avevano (e che hanno ancora) le altre e diverse forme di tecnologia.

Trattandosi di un fenomeno nuovo e in fase di forte sviluppo, non è stata ancora elaborata una disciplina organica della materia, né è stata inaugurata alcuna prassi giurisprudenziale. Data la scarsità delle fonti, assumono rilevanza fondamentale gli atti di indirizzo forniti da enti sovrannazionali (Nazioni Unite e Unione Europea in primis)[1].

Ad oggi, manca una definizione "ufficiale" del concetto di intelligenza artificiale.

Marvin Minsky, esperto di AI e cofondatore dell'Artificial Intelligence Project presso il Massachusetts Institute of Technology di Cambridge, ha definito l'IA come «the science of making machines do things that would require intelligence if done by men»[2].

John McCarthy, esperto informatico, ha definito l'IA come «the science and engineering of making intelligent machines»[3].

Un recente studio dell'università di Stanford ha proposto un interessante accostamento tra intelligenza artificiale e umana: la prima sarebbe un insieme di «computational

CamminoDiritto.it
ISSN 2421-7123

technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action»[4].

Si tratta di una visione decisamente innovativa, che pone l'accento, per la prima volta, sulle affinità esistenti tra l'intelligenza artificiale e quella umana.

2. «Machine learning», «deep learning» e «speech recognition»

Gli strumenti tecnologici dotati di AI «apprendono» (learn) attraverso una serie di procedure alle quali generalmente ci si riferisce mediante l'espressione «machine learning»[5].

L'apprendimento avviene mediante l'uso incrociato di algoritmi matematici e grandi quantità di dati (Big Data); con il passare del tempo, il sistema informatico raccoglie dati e, grazie a questi, perfeziona il procedimento computazionale[6].

I devices tecnologici, infatti, sono programmati per svolgere funzioni computazionali ben precise: partendo da un assunto di base (Input Data) effettuano una serie di operazioni matematiche attraverso algoritmi più o meno complessi e, alla fine, emettono un output, ossia un prodotto finale[7].

È evidente, dunque, che tanto maggiore è la quantità di dati a disposizione della «macchina» (qui intesa nel senso di dispositivo elettronico, dall'inglese «machine»), tanto migliore e perfezionato risulterà l'apprendimento finale. Buona parte dell'attività di machine learning ruota, dunque, attorno ad una raccolta ed analisi statistica di dati, generalmente messi a disposizione dagli stessi utenti, in cambio di un certo servizio[8].

Una particolare tecnica di machine learning è costituita dal c.d. «deep learning», che costituisce, finora, la forma di apprendimento artificiale più vicina a quello umano.

Il deep learning si basa su una rete di infrastrutture modellate sul sistema neuronale umano (si parla al riguardo di «neural networks»)[9] e permette al computer di mettere in correlazione tra loro dati diversi. Un esempio chiarirà sicuramente meglio il concetto.

Nella figura n. 1, al computer è stato affidato un compito apparentemente semplice, se non addirittura banale: quello di «imparare» che cosa sia un elefante. Partendo dunque da un dato iniziale di input (la fotografia dell'animale), il software svolge una serie di calcoli algoritmici fino a quando non trova la parola «elefante» (output), che viene

CamminoDiritto.it
ISSN 2421-7123

immagazzinata nella memoria. Potremmo, quindi, affermare il computer è riuscito ad «apprendere» una nozione.

Questo meccanismo apparentemente banale è stato utilizzato per creare software molto sofisticati: automobili che riescono ad inserirsi all'interno di un parcheggio senza ricevere comandi «umani», programmi di identificazione facciale (impiegati, ad esempio, da alcuni Paesi per catturare pericolosi terroristi) e, addirittura, attrezzature mediche che riescono a diagnosticare autonomamente alcuni tipi di patologie[10].

Un particolare tipo di apprendimento è costituito dallo «speech recognition», realizzato mediante software che riescono a registrare e «comprendere» le parole e le frasi pronunciate da un determinato soggetto, per identificarlo (nell'ipotesi in cui il timbro della sua voce risulti già registrata all'interno del database) o per trasformarle in un testo scritto. Il carattere di innovatività dello speech recognition risiede nel fatto che l'input non deve necessariamente essere preregistrato o predeterminato (come, invece, nelle ipotesi anzidette), ma, al contrario, il più delle volte il testo viene trascritto nel momento stesso in cui viene pronunciato, dunque potremmo affermare che il computer «apprende in tempo reale»[11].

3. I nuovi rischi determinati dall'AI

L'intelligenza artificiale utilizza algoritmi che, attraverso calcoli statistici, arrivano ad un risultato. Questo tipo di tecnologia oggi è coinvolto in procedimenti volti ad adottare una «decisione finale»; si parla al riguardo di «algorithmic decision-making»[12].

Gli algoritmi esistenti prima dell'affermazione dell'AI erano di tipo deterministico, cioè «pre-programmati». Si basavano su un numero predeterminato di equazioni, che tenevano conto di un numero prestabilito di variabili. In tal modo, era possibile prevedere, con precisione matematica, che ad un determinato input corrispondesse un altrettanto determinato output (2 + 2 = 4).

L'intelligenza artificiale, invece, utilizza un numero di variabili, dati, equazioni, algoritmi non definito ab origine e, soprattutto, «ever-changing», cioè che muta e si sviluppa continuamente. Per tale ragione, è assolutamente impossibile prevedere con esattezza come la macchina reagirà a un certo input.

Sebbene il margine di errore dei sistemi di machine learning sia prossimo allo zero, l'output da essi prodotto non sempre risulta migliore rispetto a quello degli esseri umani.

CamminoDiritto.it
ISSN 2421-7123

Nel 2015, il software di riconoscimento facciale di Google (Google Photos) ha commesso un errore a dir poco imbarazzante: in alcuni casi, le persone di colore venivano identificate in fotografie raffiguranti scimmie. I tecnici di Google non hanno compreso come ciò sia stato possibile, fatto sta che è stato necessario l'intervento umano per correggere questo terribile bug[13].

Un altro caso in cui l'intelligenza artificiale si è rivelata «harmful», cioè latu sensu dannosa, è quello delle fake news a scopi elettorali. Nel 2016, in occasione delle elezioni americane che hanno visto la vittoria del miliardario Donald Trump, del Referendum sulla Brexit e del Referendum italiano sulla riforma costituzionale, sono state rintracciate centinaia di account falsi sui social network (prevalentemente Facebook e Twitter), che condividevano fake news per avvantaggiare una fazione politica in danno dell'altra[14].

Ciò che ha suscitato l'attenzione degli esperti informatici è stata la modalità attraverso cui venivano effettuate le condivisioni: quasi ventiquattro ore al giorno, sempre. È quindi emerso che, dietro questi account, non vi erano persone fisiche, ma computer. Erano gestiti da software programmati per la condivisione di post, Twitts, immagini e notizie, realizzati da società e individui che ricevevano compensi (con tutta probabilità) di illecita provenienza[15].

Sotto questo specifico profilo, bisogna comunque dare conto dell'esistenza di varie iniziative dirette a impiegare l'AI al contrasto delle fake news. In base ai modelli statistici e algoritmici di cui abbiamo parlato, verranno messi a punto software in grado di individuare notizie false e/o fonti non attendibili[16].

Come è stato efficacemente affermato, «da un lato, algoritmi e reti neuronali permettono di scoprire e bloccare la propagazione di notizie false, dall'altro vengono utilizzati per diffonderle»[17].

4. Il possibile impatto dell'AI sui diritti umani: in particolare, sul diritto ad un giusto processo e sulla libertà personale

La libertà personale è un bene giuridico fondamentale, riconosciuto e tutelato dalle Costituzioni dei paesi democratici e da varie fonti internazionali.

L'articolo 9, comma 1, del Patto internazionale dei diritti civili e politici stabilisce, infatti, che «ogni individuo ha diritto alla libertà e alla sicurezza della propria persona. Nessuno può essere arbitrariamente arrestato o detenuto. Nessuno può essere privato della propria libertà, se non per i motivi e secondo la procedura previsti dalla legge».

CamminoDiritto.it
ISSN 2421-7123

Altro principio di carattere generale, relativo alla salvaguardia delle libertà fondamentali della persona, che potrebbe essere messo in pericolo dall'AI è quello dell'uguaglianza dei cittadini davanti alla legge e alle autorità giurisdizionali. Tale principio è codificato dall'articolo 14 del summenzionato Patto, che recita: «Tutti sono eguali dinanzi ai tribunali e alle corti di giustizia. Ogni individuo ha diritto ad un'equa e pubblica udienza dinanzi a un tribunale competente, indipendente e imparziale, stabilito dalla legge, allorché si tratta di determinare la fondatezza dell'accusa penale che gli venga rivolta, ovvero di accertare i suoi diritti ed obblighi mediante un giudizio civile».

Quanto al principio della tendenziale parità delle armi tra accusa e difesa, la Professoressa Quattrocolo ha messo in luce che: «La straordinaria potenza computazionale – a costi ridottissimi – e la proliferazione incontrollata di dati attraverso tecnologie digitali di uso quotidiano generano un substrato conoscitivo ricchissimo ed utilissimo anche per il processo penale. Tuttavia, l'opacità degli algoritmi che regolano la creazione e la raccolta di questi dati rischia di rendere impossibile in nuce la difesa dell'imputato, che si trova per lo più nell'impossibilità di accedere, comprendere e validare il processo che ha portato alla produzione del dato. In questo contesto, l'attendibilità della prova generata automaticamente rischia di divenire incontestabile, in violazione della più essenziale concezione di parità delle armi, sancita dalla Convenzione europea dei Diritti dell'Uomo» [18].

Nel 2018, su impulso di Amnesty International e Access Now, è stata adottata la Toronto Declaration, un documento che codifica buone pratiche relative all'utilizzo e all'implementazione dell'intelligenza artificiale, finalizzata ad assicurare il rispetto dei diritti fondamentali della persona[19].

Negli Stati Uniti, stanno trovando sempre maggiore applicazione ed utilizzo i c.d. «recidivism risk-scoring softwares», ossia programmi che, partendo da determinati dati input di base, applicano calcoli algoritmici per calcolare il rischio di recidiva relativo al singolo detenuto e «suggeriscono» la pena (o la cauzione) ritenuta più idonea.

È emerso che questi software finiscono con il giudicare in maniera più severa gli imputati di colore, irrogando loro sanzioni superiori rispetto a quelle dei deputati di altre etnie. Tale meccanismo ha determinato una violazione di svariati diritti umani, tutelati a livello internazionale, fra cui il diritto ad un equo processo, in condizioni di uguaglianza davanti alla legge[20].

E dunque, malgrado l'impiego di tali software – oggi – costituisca un mero ausilio per il giudice, i risultati (spesso falsati) relativi al rischio di recidiva potrebbero subdolamente

CamminoDiritto.it
ISSN 2421-7123

ingenerare nel giudice una sorta di pregiudizio, anche inconscio, nei confronti dell'imputato, con la conseguente violazione del principio di presunzione di innocenza fino al passaggio in giudicato della sentenza di condanna[21].

I software di identificazione facciale si sono rivelati spesso inattendibili, soprattutto per le «non white faces», e ciò si è tradotto in arresti e incarcerazioni sostanzialmente arbitrarie e prive di fondamento[22].

5. Il diritto alla privacy e la protezione dei dati personali

La salvaguardia della vita privata degli individui costituisce un preciso obbligo per gli Stati, i quali, in virtù del diritto internazionale, sono obbligati a tutelare il diritto di ogni cittadino «nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione» (art. 17 del Patto internazionale per i diritti civili e politici).

Analoga tutela è apprestata dalla CEDU, che, all'articolo 8, sancisce che «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

Infine, l'articolo 8 della Carta dei diritti fondamentali dell'UE attribuisce ad ogni cittadino il diritto alla protezione dei dati di carattere personale che lo riguardano.

I sistemi di AI si basano sull'utilizzo di enormi quantità di dati (c.d. Big Data). Tale è divenuta l'importanza delle informazioni personali, che la dottrina ha qualificato il dato personale quale nuovo bene giuridico e la cessione di dati personali in cambio di servizi informatici come modello contrattuale atipico[23].

Il ricorso ai Big Data ha permesso ai software di intelligenza artificiale di estrapolare, dai dati di input disseminati dagli utenti lungo la rete, informazioni ulteriori ed aggiuntive, che, magari, gli utenti non avrebbero voluto rendere note. A questo riguardo, ad esempio, è stato messo a punto un software in grado di individuare, peraltro con notevole precisione, dati personali quali età, sesso, lavoro e status coniugale, partendo dalla

CamminoDiritto.it
ISSN 2421-7123

semplice posizione del telefono cellulare[24].

6. La libertà di circolazione

La libertà di circolazione delle persone è una delle quattro libertà fondamentali dell'Unione europea, assieme a quella di servizi, merci e capitali[25]. A livello internazionale, è tutelata dall'articolo 12 del Patto internazionale dei diritti civili e politici, a norma del quale «ogni individuo che si trovi legalmente nel territorio di uno Stato ha diritto alla libertà di movimento e alla libertà di scelta della residenza in quel territorio. Ogni individuo è libero di lasciare qualsiasi Paese, incluso il proprio».

Ad oggi, come ricordato nel paragrafo precedente, le tecnologie di intelligenza artificiale sono in grado di mappare con estrema precisione i movimenti degli individui, combinando software di localizzazione satellitare, riconoscimento facciale e tracciamento di smartphone, tablet e computer.

Questo tipo di tracciamento non viola la libertà di circolazione e soggiorno dei cittadini, ma – in assenza di puntuali regolamentazioni della materia – c'è il serio rischio che gli Stati, specialmente quelli «meno democratici», potrebbero servirsi di queste tecnologie per elaborare restrizioni mirate alla libertà di movimento dei cittadini[26].

7. Le libertà di espressione, pensiero, religione, riunione e associazione

Le libertà di espressione, pensiero, religione, riunione e associazione sono tutelate da numerose norme internazionali[27].

Oggi i social network, e in particolare Facebook, si servono dell'intelligenza artificiale per «controllare» che gli utenti rispettino i propri standard[28], ossia le condizioni contrattuali che gli utenti stessi accettano per usufruire del servizio di socializzazione[29].

I contenuti «non conformi» agli standard della community vengono rimossi automaticamente, sulla base alle segnalazioni provenienti dagli utenti stessi.

L'intelligenza artificiale, però, finora non ha dato buona prova di sé: spesso contenuti chiaramente lesivi della reputazione o di altri beni giuridicamente rilevanti non sono stati rimossi oppure sono stati rimossi soltanto dopo un esplicito ordine del giudice[30].

Al contrario, sono state rimosse fotografie o altri contenuti che, in realtà, non

CamminoDiritto.it
ISSN 2421-7123

contravvenivano alle regole fissate dal social[31].

O ancora, YouTube ha rimosso più di 100.000 video che documentavano le atrocità commesse durante la guerra civile siriana, spesso in danno di minori[32], anche quando essi costituivano l'unica prova documentale per fare valere in giudizio la responsabilità penale dei soldati. In pratica, la salvaguardia della sensibilità degli utenti è stata anteposta alla necessità di perseguire crimini di guerra, secondo un giudizio di bilanciamento di valori totalmente privo di umanità, oltre che di senso logico e giuridico[33].

Prendendo come modello Facebook, anche il governo cinese ha avviato un graduale processo di sostituzione dei censori umani con i robot, anche al fine di ridurre la spesa pubblica[34].

Inoltre, negli Stati in cui la libertà di religione è minacciata o, addirittura, proibita, l'intelligenza artificiale potrebbe essere utilizzata per monitorare e tenere sotto controllo i fedeli professanti culti proibiti. Di conseguenza, questi soggetti potrebbero evitare di riunirsi e associarsi, anche pacificamente, per timore di essere individuati e subire sanzioni penali[35].

8. La libertà di autodeterminazione nelle scelte politiche e il divieto di propaganda

L'articolo 25 del Patto internazionale per i diritti civili e politici attribuisce ad ogni individuo il diritto di: a) «Partecipare alla direzione degli affari pubblici, personalmente o attraverso rappresentanti liberamente scelti; b) Votare e di essere eletto, nel corso di elezioni periodiche, veritiere, effettuate a suffragio universale ed eguale, ed a voto segreto, che garantiscano la libera espressione della volontà degli elettori; c) Accedere, in condizioni generali di eguaglianza, ai pubblici impieghi del proprio Paese».

È tristemente noto il ruolo che alcune potenze straniere hanno avuto nelle elezioni presidenziali americane del 2016, riuscendo a orientare una parte dell'elettorato grazie alla diffusione di fake news sulla candidata democratica Hillary Clinton[36].

Analogo meccanismo potrebbe essere utilizzato per propagandare odio sociale, in violazione del divieto di propaganda a favore della guerra e della violenza, di cui all'articolo 20 del Patto internazionale per i diritti civili e politici, a norma del quale «qualsiasi propaganda a favore della guerra deve essere vietata dalla legge. Qualsiasi appello all'odio nazionale, razziale o religioso che costituisce incitamento alla discriminazione, all'ostilità o alla violenza deve essere vietato dalla legge».

CamminoDiritto.it
ISSN 2421-7123

9. Considerazioni conclusive: possibili strategie per conciliare lo sviluppo tecnologico e la salvaguardia dei diritti umani

L'intelligenza artificiale, per poter funzionare, ha bisogno dei Big Data. Il presupposto per evitare che questa forma di tecnologia si presti ad abusi, tanto da parte dei privati, quanto da parte degli Stati, è che vengano implementate, sia a livello nazionale che internazionale, serie riforme legislative volte ad assicurare l'effettività della tutela della privacy e dei dati personali.

Il Regolamento europeo per la protezione dei dati personali (GDPR) ha ricevuto valutazioni positive, non soltanto per l'elevato livello di tutela dei dati, ma anche perché, in considerazione del «peso» politico ed economico dell'Unione europea, de facto, sta obbligando le società di tutto il mondo ad accettare gli standard europei di tutela della privacy. Le società aventi sede legale all'estero che intendono offrire beni o servizi all'interno del territorio dell'Ue o, comunque, a cittadini europei, hanno infatti l'obbligo di applicare il GDPR, che assume, quindi, efficacia extraterritoriale e che sta influenzando le legislazioni di molti Stati[37].

La professoressa Anu Bradford della Columbia Law School ha coniato il termine «Brussels effect», per riferirsi a tale fenomeno[38], sul modello di quanto accaduto in passato negli Stati Uniti, con il c.d. «California effect»[39].

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] ACCESS NOW, Human Rights in the Age of Artificial Intelligence, novembre 2018, 5, www.accessnow.org

[2] WORLD COMMISSION ON THE ETHICS OF SCIENTIFIC KNOWLEDGE AND TECHNOLOGY, Report of COMEST on robotics ethics, 2017, 17, {https/URL}:/48223/pf0000253952.

[3] J. MCCARTHY, What Is AI? Basic Questions, in www.jmc.stanford.edu.

[4] Rapporto "Artificial Intelligence and Life in 2030", 2018, https://ai100.stanford.edu.

[5] ACCESS NOW, op. cit., 8.

[6] Committee on Technology, National Science and Technology Council (Organo esecutivo in funzione presso la Presidenza degli Stati Uniti – Executive Office of the President of the United States, Preparing for the Future of Artificial Intelligence, ottobre 2016, 5, https://obamawhitehouse.archives.gov.

[7] D. MALAN, Lesson on «Computational Thinking», in Computer Science for Lawyers course, Harvard, www.edx.org.

[8] A. PRETA, L'economia dei dati, Contributo scientifico di ASK Università Bocconi, 10 e ss.

[9] ACCESS NOW, op. cit., 9.

[10] S. YEE, T. CHU, A visual introduction to machine learning, http://www.r2d3.us.

[11] ACCESS NOW, op. cit., 10.

[12] ACCESS NOW, op. cit., 13.

[13] T. SIMONITE, When It Comes to Gorillas, Google Photos Remains Blind, in Wired, 1° novembre 2018,

su https://www.wired.com.

[14] C. MELI, Fake News e Intelligenza Artificiale: le due facce della medaglia, in Ultima Voce, 18 febbraio 2019, {https/URL}

[15] K. BREUNINGER, Mueller Probe Is Over: Special counsel submits Russia report to Attorney General William Barr, in CNBC, 22 marzo 2019, www.cnbc.com.

[16] Riconoscere le fake news con l'intelligenza artificiale, Convegno del 15 e 16 giugno 2018 a Piacenza organizzato dall'Università Cattolica, www.centridiricerca.unicatt.it.

[17] D. BENEDETTI, Fake news, il duplice e contrastante ruolo dell'intelligenza artificiale, in AI 4 Business, 8 giugno 2020, https://www.ai4business.it.

[18] S. QUATTROCOLO, Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo, in Revista Italo-Española de Derecho Procesal, Vol. 1/2019, 107 e ss.

[19] ACCESS NOW, The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems, https://www.accessnow.org.

[20] J. LARSON, J. ANGWIN, Machine Bias, in ProPublica, 23 maggio 2016, https://www.propublica.org.

[21] Come riscontrato dal Comitato per i diritti umani delle Nazioni Unite, nel commento all'articolo 14 del Patto internazionale per i diritti civili e politici, 2007, consultabile all'indirizzo https://digitallibrary.un.org. Sulle possibili interferenze dell'AI sull'iter logico-motivazionale seguito dal giudice ai fini della decisione, si veda S. QUATTROCOLO, Qualcosa di meglio del diritto (e del processo) penale?, in Discrimen, 26 giugno 2020.

[22] L. GOODE, Facial recognition software is biased towards white men, researcher finds, in The Verge, 11 febbraio 2018, https://www.theverge.com.

[23] V. RICCIUTO, La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, in I dati personali nel diritto europeo, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 25.

[24] S.M. BELLOVIN, When enough is enough: Location tracking, mosaic theory, and machine learning, in NYU Journal of Law and Liberty, 8(2), 2014, 555-628.

[25] La libertà di circolazione delle persone è assicurata dai c.d. Accordi di Schengen.

[26] ACCESS NOW, op. cit., 21.

[27] «Ogni individuo ha diritto alla libertà di pensiero, di coscienza e di religione. Tale diritto include la libertà di avere o di adottare una religione o un credo di sua scelta, nonché la libertà di manifestare, individualmente o in comune con altri, e sia in pubblico sia in privato, la propria religione o il proprio credo nel culto e nell'osservanza dei riti, nelle pratiche e nell'insegnamento» (art. 18 del Patto internazionale per i diritti civili e politici); «Ogni individuo ha diritto alla libertà di pensiero, di coscienza e di religione; tale diritto include la libertà di cambiare di religione o di credo, e la libertà di manifestare, isolatamente o in comune, e sia in pubblico che in privato, la propria religione o il proprio credo nell'insegnamento, nelle pratiche, nel culto e nell'osservanza dei riti» (art. 18 della Dichiarazione universale dei diritti umani); «Ogni individuo ha diritto a non essere molestato per le proprie opinioni. Ogni individuo ha il diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto, attraverso la stampa, in forma artistica o attraverso qualsiasi altro mezzo di sua scelta» (art. 19 del Patto anzidetto); «Qualsiasi propaganda a favore della guerra deve essere vietata dalla legge. 2. Qualsiasi appello all'odio nazionale, razziale o religioso che costituisce incitamento alla discriminazione, all'ostilità o alla violenza deve essere vietato dalla legge» (art. 20 del Patto); «È riconosciuto il diritto di riunione pacifica. L'esercizio di tale diritto non può formare oggetto di restrizioni tranne quelle imposte in conformità alla legge e che siano necessarie in una società democratica, nell'interesse della sicurezza nazionale, della sicurezza pubblica, dell'ordine pubblico o per tutelare la sanità o la morale pubbliche, o gli altri diritti e libertà» (art. 22 del Patto).

[28] Facebook Community Standards, consultabili su https://www.facebook.com.

[29] R. COSIO, Facebook e Social: Natura del contratto tra utente e social, in Ricerche giuridiche, Vol. 6 – Num. 1 – Giugno 2017, 133-154.

[30] M. IASELLI, Facebook rimuova i contenuti simili ad illeciti! La sentenza 3 ottobre 2019 (causa C-18/2018) della CGUE è molto innovativa sul fronte della responsabilità dei provider, in Altalex, 8 ottobre 2019, https://www.altalex.com.

[31] D. NOLASCO, P. MICEK, Access Now responds to Special Rapporteur Kaye on 'Content Regulation in the Digital Age, in ACCESS NOW, 11 gennaio 2018.

[32] R. SAMPERI, I diritti dei minori nella guerra civile siriana, in Rivista Cammino Diritto, n. 3/2020.

[33] K.O'FLAHERTY, YouTube keeps deleting evidence of Syrian chemical weapon attacks, in Wired, 26 giugno 2018, http://www.wired.co.uk.

[34] Y. TANG, Artificial intelligence takes jobs from Chinese censors, in Financial Times, 21 maggio 2018, https://www.ft.com.

[35] ACCESS NOW, op. cit., 23.

[36] ACCESS NOW, op. cit., 25.

[37] F. BORGIA, Profili critici in materia di trasferimento dei dati personali verso paesi extra-europei, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, I dati personali nel diritto europeo, Torino, 2019, 961-982.

[38] A. BRADFORD, The Brussels Effect, in Northwestern University Law Review, Vol. 107, 1, 2012.

[39] R. PERKINS, E. NEUMAYER, Does the 'California effect' operate across borders? Trading- and investing up

CamminoDiritto.it
ISSN 2421-7123

in automobile emission standards, in Journal of European public policy, n. 19/2012, 217-237.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=7518