World Law and Economics

GLOBAL KNOWLEDGE

#

Gerard van Schagen, World Map, 1689

Anno IV- Gennaio – Agosto 2018 n. 1-2 – Settembre-Novembre 2018 - Periodico quadrimestrale *on line open access*

PONTANI E ASSOCIATI - MILANO

EDITORIALE

In questo numero della nostra rivista proponiamo alla lettura due contributi che riteniamo di interesse.

Il primo inerisce un tema di particolare attualità, quello della *privacy*, anche perché essendo un tema risalente a tempi passati, solo ora ci si rende conto o appare ci si renda conto della portata del problema in un sistema sociale, finanziario ed economico, nel quale il mutamento dei rapporti tra soggetti a ragione delle nuove tecnologie, rende indispensabile un profondo mutamento culturale.

Il secondo, anticipato nell'editoriale del precedente numero di questa rivista, inerisce il rapporto tra intelligenza artificiale, robotica e responsabilità civile e la qualificazione della *persona elettronica*. Anche per questo tema si è in presenza di una diffusa ignoranza sociale e politica e vi è il rischio di pensare ad una disciplina giuridica della materia inadeguata ed in ritardo rispetto alle necessità di definire regole di tutela per la società civile.

In relazione alla questione della *privacy* assistiamo alla prima irrogazione di sanzioni per violazione delle norme dettate dal GDPR (*General Data Protection Regulation*, UE, n. 2016/679) in applicazione, in Italia, dal 25 maggio 2018. Citiamo, ad esempio, i casi di una sanzione di 4.800 euro ad un'azienda austriaca che usava male il sistema di videosorveglianza (Fritz Gernot, https://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator 5 oct. 2018), di 20 mila euro ad un'azienda tedesca per la mancata cifratura delle password degli utenti, (*ibidem*), di 400 mila euro ad una struttura ospedaliera portoghese per problemi di accesso ai dati (https://blog.cuatrecasas.com/propiedad-intelectual/hospital-do-barreiro-fined-by-comissao-nacional-proteccao-dados-in-400000-euro-for-allowing-improper-access-to-clinical-files/?lang=en) e a un procedimento di accertamento in corso nei confronti di una catena alberghiera (internazionale) di grandi dimensioni in relazione ad un caso di *data breach*, relativo al periodo 2014 - sett.2018, inerente i dati di oltre 500 milioni di persone, con la compromissione di 327 milioni di clienti anche in relazione all'utilizzo della carte di credito *(https://answers.kroll.com/*, con costante aggiornamento delle informazioni dal novembre 2018). A questi esempi non si può fare a meno di aggiungere, oltre alle sanzioni rilevantissime a seguito di investigazioni sui colossi del *web* come Google e Facebook, sia il caso (per il sistema valutativo dei comportamenti) della sanzione di £ 500.000 comminata (dopo rituale istruttoria e contraddittorio), il 24 ottobre 2018 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/) all'Infor mation Commissione's Office del Regno Unito, a Facebook, per la violazione (*at least 50 million accounts*) della disciplina sulla *privacy* (secondo i disposti del Data Protection Act , Section 55A) e, pertanto, con riferimento alla previgente disciplina normativa rispetto a quella del GDPR, sia il fatto che altre istruttorie sono in corso.

In riferimento, invece, al tema dell'intelligenza artificiale utilizzata nei più disparati ambiti (ad iniziare dai sistemi di interfaccia vocale degli smartphone e dei personal computer), non

vi è ancora consapevolezza reale, da parte degli utilizzatori – consumatori, della sua esistenza in moltissimi apparati tecnologici (anche indossabili), delle sue reali funzioni e del flusso di dati che da detti "oggetti" di uso assai diffuso viene indirizzato al mondo circostante con la possibilità, concreta, di intercettazione, acquisizione ed utilizzo di informazioni personali e non, ma utili anche economicamente utili.

L'intelligenza delle reti è poi distribuita ed il rischio moltiplicato a livello esponenziale in presenza di miliardi di computer che sono, nel sistema globale, fra di loro in costante interrelazione e comunicazione sistemica.

Solo per sottolineare la rilevanza dell'autonomia decisionale di una parte dei sistemi di intelligenza artificiale, basti fare mente ai quasi androidi del tipo Sophia, della Hanson Robotics Limited, di Hong Kong, (attivata il 19 aprile 2015 e presentata al pubblico in occasione del South by Southwest Festival, SXSW, tenutosi a metà marzo del 2016 ad Austin, Texas, USA). Detto quasi androide ha ottenuto (si tratta del primo caso al mondo) la cittadinanza saudita, durante i lavori del Future Investment Initiative summit (October 24, 2017, Ryad). Gli androidi possono divenire (in realtà sono già) espressione di una nuova realtà che vede gli intelligenti artificiali operare, forse competere con gli intelligenti naturali o, forse, ibridazioni degli stessi umani con componenti di intelligenza artificiale.

Il Direttore responsabile
Franco Pontani

SOMMARIO

Dottrina

In questo numero della rivista non vengono riportati testo od estremi di norme di legge, di pronunciamenti giurisprudenziali o di enti pubblici con poteri regolamentari. Tutti i riferimenti alle fontidella predetta natura sono riportate negli scritti di dottrina pubblicati.

Il Direttore responsabile

This page is left intentionally blank

Privacy e Protezione dei Dati
La nuova disciplina in un Sistema "Globale"

Franco Pontani

Il Regolamento (UE) N. 679 del 27 aprile 2016 del Parlamento europeo e del Consiglio
Intervento di apertura al Convegno del 13 luglio 2018. Camera dei Deputati - Sala Aldo Moro

Abstract

Privacy, protezione dati, società e impresa. Lineamenti di una riforma della tutela della *privacy* e della sicurezza dei dati. La persona al centro del sistema socioeconomico d'impresa. Organizzazione, tutela, responsabilizzazione e controllo, monitoraggio dei comportamenti nel sistema di gestione dei dati. La questione della cultura socio-ambientale

BIBLIOGRAFIA E SITOGRAFIA

BUSCEMA M., "*Squashing Theory. Modello a Reti Neurali per la Previsione dei Sistemi Complessi*", 1994, Armando, Roma; CANTONI L., DI BLAS N., *Teoria e pratiche della comunicazione*, Maggioli/Apogeo Education, http://www.apogeoeducation. com, Ott. 2002; DEL GOBBO G., "*Processo formativo tra potenziale di conoscenza e reti di saperi. Un contributo di riflessione sui processi di costruzione di conoscenza*", Firenze, University Press, 2007; DE MAURO T., "*Analfabeti d'Italia*", Internazionale, n. 734, 6 marzo 2008, http://internazionale.it; DENEAULT A., "*Governance. Il management totalitario*", Neri Pozza, I Colibrì, 2018; DI CRISTOFARO C., "*Stiamo crescendo una generazione di «ignoranti digitali»?",* 15 dicembre 2016, http://alleyoop.ilsole24ore.com/2016/12/15/stiamo-crescendo-una-generazio ne-di-ignoranti-digitali/. Indagine OCSE, *Dossier* MIUR, Pisa, 2012,"*Studenti, computer e apprendimento: dati e riflessioni*"; DI NUNZIO G. M., "*Dati e informazioni*" in http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf; EYSENCK H. J., *The structure of Human Personality*, Methuen & Company, London, 1953; FERRARA SANTAMARIA M., "*Il diritto alla illesa intimità privata*", Rivista di diritto privato, Cedam, 1937;GEERT C. Z, "*Mondo globale, mondi locali. Cultura e politica alla fine del ventesimo secolo",* Il Mulino, 1999; GIAMMARCO V. E., "*L'uomo digitale. Oltre il dualismo tecnologico*", Frenico self publishing hub; HAAS H., "*Wireless data from every light bulb*", TED (*Technology Entertainment Design*) Global, Edimburgo, Conferenza, 11-15 luglio 2011; HAMEL G., "*Primo, licenziamo tutti i manager*", 1 dicembre 2011, HBR Italia; HODSON R., ROSCIGNO V. J., LOPEZ S. H. (Ohio State University), "*Chaos and the Abuse of Power Workplace Bullying in Organizational and Interactional Context*", Work and Occupations, Vol.33, n. 4, November 2006, Sage Publications, http://wox.sagepub.com hosted at http://online.sagepub.com; LEWIS J. A., *"Rethinking Cybersecurity. Strategy, Mass effect and States*". A Report of the CSIS (Center for Strategic & International Studies) Technology Policy Program, Rowaman & Littlefield, Lanham, Boulder, New York, London, Jan. 2018; LUKÁS A., "*What is privacy? The history and definition of privacy*", University of Szeged, Faculty of Law and Political Sciences, Department of Labour Law and Social Security and Sorbonne Law School Université Paris 1, PhD student, lukacs.adrienn@juris.u-szeged.hu; MCCLIMANS F., FERSHT P., SNOWDON J., PHELPS B., LASALLE R., "*The State of Cybersecurity and Digital Trust 2016. Identifying Cybersecurity Gaps to Rethink State of the Art*," Accenture and HfS Research, Ltd, June 2016; Bharti V. (advocate and Vice President & Global Head - Security Services - Cyber, Cloud, IOT- and CISO at Happiest Minds Technologies Bengaluru Area, India), *White paper* (data non indicata), "*Unified Cyber Security Monitoring and Management Framework*", https:// www.happiestminds.com/whitepapers/Unified-Cyber-Security-Monitoring-and-Management-Framework.pdf;

MARANI S., "*Principio di ne bis in idem: la Corte di Giustizia ne delinea i limiti*", Corte giustizia Unione Europea, Grande Sezione, sentenza 20/03/2018 n° C-537/16, in http://www.altalex.com/documents/news/2018/03/21/ne-bis-in-idem-corte-di-giustizia; MASSARI M., "*Sopravvento del digitale e tramonto dell'essere umano. Un approfondimento in merito al sopravvento del digitale, passando per il tramonto dell'umano e la rinascita dell'uomo primitivo 4.0*", 31 marzo 2018, in http://www.responsabilecivile.it/sopravvento-del-digitale-tramonto-dellessere-umano/; MAZZA O., "*I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*", Relazione al Convegno di studi "*Garanzia dei diritti fondamentali e processo penale*", Diritto penale contemporaneo, Magistratura Democratica, Camera Penale di Milano, 9 -10 novembre 2012 Milano, "Diritto penale contemporaneo" 3/2013, in https://www.penalecontemporaneo.it/foto/49683_2013.pdf#page=10& view= Fit; MINGHETTI M., *"Humanistic Management 4.0*", http://www.marcominghetti.com/; MURGESE E., "*Analfabeti funzionali, il dramma italiano: chi sono e perché il nostro Paese è tra i peggiori*", in L'Espresso, http://espresso.repubblica.it/inchieste/2017/03/07/ news/analfabeti-funzionali-il-dramma-italiano-chi-sono-e-perche-il-nostro-paese-e-tra-i-peggiori-1.296854; PONTANI F., "*Corporate governance*", Digesto delle Discipline Privatistiche, Sezione Commerciale, Utet, 2009; PONTANI F., "*Ethics and privacy rules in a global digital world*",World law and economics. Global Knowledge, n. 1-2/2017, www.pontani.it; PONTANI F. "*Privacy e protezione dei dati*", Occasional papers, 10 febbraio 2018, www.pontani.it; RICCHIUTO P., "*Data Protection Officer: dentro, fuori, o da nessuna parte. Privacy e sicurezza*", 19 marzo 2018, http://www.interlex.it/privacyesicurezza/ricchiuto47.html; RUSCONI G., "*Azienda senza capi, una nuova via verso il «*Nirvana organizzativo*»*", Ambrosetti Global Leadership Summit (http://www.ilsole24ore.com/art/management/2016-07-05/azienda-senza-capi-nuova-via-il-nirvana-organizzativo-085 157.shtml?uuid=ADmh 4Fo; SOLOVE D. J., *"A taxonomy of privacy",* University of Pennsylvania Law Review, Vol. 154, January 2006, no. 3; 2013; SORO A., "*Vi spiego la cultura necessaria a proteggere i dati. Parola del Garante della Privacy*", "*Formiche*", n. 132, gennaio 2018, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/content/id/422841; UNESCO, *Handbook of Household Surveys*, Revised Edition, *Studies in Methods*, Series F, No. 31, United Nations, New York, 1984;VIGINI G., *Glossario di biblioteconomia e scienza dell'informazione*, Editrice Bibliografica, Milano, 1985; VIOLA F., "*Lo statuto giuridico della persona in prospettiva storica", in "Studi in memoria di Italo Mancini*", a cura di PANSINI G., Esi, Napoli 1999; VISCO I., "*Investire in conoscenza. Per la crescita economica*", Bologna, Il Mulino, 2009, cap. 3; VISCO I.," "*Il capitale umano per il XXI secolo*", Il Mulino, n. 1/2011, pp. 6-20; VISCO I.," *Investire in conoscenza, partendo dai libri*", 35° Seminario di Perfezionamento della Scuola per Librai, *"Tradizione e innovazione in libreria, Giornata conclusiva: Dove nascono le storie?*" Venezia, Fondazione Cini, 26 gennaio 2018.
VOCE "*Cultura*" in Vocabolario Treccani, http://www.treccani.it/vocabolario/cultura_%28Sinonimi-e-Contrari%29/); VOCE "*Mononucleare*", Vocabolario Treccani in http://www.treccani.it/vocabolario/mononucleare/; VOCE

Pontani e Associati S.p.A. - Piazza Castello 5 - 20121 Milano – www.pontanieassociati.com
E-mail fpontan@tin.it

"*Persona*" in http://www.treccani.it/enciclopedia/persona/, http:/ /www. treccani.it/enciclopedia/persona_%28Dizionario-di-filosofia%29/, , http:// www. treccani.it/ enciclopedia/persona_%28Universo-del-Corpo %29/; VOCE "*Persóna*", http://www.treccani.it/vocabolario/persona/;WARREN S. D., BRANDEIS L. D., "*The Right to Privacy*", Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890); WELCHMAN L., "*Managing Chaos: Digital Governance by Design",* Rosenfeld Media, Brooklyn, NY, USA, 2014; WIEDMAN S., "*Building a Digital Governance Program*", ISACA Geek Week, August 8 – 10, 2016, www.isaca. org/chapters3/Atlanta/AboutOurChapter/Documents/ GW 2016/ 08 08%204 pm-S.Wiedman-Digital%20 Governance.pdf; YAEL ONN I. et. al., *Privacy in the Digital Environment,* Haifa Center of Law & Technology, Niva Elkin-Koren, Michael Birnhack, eds., 2005, Pub. N. 7, in collaboration with The Caesarea Edmund Benjamin Digital Environment, Rothschild Foundation Institute for Interdisciplinary Applications of Computer Science, 2005/2006 - Haifa Center of Law & Technology.

SOMMARIO

1. Scenari

Il 25 maggio 2018 è entrato in applicazione il Regolamento (UE) N. 679, del 27 aprile 2016[1], Regolamento emesso contemporaneamente alla Direttiva (UE) N. 680/2016.

Ambedue questi provvedimenti normativi del Parlamento europeo e del Consiglio fanno parte di un sistema di regole indirizzate a rendere più solido e coerente, nell'Unione europea, il quadro di disciplina della protezione dei dati[2], quadro "*affiancato da efficaci misure di attuazione, **data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno***".

Si percepisce immediatamente la funzione strumentale del citato intervento regolatorio: non la tutela dei dati personali in sé, ma quella finalizzata allo sviluppo economico dell'Unione grazie ad un clima di maggiore fiducia.

La protezione dei dati personali è ricondotta al sistema dei principi e delle norme poste a tutela delle persone fisiche. Questo al fine del rispetto dei loro diritti e libertà fondamentali.

L'intendimento, dichiarato, del legislatore comunitario è quello di contribuire alla

> "*realizzazione di uno spazio di libertà, sicurezza e giustizia e di **un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno** e al benessere delle persone fisiche"*[3].

I principi che debbono essere rispettati, e che sono specificatamente richiamati, per la predetta tutela sono quelli dell'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea («Carta»[4]) e dell'art.16, par. 1, del Trattato sul Funzionamento dell'Unione Europea («TFUE»)[5] che stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano[6].

Lo scopo del Regolamento è anche quello di "*fare ordine*" nei comportamenti adottati dai singoli Paesi dell'Unione a seguito del recepimento, con modalità non uniformi, nelle legislazioni nazionali, della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, Direttiva abrogata con l'entrata in efficacia del Regolamento e quindi dal 25 maggio 2018.

Lo scenario in cui si inseriscono il Regolamento e la Direttiva del 2016 sopra richiamate deve, tuttavia, tener conto di numerosi interventi normativi e Raccomandazioni dell'Unione Europea tra i quali appaiono di rilievo:

1) la Raccomandazione della Commissione 2009/387/CE del 17 maggio 2009 sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza (*RFID, Radio-Frequency IDentification*)[7]
2) la Comunicazione della Commissione, COM (2015) 192 final, del 6 maggio2015, per una "*Strategia per il mercato unico digitale in Europa*". Nella Comunicazione si sottolinea che "***le tecnologie dell'informazione e della comunicazione (TIC)** non **costituiscono** più un settore a sé stante, bensì **il fondamento medesimo di tutti i sistemi economici innovativi moderni**. Via via che ne aumenta l'integrazione in tutti i settori della nostra economia e società, internet e le tecnologie digitali ci trasformano la vita, ci trasformano il modo di lavorare, nella sfera tanto personale quanto professionale e collettiva*"[8]

---

[1] Noto con l'acronimo *GDPR* (*General Data Protection Regulation*).

[2] In questo senso il 7° Considerando del Regolamento.

[3] In questo senso il 2° Considerando del Regolamento.

[4] "*Carta di Nizza*", 2000/C 364/01 del 18 dicembre 2000.

[5] "*Trattato di Lisbona*", del 13 dicembre 2007, efficace dal 1° dicembre 2009, in versione consolidata in Gazzetta ufficiale n. C 326 del 26/10/2012.

[6] Molto chiaramente il 1° Considerando del Regolamento.

[7] Si veda anche l'ampio lavoro del "*Gruppo di Lavoro Articolo 29*" (organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata, i cui compiti sono fissati all'art.30 della direttiva 95/46/CE e all'art. 15 della direttiva 2002/58/CE, in https://ec.europa.eu/info/law/law-topic/data-protection_en), istituito in forza dell'art. 29 della Direttiva 95/46/CE, ed in particolare il Parere n. 9/2011 sul tema. Per l'attività del Gruppo di lavoro il rinvio è a http://ec.europa. eu/ justice/article-29/documentation/opinion-recommendation/index_en. htm .
Il Gruppo di lavoro, con l'entrata in efficacia del GDPR, è stato sostituito dal "*Comitato europeo per la protezione dei dati*" che eredita (ed amplia) i compiti del "*Gruppo di Lavoro Articolo 29"* (https://edpb.europa.eu/edpb_it). Significativi sono i parr. 3.3.2. *Contrasto ai contenuti illeciti su internet* e 3.4. *Aumentare fiducia e sicurezza nei servizi digitali e nella gestione dei dati personali*.

[8] Significativi sono i parr. 3.3.2. *Contrasto ai contenuti illeciti su internet* e 3.4. *Aumentare fiducia e sicurezza nei servizi digitali e nella gestione dei dati personali.*

3) la Direttiva (UE) 2016/1148 del 6 luglio 2016 che reca *"misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" (nota anche come Direttiva *NIS, Network and Information Security*[9]) recepita in Italia con il D. Lgs. 18 maggio 2018, n. 65

4) la Proposta di Direttiva (COM 2016/590 final del 12. 10. 2016) che istituisce il "*Codice Europeo delle Comunicazioni Elettroniche*"[10].

Nel contesto rappresentato, si deve, anche e soprattutto, tener presente il fatto che, con le nuove tecnologie di informatizzazione e comunicazione, scompaiono sostanzialmente i confini geopolitici e, pertanto, di applicazione delle norme di tutela compatibili con una concezione di privacy di dato e di informazione personale[11].

Si deve precisare che non esiste una concezione di privacy universalmente condivisa e suscettibile di una concreta ed efficace tutela "*globale*" attraverso il ricorso a norme giuridiche che si possano, in un sistema mondializzato, ritenere altrettanto universalmente condivise ed applicabili[12].

Consegue il naturale limite di applicabilità delle predette norme alla sola Unione europea lasciando ampio spazio alle convenzioni con singoli Paesi, terzi rispetto all'Unione, o all'iniziativa di normazione legale autonoma dei singoli Stati.

I principi etici, laici e religiosi, come, d'altra parte, le norme giuridiche, in un sistema sociale inteso come globale, non sono universalmente condivisi. Siamo, di conseguenza, in presenza di concezioni di persona e di tutela dei dati che la riguardano assai differenziate nello spazio e variabili nel tempo.

Gli strumenti di cui si dispone per contrastare, realmente, nell'ottica della prevenzione e della sanzionabilità dei comportamenti dei soggetti che violano le regole poste a tutela dei dati riferiti o riferibili alla persona fisica, sono, in ogni caso, condizionati non solo dall'efficacia degli strumenti tecnici utilizzati allo scopo, ma anche dalla politica degli investimenti, pubblici e privati, dei e nei singoli Paesi, dalle priorità che governano tali politiche, dai livelli di democrazia sociale dei singoli Stati, dai sistemi culturali esistenti.

In altre parole, nell'Unione Europea, con il GDPR, ci troviamo di fronte all'avvento di un sistema di tutela "*de minimis*" che, allo stato, deve essere valutato nella sua concreta applicazione in modo armonizzato.

Se, da un lato, si è in presenza di interessi individuali e collettivi da tutelare attraverso l'intervento pubblico, dall'altro molto è delegato al sistema privato ed è a questo che, sostanzialmente si rivolge il Regolamento N. 679/2016.

Non si tratta, poi, solo di una questione di "*condivisione*" del concetto e del principio in uno scenario geopolitico internazionale od in presenza di culture diverse, ma del concetto di privacy in sé e che nel GDPR appare sostanzialmente indefinito; questo considerato il fatto che anche l'Unione europea vede una coesistenza di culture[13] e tradizioni (laiche e religiose) diverse, situazione che si aggrava anche a ragione dei fenomeni migratori che negli ultimi decenni si sono sempre più intensificati per le più disparate ragioni.

La difficoltà definitoria è rilevante perché di *privacy* si tratta in contesti diversi e a tutele differenziate a seconda dell'interesse specifico (di valore anche collettivo, sociale) oggetto di protezione.

In dottrina si è rimarcato che[14]:

"***It is difficult to define the right to privacy, since privacy is not a pure legal term*** *- it has psychological, social and political aspects. The conceptual difficulties in defining the right to privacy are due to the fact that various interests protected by the right are also protected by other laws and due to the fact that privacy is affected by political, social and economic changes and by technological developments".*

Si è, altresì sottolineato[15] che "***privacy is a concept in disarray***. *Nobody can articulate what it means*".

---

9 Di rilievo sono le attività di studio e ricerca sia dell'Autorità Garante per la protezione dei dati personali (https://www.garanteprivacy.it/) , sia dell'ENISA (*Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione*, istituita nel 2004. Il rinvio è a https://www.enisa.europa.eu/).
L'ENISA, il 29 giugno 2018, ha pubblicato un utile manuale sull'applicazione del GDPR alle PMI (SME), datato dicembre 2017 (*Handbook on Security of Personal Data Processing*) accessibile in https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing .

10 Nel momento in cui scriviamo risulta che l'ultima discussione, in Consiglio, sulla Proposta è del 29 giugno 2018 (https://eur-lex.europa.eu/procedure/IT/ 2016_288).

11 L'informazione è un insieme di dati, correlati tra loro, con cui un'idea (o un fatto) prende forma ed è oggetto di comunicazione (G. VIGINI, *Glossario di biblioteconomia e scienza dell'informazione*, Editrice Bibliografica, Milano, 1985, p. 62). Consegue che non si può confondere l'un termine con l'altro. I dati singoli possono solo essere raccolti o trasmessi, ma non costituiscono, singolarmente considerati, un'informazione.
Il dato è un segno (nelle sue due componenti di significato e significante) e come tale assume significato solo in un determinato contesto di relazioni tra entità biologiche ed assume diverse forme (scritto, immagine, movimento corporeo, ecc.). Sul tema, *ex multis*, il rinvio è a L. CANTONI, N. DI BLAS, *Teoria e pratiche della comunicazione*, Maggioli/Apogeo Education, in http://www.apogeoeducation.com /, Ott. 2002, Cap. I, pag. 1 e segg.

12 Il dibattito dottrinario in tema di *privacy* risale almeno al 1890 ed al lavoro di S. D. WARREN and L. D. BRANDEIS, "*The Right to Privacy*", pubblicato nell'Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220, da *The Harvard Law Review Association*. In Italia v. M. FERRARA SANTAMARIA, "*Il diritto alla illesa intimità privata*", in Rivista di diritto privato, Cedam, 1937, I, p. 168 e segg. e bibl. ivi citata.
Di particolare interesse è anche il lavoro di YAEL ONN et. al., *Privacy in the Digital Environment* (Haifa Center of Law & Technology, Niva Elkin-Koren, Michael Birnhack, eds., 2005, Pub. N. 7*)*, in collaboration with The Caesarea Edmund Benjamin digital environment Rothschild Foundation Institute for Interdisciplinary Applications of Computer Science, 2005/2006 - Haifa Center of Law & Technology.
Di utilità sono anche i contributi di A. LUKÁS, "*What is privacy? The history and definition of privacy*", University of Szeged, Faculty of Law and Political Sciences, Department of Labour Law and Social Security and Sorbonne Law School Université Paris 1, PhD student, lukacs.adrienn@juris.u-szeged.hu, e di A. MOORE, *Defining privacy*, Journal of Social Philosophy, Vol. 39, No. 3, pp. 411-428, Fall 2008, in https://ssrn.com/abstract=1980849.

13 Per "*cultura*" si intende "*l'insieme delle acquisizioni intellettuali di una persona ottenute mediante lo studio e l'esperienza*", ma anche "*l'insieme di valori, modelli di comportamento e simili, che caratterizzano il modo di vivere di un gruppo sociale […]*" e "[…] acquisita dall'ambiente" (VOCE "*Cultura*" in Vocabolario Treccani, http://www.treccani.it/vocabolario/cultura_%28Sinonimi-e-Contrari%29/).

14 YAEL et alt. cit. *Executive summary*, pag. vii.

15 D. J. SOLOVE, "*A taxonomy of privacy*", in University of Pennsylvania Law Review, Vol. 154, January 2006, no. 3, pagg.477-478.

*"As one commentator has observed, privacy suffers from «an embarrassment of meanings». **Privacy is far too vague a concept to guide adjudication and lawmaking**, as abstract incantations of the importance of «privacy» do not fare well when pitted against more concretely stated countervailing interests".*

In definitiva e in sintesi, si è pervenuti, in qualche modo, a qualificare questo complesso diritto in termini di "*confini*" seppur in un'ottica di sensibilità personale e quindi di qualificazione di ciò che è dai singoli definito o definibile come tale:

"***the right to privacy is our right to keep a domain around us**, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy enables us to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose*".

L'"*ambiente*" della *privacy*, profondamente mutato dall'evoluzione tecno-digitale, deve tener conto del fatto che:

"***the technological developments have created a new reality, on both the legal and the practical level**. While technological progress has changed the rules of the game completely, the legal system lags be-hind. While lawyers are still thinking over the appropriate form of regulation and its appropriate boundaries, the violators of privacy are accumulating knowledge, power and information and impose norms of conduct which will be almost impossible to uproot. A reality where there is no law and or-der raise the question: is it still possible to protect privacy? All of these issues lead to legal questions about the appropriate scope of the right to privacy and the choice of the best form of regulation*"[16].

Non siamo convinti, al di là dell'impatto conseguente al Regolamento 2016/679 ed ai provvedimenti allo stesso correlati o correlabili, quale la Direttiva 2016/680 e gli altri in precedenza richiamati, la situazione di tutela della *privacy* possa mutare in modo significativo in tempi contenuti.

Siamo al cospetto di una rilevante questione culturale delle comunità sociali e come tale ha necessità tempi molto lunghi per un mutamento sostanziale conseguente ad un'integrazione intersoggettiva che, per la sua natura sistemica, è di tipo precario.

In questo scenario il legislatore non è in grado, anche tenuto conto del fatto che i livelli culturali nazionali medi, di natura anche politica, sono assai carenti, di affrontare in modo coerente con l'evoluzione tecnologica, una questione estremamente complessa come quella dell'efficace ed efficiente tutela di questo composito diritto della persona.

2. La centralità della persona fisica

La persona fisica è il "*soggetto interessato*" alla tutela dei suoi dati ed informazioni.

La questione preliminare che si pone è cosa si intenda per "*persona*" e per "*persona fisica*".

Nel processo evolutivo dei rapporti umani la concezione di "*persona*" si è arricchita di connotazioni che l'hanno variamente definita, nel tempo, dal punto di vista antropologico, bioetico, filosofico, psicologico, religioso e giuridico, ponendo distinzioni tra la qualificazione fisica e quella mentale, sino ad interrogarsi sugli elementi costitutivi dell'essere umano[17].

In questa sede adottiamo la concezione di "*persona*" come "*individuo della specie umana, senza distinzione di sesso, età, condizione sociale e simili, considerato sia come elemento a sé stante, sia come facente parte di un gruppo o di una collettività*"[18].

La nozione di persona fisica quale desumibile dal sistema delle norme giuridiche nazionali ed internazionali non appare oggi più atta a qualificarla compiutamente ai fini dei suoi diritti oggetto di tutela.

Siamo in presenza di un difficile e non sempre condiviso e condivisibile rapporto tra etiche, culture e diritti, per cui appare più agevole pensare alla persona fisica come a un soggetto di diritto, dal concepito al vivente e, per certi aspetti, anche, sia pure in modo indiretto, in relazione al defunto.

In questa sede, ancora, non ci intratteniamo sulla vera natura della persona in presenza di ibridazioni dell'individuo vivente, con cellule recanti DNA diversi o con parti sostitutive (e inserite chirurgica-mente) provenienti da altro vivente umano (allotrapianto) e non umano (xenotrapianto) o da soggetto biologico deceduto (anche non umano), organi o loro parti con DNA compatibile, ma certamente non identico, stante l'individuata impossibilità; questo salvo il caso dell'isotrapianto (tra gemelli monocoriali), della sussistenza di individui geneticamente identici, ma altamente improbabile la sussistenza di DNA identici, con una necessaria ulteriore considerazione dei rapporti tra consapevolezza (intesa come percezione e reazione cognitiva) e memoria (intesa come capacità del cervello di conservare informazioni) e memoria cellulare[19] .

Nemmeno ci intratteniamo della questione dell'ibridazione del vivente umano con componenti elettroniche (protesi sostitutive o integrative del vivente) dotate di intelligenza artificiale e delle possibili interazioni tra i due tipi di intelligenza, nonché dei livelli ipotetici di prevalenza dell'artificiale sul naturale biologico.

Infine, non ci occupiamo delle relazioni tra la privacy

---

[16] *Ibidem*, pag. viii. V. anche F. PONTANI, "*Ethics and privacy rules in a global digital world*", e bibl. ivi citata, in World law and economics. Global Knowledge (*open access*) N. 1-2/2017, in www.pontani.it, e "*Privacy e protezione dei dati*", Occasional papers, 10 febbraio 2018, sempre in www.pontani.it.

[17] Per una rappresentazione dei diversi modi di qualificazione della persona v. VOCE "*Persona*" in http://www.treccani.it/enciclopedia/persona/ e http://www.treccani.it/enciclopedia/persona_%28Dizionario-di-filosofia%29/ nonché in http://www.treccani.it/enciclopedia/persona_%28Universo-del-Corpo%29/.

[18] VOCE "*Persóna*", in http://www.treccani.it/vocabolario/persona/.

[19] "*Ogni cellula del nostro organismo, tramite il suo DNA che funziona come un trasmettitore-ricevitore, emette e può ricevere segnali frequenziali. Tutte le cellule dell'organismo sono quindi in continua ed istantanea comunicazione fra di loro e si scambiano messaggi sotto forma di frequenze elettromagnetiche che hanno precisi effetti biologici. Le nostre cellule (ogni singola cellula del nostro corpo) contengono una vera e propria memoria. Ciò che chiamiamo «me-moria cellulare» è il campo energetico cellulare collettivo, generato dalle memorie cellulari individuali*", 18 agosto 2013 (a cura di "*Beatrice*" (https://www.fisicaquantistica.it/fisica-quantistica/memorie-cellulari, dalla fonte dichiarata, ora non più attiva, http://umaniindivenire.grou.ps/60_9767). Aggiungiamo che ponendo in stretta connessione cellule con DNA diversi si possono modificare sia le percezioni, sia le comunicazioni, sia i sistemi di memorizzazione del vivente.

della persona fisica e la persona elettronica, questa come definita come quella dei "*robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi*"[20].

Qui possiamo ricordare, con richiamo alla teoria dei sistemi (Ludwig Von Bertalanffy) e allo studio della loro dinamica (Jay Forrester), che una persona, in generale e, quindi, anche una persona fisica, può essere concepita come un sistema ultra-complesso, aperto, dinamico soggetto a flussi in entrata ed uscita di dati (poi elaborati) ed informazioni, consciamente od inconsciamente percepiti e memorizzati, ma tali da generare comportamenti o consentire l'accettazione e la condivisione di comportamenti di altri.

I dati sono rappresentazioni originarie, cioè non interpretate, di un fenomeno, evento, fatto, realizzate attraverso simboli, combinazioni di simboli o di qualsiasi altra forma espressiva, legate a un supporto[21] di qualsiasi natura.

Le informazioni sono quelle desunte dalla elaborazione e interpretazione dei dati che fluiscono attraverso rapporti di interrelazione.

L'elaborazione e interpretazione dei dati, le loro relazioni ed aggregazioni per trasformarli in informazioni, vengono adattate alle circostanze ambientali e, soprattutto, culturali.

Si tratta, per quanto qui non trattato, di temi che meritano amplissimo spazio ed approfonditi studi interdisciplinari, per altro in corso da svariati decenni.

Non è oggetto di approfondimento in questa sede la questione della differenza tra persona, soggetto ed individuo, differenza oggetto di interessante e complesso dibattito dottrinario; questo anche a ragione del fatto che le norme o dissertazioni e contributi scientifici in materia giuridica[22] utilizzano variamente i termini richiamati (a volte utilizzati impropriamente come sinonimi), ove il riferimento all'individuo è proposto anche con riferimento alla sua "*personalità*"[23].

Di interesse, in questa sede è, invece, il rapporto tra la persona fisica, l'azienda (come definita all'art. 2555 c.c.), in particolare quella di produzione o impresa (*ex* art. 2082 e segg. c.c.), e la sua organizzazione e, conseguentemente, anche altre persone fisiche. Ricordiamo anche che il GDPR si riferisce, in un'ottica regolatoria più ampia, a tutte le organizzazioni.

L'azienda (di produzione o di erogazione o mista, incluse quindi le aziende *no profit*, le associazioni senza scopo di lucro, le associazioni di volontariato, i comitati, i sindacati, i partiti politici, ecc. espressione tutti delle organizzazioni) diviene condizione essenziale per il trasferimento e la circolazione dei dati e delle informazioni degli individui persone fisiche e per la loro tutela, anche loro malgrado, cioè per proteggerli nonostante un loro possibile contrasto invocato un sovraordinato diritto di libertà, non definibili in modo assoluto e generale i limiti del secondo ed i confini del primo.

3. Il sistema organizzativo d'azienda e la tutela della persona fisica nella sua rappresentazione digitale. Il connubio tra sfera privata, comunicazione e azienda

Nell'ottica sistemica di qualificazione della persona fisica, cioè di un sistema complesso di informazioni e di dati in costante dinamica spazio-temporale, si perviene, nel sistema digitale globale e in quello dell'informazione senza confini, ad una sorta di rappresentazione digitale della persona, di un sé stesso come espressione di un sistema di dati dinamico[24].

Nell'azienda, da tempo, prevalgono sempre più le comunicazioni digitali, flussi di radiofrequenze (a mezzo di impulsi elettrici o di onde elettromagnetiche) attraverso sistemi cablati e non; questo comporta la possibilità di intercettazione, alterazione, appropriazione indebita di dati e informazioni.

Il connubio interaziendale[25] (cioè tra azienda di produzione - l'impresa- ed aziende di erogazione – in ispecie della famiglia in generale e di quella mononucleare[26]), in qualsiasi spazio-tempo, non rende agevole la realizzazione di un'adeguata tutela dei dati delle persone fisiche; questo, in particolare, in assenza di confini fisici e geopolitici al sistema delle comunicazioni wireless (WI-FI) e non solo, in attesa di valutare l'impatto delle nuovi sistemi di comunicazione LI-FI[27] (che utilizzano la luce LED visibile con impulsi luminosi ad alta frequenza).

---

[20] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL), P8_TA (2017) 0051, a seguito del *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics, Committee on Legal Affairs*, Rapporteur: Mady Delvaux.

[21] G. M. DI NUNZIO, "*Dati e informazioni*" in http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf.

[22] Per il rapporto tra uomo, soggetto, persona ed individuo e correlato riconoscimento, il rinvio, tra gli altri, è a F. VIOLA, "*Lo statuto giuridico della persona in prospettiva storica", in "Studi in memoria di Italo Mancini*", a cura di G.PANSINI, Esi, Napoli 1999, pagg. 636-637.
Si veda anche, tra gli altri, O. MAZZA, "*I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*", Relazione al Convegno di studi, organizzato da Diritto penale contemporaneo, Magistratura Democratica e la Camera Penale di Milano il 9 e 10 novembre 2012 presso l'Aula Magna del Palazzo di Giustizia di Milano, su "*Garanzia dei diritti fondamentali e processo penale*", in "*Diritto penale contemporaneo" 3/2013*, https://www.penalecontemporaneo.it/foto/49683_2013.pdf#page= 10 &view= Fit.

[23] H. J. EYSENCK, *The structure of Human Personality*, Methuen & Company, London, 1953, ove: "*la personalità è la più o meno stabile e durevole organizzazione del carattere, del temperamento, dell'intelletto e del fisico di una persona: organizzazione che determina il suo adattamento totale all'ambiente*".

[24] Sempre maggiore attenzione si dovrà dedicare alle ricerche in materia di "*antropologia digitale*" e all'emergente concezione di "*uomo digitale*". V. E. GIAMMARCO, "*L'uomo digitale. Oltre il dualismo tecnologico*", Frenico self publishing hub, 2013 e M. MASSARI, "*Sopravvento del digitale e tramonto dell'essere umano. Un approfondimento in merito al sopravvento del digitale, passando per il tramonto dell'umano e la rinascita dell'uomo primitivo 4.0*", 31 marzo 2018, in http://www.responsabilecivile.it/sopravvento-del-digitale-tramonto-dellessere-umano/.

[25] I singoli lavoratori vivono molte ore del loro tempo in, con e per l'azienda vuoi con scopo di lucro (impresa) vuoi assente tale scopo.

[26] La persona fisica e la famiglia sono espressione di aziende di erogazione. La famiglia mononucleare è costituita da un solo individuo (VOCE "*Mononucleare*", Vocabolario Treccani in http://www.treccani.it/vocabolario/mononucleare/).

[27] H. HAAS," *Wireless data from every light bulb*", TED (*Technology Entertainment Design*) Global, Edimburgo, Conferenza dell'11-15 luglio 2011.

Il citato connubio produce effetti diversi. Questo a ragione non solo dei conflitti di interessi personali (competizione per la carriera, contrasti di natura retributiva, associazionismo sindacale, ecc.), ma anche tra gruppi di persone legate tra loro da fini ed interessi condivisi, ma in conflitto con quelli dell'entità (l'impresa o l'azienda di erogazione) nella quale le persone svolgono la loro attività e determina.

Nell'evidente disordine che ne consegue, diventa difficile l'attuazione del "*chaos management in the workplace*"[28], in particolare, nell'impresa, cellula fondamentale del sistema economico produttivo della ricchezza, intesa come complesso dei beni, mobili e immobili, materiali ed immateriali posseduti da un qualsiasi soggetto, in un determinato tempo, e destinata al soddisfacimento dei suoi bisogni.

Le comunicazioni di cui parliamo avvengono spesso in ambiente fisico non protetto tecnicamente (si pensi al rapporto tra un lavoratore, dipendente o autonomo, ed il suo datore di lavoro ove il primo, il lavoratore, si pone in contatto con il secondo, il datore di lavoro, da un ambiente non protetto (ad esempio una strada cittadina).

Nel contesto ambientale di una qualsiasi entità l'utilizzo di strunmenti informatici e le comunicazioni *wireless* di natura privata si "*mescolano*" con quelle aziendali senza specifiche distinzioni e con la possibilità di illecite intercettazioni. Molti archivi sono condivisi e, frequentemente, l'accesso agli stessi non è disciplinato o le evidenze dello stesso accesso non sono indagate o non lo sono in modo adeguato.

Gli accessi illeciti, spesso, non sono soggetti a denuncia[29] alle Autorità preposte all'investigazione per l'individuazione (non sempre agevole o possibile) dei soggetti che hanno operato in violazione di regole date al fine dell'applicazione delle sanzioni di legge.

I sistemi organizzativi degli enti nei quali si concretano relazioni, anche private, delle persone dovrebbero garantire un adeguato sistema di tutela della *privacy* delle comunicazioni. Queste garanzie rendono indispensabile una riconsiderazione di tutti i sistemi tecnici esistenti in azienda, la definizione o ridefinizione delle procedure di comunicazione e del trattamento dati.

Specifica attenzione deve essere rivolta alla formale proceduralizzazione dei rapporti che vengono realizzati tra persone fisiche che ricoprono in azienda ruoli diversi e tra persone fisiche e strumenti digitali, più o meno caratterizzati da livelli differenziati di intelligenza artificiale, inclusa quella o quelle distribuite nei sistemi di comunicazione attraverso le reti digitali.

In altre parole, si deve ripensare, nel sistema organizzativo d'azienda, al concetto di *cybersecurity* ed alla sua efficiente ed efficace realizzazione tecnica.

4. *Governance* d'azienda, *digital governance* e costante monitoraggio.

La *governance* viene generalmente intesa come l'insieme di regole, di ogni livello, che disciplinano la gestione d'azienda in generale, e d'impresa in particolare, e include sia le relazioni tra i diversi attori coinvolti, gli stakeholder, cioè i portatori di interessi; gli attori principali sono, in genere, i soci o associati, il management, l'organo di gestione, gli organi di controllo.

Da una corretta governance consegue la massimizzazione, l'ottimizzazione della tutela dei soci, degli associati o dei componenti di entità senza scopo di lucro e con finalità sociale o di particolari aree di interesse collettivo.

Questo a prescindere dalla rilevanza economico-finanziaria della loro partecipazione al capitale sociale o al fondo di dotazione o alla raccolta di mezzi finanziari e non), sia gli obiettivi per cui l'impresa (o l'organizzazione senza finalità di lucro) è amministrata.

Il termine "*governance*" origina da un'analogia tra il governo delle città, delle nazioni o degli Stati ed il governo delle imprese. È a seguito di questo approccio di tipo analogico che derivano diversità di modelli e modalità applicative dei principi.

Ciò sempre in stretta relazione con le situazioni culturali e ambientali che connotano le diverse società civili ed economiche, il diverso sistema normativo, le diverse dimensioni d'impresa o di organizzazione in genere, anche in presenza di questioni cruciali, quali quelle dei rapporti tra proprietà e *management*, proprietà che designa anche gli organi di controllo, e comunque tra portatori di interessi (*stakeholder*), anche non economici, e soggetti che amministrano, governano, di fatto o di diritto, e controllano dette entità[30] .

In un mondo pervaso dalla comunicazione digitale per "***digital governance***" possiamo intendere

> "***a framework for establishing accountability, roles, and decision-making authority for an organization's digital presence - which means its websites, mobile sites, social channels, and any other Internet and Web-enabled products and services***[31]"

---

[28] Il rinvio, *ex multis*, è a R. HODSON, V. J. ROSCIGNO, S. H. LOPEZ (Ohio State University), "*Chaos and the Abuse of Power Workplace Bullying in Organizational and Interactional Context*", Work and Occupations, Vol. 33 N. 4, November 2006, Sage Publications, http://wox.sagepub.com hosted at http://online.sagepub.com, e a A. DENEAULT, "*Governance. Il management totalitario*", Neri Pozza, I Colibrì, 2018, tra le altre, pagg. 51-55.

[29] Questo per varie ragioni, incluse quelle riconducibili alla tutela della reputazione delle entità coinvolte dagli "*attacchi*" da parte di soggetti non identificati e non sempre identificabili. Da detto, diffuso, comportamento, non solo da parte delle organizzazioni lucrative e non, ma anche delle singole persone, consegue l'obbligo di denuncia alle Autorità competenti *ex* art. 33 del GDPR.

[30] Sul tema, ampiamente, *ex multis*, F. PONTANI, "*Corporate governance*" in Digesto delle Discipline Privatistiche, Sezione Commerciale, Utet, 2009.

[31] L. WELCHMAN, "*Managing Chaos: Digital Governance by Design",* Rosenfeld Media, Brooklyn, NY, USA, 2014, pag.11, richiamata anche da ISACA (*Information Systems Audit and Control Association, Inc*., A California Nonprofit Mutual Benefit Corporation), S. WIEDMAN, "*Building a Digital Governance Program*", ISACA Geek Week, August 8 – 10, 2016, in www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/GW2016/ 0808%204pm-S.Wiedman-Digital%20 Governance.pdf.

con la necessaria fissazione di "*digital strategies*[32]*, policies*[33] *and standards*[34] " e la realizzazione concreta di un loro costante monitoraggio in presenza dell'evoluzione dei sistemi di organizzazione e dei rapidi cambiamenti delle tecnologie.

Tutto ciò comporta l'esistenza di un sistema organizzativo complesso (anche in presenza delle c.d. *lean organization*), possibilmente reticolare (si pensi alle reti di impresa digitalmente interconnesse), indirizzato alla mappatura e prevenzione del, e contrasto al, **sistema dei rischi** (endogeni ed esogeni) dell'intero "*sistema azienda*" (di produzione o di erogazione che sia), incluse anche le *accounting* e *law firm* e qualsiasi altro soggetto che si trovi nelle condizioni di trattare, manipolare, utilizzare, trasmettere, conservare dati personali (e non solo tali).

Questo impone di pensare all'entità di cui trattasi come ad un soggetto che non può e non deve distinguere nel suo sistema organizzativo e di protezione dei dati solo una parte dei dati, quelli ritenuti personali, dagli altri dati, inclusi quelli che, solo all'apparenza, non si possono considerare personali ma che, aggregati ad altri, possono consentire l'individuazione e fissazione di relazioni con le persone fisiche generando informazioni che debbono essere tutelate nel contesto dello scenario normativo in precedenza sommariamente richiamato.

In un sistema dinamico, tecnologicamente ed organizzativamente complesso di rischi, si impone l'obbligo di attuare, applicare, valutare, adattare alle circostanze, quindi non solo prevedere[35] , delineare, progettare (art. 25 del GDPR e correlati Considerando nn.75 e 76) , un adeguato sistema di *cybersecurity*[36] (sottolineando che l'insicurezza digitale[37]ed il correlato rischio di una singola entità conducono ad un'infezione pandemica dei sistemi aperti e fortemente interconnessi) e, come detto, di un suo costante monitoraggio[38].

Qui si deve ricordare che, al di là dei difetti delle tecniche utilizzate (per quanto sofisticate esse siano), l'anello debole di qualsiasi sistema digitalmente interconnesso è la persona (sempre al centro del sistema) che, per difetto culturale o per incuria, non tiene conto dei (o non conosce i) fattori di rischio connessi anche alla spontanea divulgazione, con conseguente trattamento, dei suoi dati ed è sempre la persona che da tali difetti (diffusi) intende trarre (e trae) illecito vantaggio ricorrendo sempre all'utilizzo di sistemi tecnici (anche di avanguardia o sperimentali) esistenti o creati allo scopo.

La natura reale dell'organizzazione della singola entità che tratta i dati o, comunque ne dispone, deve essere oggetto di un'individuazione attenta e di una corretta diagnostica di rischio per difetto di adeguata *governance*[39].

5. La qualificazione di "*dato personale*" e il concetto di "*trattamento dei dati*"

La qualificazione di "*dato personale*" ai fini dell'applicazione del Regolamento UE 2016/679 si rinviene all'art. 4, n. 1, della norma ove il "***dato personale***" viene definito come

> "***qualsiasi informazione riguardante una persona fisica identificata o identificabile (il soggetto «interessato»)****; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Dobbiamo, tuttavia, considerare, ancorché indicati distintamente nello stesso articolo del dispositivo del Regolamento comunitario, **che "*dati personali*" sono anche i "*dati genetici*"** definiti (art. 4, n. 13) come

---

32 *Ibidem*, pag. 11 e in ISACA cit.

33 *Ibidem*, pag. 13 e in ISACA cit.

34 *Ibidem*, pag. 18 e in ISACA cit.

35 Ricorrendo anche alle applicazioni della "*squashing theory*" consistenti in modelli previsionali dei comportamenti con il ricorso alle reti neurali (M. BUSCEMA, "*Squashing Theory. Modello a Reti Neurali per la Previsione dei Sistemi Complessi*", 1994, Armando, Roma).

36 Una concezione da ripensare, ridefinire, riprogettare senza ricorrere o ricopiare modelli di altri. Sul tema v., *ex multis*, e non solo in relazione a ricerche e contributi dottrinari recenti, J. A. LEWIS, *"Rethinking Cybersecurity. Strategy, Mass effect and States*". A Report of the CSIS (Center for Strategic & International Studies) Technology Policy Program, Rowaman & Littlefield, Lanham, Boulder, New York, London, Jan. 2018 e F. MCCLIMANS, P. FERSHT, J. SNOWDON, B. PHELPS, R. LASALLE, "*The State of Cybersecurity and Digital Trust 2016. Identifying Cybersecurity Gaps to Rethink State of the Art*," Accenture and HfS Research, Ltd, June 2016.

37 Non esiste alcuna "*sicurezza digitale*", ma si debbono sempre considerare i livelli di "*insicurezza digitale*" e la loro rilevanza in termini di rischio in relazione alle singole circostanze. Ogni azienda è una singolarità, è espressione di un'unicità, è irripetibile nella sua genesi e nella sua gestione, non esiste un'azienda *standard*; le persone di ogni azienda sono diverse da quelle di un'altra azienda. Ogni standard di controllo deve essere adattato alla singola azienda.

38 *Ex multis*, per una rappresentazione sintetica, vedi V. Bharti (advocate and Vice President & Global Head - Security Services - Cyber, Cloud, IOT- and CISO at Happiest Minds Technologies Bengaluru Area, India), *White paper* (data non indicata), "*Unified Cyber Security Monitoring and Management Framework*", in https://www.happiestminds.com/whitepapers/Unified-Cyber-Security-Monitoring-and-Management-Framework.pdf , ove: "*In order to ensure a unified and holistic approach to cyber security, it's important to convert data (logs, packets, policies, activities, configurations etc.) available across various layers and across different functions/tools into real actionable intelligence. Some of the latest tools such as SIEM (Security Information and Event Management) have evolved on this premise and can serve as a basic building block for a unified framework*.". Questo si realizza procedendo per passi: "*Step 1 - Risk Awareness; Step 2: - Environment Awareness; Step 3: - Identity and Data Awareness; Step 4: - Business Awareness; Step 5: - Content Visibility; Step 6: Hidden Intelligence*".

39 Si pensi, ad esempio, ai sistemi di organizzazione fondati sui principi dell'*Humanistic Management 4.0* (sul tema il rinvio è a M. MINGHETTI, *"Humanistic Management 4.0*", in http://www.marcominghetti.com/ e alle teoriche ed alle applicazioni oggetto degli studi di Ginka Toegel (G. RUSCONI, "*Azienda senza capi, una nuova via verso il «Nirvana organizzativo»*", Ambrosetti Global Leadership Summit (http://www.ilsole24ore.com/art/management/2016-07-05/azienda-senza-capi-nuova-via-il-nirvana-organizzativo-085157.shtml?uuid=ADmh4Fo , e richiami all'evoluzione del tipo sociale di organizzazione, oggetto di applicazioni pratiche a partire dalle esperienze negli USA, dalla "*managerless organization*" alla "*timeless leadership*" ed al lavoro del "*Self management Institute*"). Sul tema il rinvio è agli studi di G. HAMEL (tra cui, HBR Italia, "*Primo, licenziamo tutti i manager*", 1 dicembre 2011).

*"**dati personali** relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica **che forniscono informazioni univoche** sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*".

Quella considerata come "*detta persona fisica*" presuppone l'individuazione della stessa e questo può avvenire anche attraverso i "*dati biometrici*".

*I **"dati biometrici"*** (art. 4, n. 14*)* sono i

*"**dati personali** ottenuti da un trattamento tecnico specifico **relativi alle caratteristiche** fisiche, fisiologiche o comportamentali **di una persona fisica che ne consentono o confermano l'identificazione univoca,** quali l'immagine facciale o i dati dattiloscopici*".

Tutto questo presuppone un'elaborazione di dati attribuiti ad una persona identificata o identificabile.

Infine, vi sono anche **"*i dati relativi alla salute*"** che sono ricondotti a quelli

"[..] *alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

Siamo in presenza di una segmentata qualificazione (non necessariamente esaustiva dell'intero sistema dei dati di cui trattasi) dei "*dati personali*", cioè attinenti alla persona, ad **una determinata persona identificata o identificabile** (art. 4 del Regolamento UE) attraverso quei dati opportunamente posti in relazione tra di loro.

In altre parole, il legislatore comunitario disciplina indifferentemente, ai fini della tutela giuridica delle persone, dati che, come detto, vengono posti in relazione fra di loro, con il ricorso a tecniche più o meno sofisticate, e informazioni che pertengono a persone fisiche, arrivando a qualificare le persone identificate o identificabili come soggetti di diritto e portatori di diritti che debbono essere tutelati.

Il **"*trattamento dei dati*"** viene definito (art. 4, n.2 del Regolamento) come

"*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati* (quindi anche con il ricorso a sistemi manuali) *e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione* (in un "*archivio*", ex art. 4, n.6 del Regolamento, un *data base* anche di tipo relazionale*), l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

Il "***processo automatizzato***" è anche quello peculiare dei sistemi di c.d. *intelligenza artificiale* presente nelle reti digitali della cui sicurezza si occupa il D. Lgs.18 maggio 2018, n. 65, di attuazione della Direttiva NIS.

Nel predetto *"trattamento"* è inclusa la c.d. "profilazione" definita (art. 4, n. 4) come

"*qualsiasi forma* (espressione che appare amplissima e tecnicamente indefinita o indefinibile, quindi assolutamente generica) *di **trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali*** (pensiamo ai dati che, coordinati a sistema, consentano anche di realizzare un oroscopo personale, di rilievo in alcuni sistemi culturali) *per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti*[40] *di detta persona fisica*".

Per il trattamento dei dati degli "*interessati*" sia il "*titolare del trattamento*", sia il "*responsabile del trattamento*" debbono tenere (salvo ricorrano le condizioni di esonero dall'obbligo di cui al comma n. 5[41]), in forma scritta od elettronica (*ex* comma n. 3), appositi registri (art.30 del Regolamento).

Il "*titolare del trattamento*" deve tenere il "*registro delle attività di trattamento*" (comma 1), mentre ogni soggetto "*responsabile del trattamento*" deve tenere un registro "*di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento*".

Si tratta di registri, particolarmente utili in quanto indispensabili per ogni valutazione e analisi del rischio, con contenuti normati, variamente regolati, ma liberi nelle forme e soggetti all'obbligo di esibizione alle Autorità vigilanti.

Siamo in presenza di registri sistematico-cronologici a forma libera, ma con contenuto minimo obbligatorio.

6. La sicurezza del trattamento dei dati, l'*accountability* ed il "*sistema*" delle responsabilità

Nel sistema azienda (ed in particolare nell'impresa) e nel suo subsistema di controllo interno è sempre più di rilievo la questione di un'adeguata e diffusa consapevolezza dei rischi e delle loro conseguenze sulle persone e sulla sua gestione economica, patrimoniale e finanziaria.

I rischi interni ed esterni debbono essere noti in relazione al tipo di attività dell'azienda ed al mutare delle circostanze oggettive e soggettive.

I rischi debbono essere costantemente riconsiderati nel rapporto tra possibilità e probabilità di accadimento e valutazione di impatto sulle diverse risorse

---

[40] Si pensi all'utilizzo dei dati rilevabili dai dispositivi digitali indossabili dotati di un GPS, cioè di un sistema che consenta, anche in modo indiretto od approssimativo, di rilevare il posizionamento geo-temporale di una persona.

[41] A detti soggetti non è comunque inibita la tenuta dei registri su base volontaria. Si veda anche il "*Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*" del 19 aprile 2018 e la "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*", in "*Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili*" dell'Autorità Garante per la protezione dei dati personali (https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#registro).

dell'azienda, impatto da considerare anche in termini di rischio del venir meno delle condizioni di funzionamento dell'azienda stessa. Questo anche allo scopo di ricorso gli strumenti di negoziazione dei rischi ed il ricorso ad adeguati strumenti assicurativi.

Il tema della "*sicurezza dei dati*" è da porsi in stretta relazione con il "*trattamento*" degli stessi (art. 32 del GDPR), nel rapporto "*stato dell'arte*" e "*costi di attuazione*", consapevoli sempre del fatto che non vi sono gestioni esenti da rischi.

La sicurezza di cui trattasi, oltre che di tutti i dati connaturati ad una concezione di tipo globale delle attività d'azienda, per i dati personali deve tenere specifico conto (art. 32 del GDPR) della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio, di varia probabilità e gravità, per i diritti e le libertà delle persone fisiche.

Allo scopo (art. 32 del GDPR) debbono essere adottate misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

A ben vedere, non si tratta di proteggere dai predetti rischi solo i dati personali ma, in un'entità convenientemente organizzata per la tutela di tutti i suoi dati, di adottare le misure indicate dal GDPR, in modo pervasivo dell'intero sistema dei dati e delle informazioni aziendali e quindi non esclusivamente di quelli relativi alle persone fisiche.

Appare, infatti, concretamente più semplice ed economicamente conveniente, porre in sicurezza tutti i dati invece di porsi il problema di una non sempre facile distinzione tra dati personali, dati potenzialmente riconducibili alle persone fisiche e dati che, con assoluta certezza, non hanno queste connotazioni.

Per altro, un sistema di *cybersecurity* globale d'impresa (o di altro tipo di azienda) risponde meglio agli obiettivi del sistema di controllo interno volto alla tutela patrimoniale (ed i dati, tutti i dati, sono, nella società dell'informazione e della comunicazione, sono componenti del patrimonio d'azienda).

L'adozione di codici di condotta (artt. 32 e 40 del GDPR), il loro costante monitoraggio (art. 41) ed il ricorso, anche volontario, a sistemi di certificazione (art. 42) sono espressione di regole razionali di qualsiasi organizzazione che nel suo sistema organizzativo dovrebbero essere in funzione in stretta coerenza con un adeguato sistema di controllo interno volto, come detto, a garantire la conservazione del patrimonio delle sue informazioni (ricordiamo i principi informatori, in sede comunitaria, della circolazione, e appropriata conservazione, dei dati ai fini di una corretta gestione dell'economia dei dati[42] e delle informazioni).

In presenza di regole da osservare non si possono non individuare soggetti che debbono rendere conto, anche alle Autorità vigilanti (art. 33) ed agli stessi interessati (le persone fisiche i cui dati sono oggetto di trattamento) delle violazioni di dette regole.

I soggetti che debbono considerare, valutare, interpretare i dati, i segni ed il loro essere coordinati a sistema e, quindi, generatori di informazioni personali (quelli del "*soggetto interessato*", ex Capo III del GDPR 679/2016) meritevoli di tutela, sono elencati all'art. 4 del Regolamento comunitario[43] ed in capo agli stessi gravano, in relazione alla loro attività, doveri di comportamento e correlate *responsibility* e *accountability*[44]).

Si tratta, in particolare, del "*titolare del trattamento*"[45] (art. 24) o del suo "*rappresentante*"[46] (art. 27), dei "*contitolari del trattamento*"[47] (art. 26), del "*responsabile del trattamento*" (art. 28), del "*responsabile della protezione dei dati*"[48] (artt. 37, 38, 39) o "*data protection officer (DPO)*"[49]. Questa nuova figura di soggetto responsabile appare, allo stato, ancora indefinita od indefinibile in termini concreti, sia quando la sua designazione avvenga con l'individuazione di un soggetto interno all'organizzazione ovvero esterno alla stessa[50]

Il Regolamento non fa alcun riferimento all'"***amministratore di sistema***" che è stato oggetto di disciplina all'art. 1, comma 1, lett. c) d.P.R. 318/1999 e di provvedimenti dell'Autorità Garante della protezione dei dati ("*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici*

---

42 Tra gli ultimi documenti comunitari si vedano la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "*Costruire un'economia dei dati europea*" https://eur-lex.europa.eu/legal-connt/EN/TXT/?uri=COM:2017:9:FIN e la "*Commission staff working document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy*" {COM(2017) 9 *final*} in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC 0002.

43 L'art. 4, n.8 del GDPR definisce *"«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

44 *Nella posizione dell'Autorità Garante dei dati sembra si equipari la* responsibility all'*accountability*, ma i due termini, nella lingua inglese, hanno un diverso significato che qui ci sembra utile sottolineare, anche ai fini giuridici: "*the main difference between responsibility and accountability is that responsibility can be shared while accountability cannot. Being accountable not only means being responsible for something but also ultimately being answerable for your actions. Also, accountability is something you hold a person to only after a task is done or not done. Responsibility can be before and/or after a task*" in https://www.diffen.com/difference/Accountability_vs_Responsibility.

45 "*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali [omissis*]" (art. 4, n. 7).

46 *"La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento"* (art. 4, n. 17).

47 "*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (art. 4, n. 8).

48 Si tratta di una "*figura*" nuova nel panorama della normativa comunitaria dotata di particolare autonomia e di un'articolata cultura interdisciplinare, di designazione obbligatoria o volontaria a seconda dei casi disciplinati dal GDPR.

49 Di particolare interesse sul tema sono le *Linee guida sui responsabili della protezione dei dati del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati (WP 243 rev. 0),* adottate il 13 dicembre 2016 emendate e adottate il 5 aprile 2017.

50 Eloquente e concreto quanto rappresenta P. RICCHIUTO nel suo scritto "D*ata Protection Officer: dentro, fuori, o da nessuna parte. Privacy e sicurezza*", 19 marzo 2018, in http://www.interlex.it/privacyesicurezza/ricchiuto47.html.

relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, modificato con provvedimento del 25 giugno 2009 [51]).

Tale soggetto viene definito come "***figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti***", altro tipo di figura professionale ritenuta equiparabile, dal punto di vista dei rischi relativi alla protezione dei dati, a quelle dell'amministratore di basi di dati, dell'amministratore di reti e di apparati di sicurezza e dell'amministratore di sistemi *software* complessi.

Non siamo in presenza di un mutamento del novero dei soggetti responsabili, ma di una previsione di specifiche figure, sempre professionali dell'area informatica, per le quali il GDPR prevede specifici compiti, non facendo venir meno preesistenti e, in parte, differenti posizioni di responsabilità.

Qui si ricorda che, nel "***sistema sanzionatorio***" le (pesanti) **sanzioni** previste dal GDPR (art. 83) sono **di natura amministrativa** e non escludono **sanzioni civili** (a titolo di risarcimento danni subiti dai soggetti interessati e dalle entità di riferimento a ragione della violazione dei disposti del Regolamento) e **sanzioni penali** lasciate per la loro previsione normativa e modalità applicativa all'iniziativa dei singoli Paesi dell'Unione[52].

Questo a tacere della **corresponsabilità tra persone** diverse all'interno della stessa organizzazione.

La materia **delle responsabilità non amministrative** trova specifico richiamo all'art. 82 del GDPR ove si sottolinea la natura, come detto, amministrativo - pecuniaria delle sanzioni previste dallo stesso GDPR (art.83).

Non sono, tuttavia, escluse altre sanzioni (civili e/o penali) che sono liberamente applicabili nei singoli Stati membri dell'Unione anche non in relazione a comportamenti sanzionati dal GDPR, ma sempre in relazione a comportamenti da osservare in forza delle disposizioni di detto Regolamento (art.84) ove si sottolinea che "***tali sanzioni devono essere effettive, proporzionate e dissuasive***".

7. La questione della cultura socio-ambientale. Conoscenza, ignoranza funzionale e comunicazione digitale

A seguito di quanto sin qui esposto appare evidente che la materia della *privacy* e della tutela dei dati e delle informazioni delle persone non possa non considerare, anche per il rapporto tra comportamenti e accountability, responsabilità amministrativa, civile e penale, la questione della cultura socio-ambientale.

Il tema è di particolare rilievo ai fini di un'efficace tutela di un diritto così personale come quello della *privacy* ed al tempo stesso non consegnato alla sola sfera della singola persona in quanto l'uomo è un "*animale sociale*", vive in una società di persone, vive, nei tempi attuali, a contatto con un mondo virtuale che non percepisce appieno.

Ciò che di nocivo al suo essere "*persona di relazioni*" derivava e deriva, ancora in parte, dall'interrelazione fisica immediata o di natura comunicativa a distanza, anche con l'utilizzo di strumenti meccanici ed elettrici, più o meno sofisticati.

Oggi l'essere umano vive altresì immerso nel mondo delle comunicazioni digitali, in un complesso sistema di segnali coordinati o che lo possono essere traendo dagli stessi informazioni che possono essere indirizzate anche al nocumento fisico, psicologico, economico e finanziario delle singole persone o di intere collettività.

L'essere umano[53], sostanzialmente, vive con strumenti elettronici (dispositivi) di comunicazione, li indossa (*wearable devices*)[54], li porta costantemente con sé, ne è preda, ne è dipendente[55], ma non li conosce realmente o li conosce solo modestamente, parzialmente, in relazione alle loro reali, complesse, funzioni e fattori di rischio, diretto ed indiretto.

Il nostro Paese ha raggiunto non invidiabili primati mondiali in termini di ignoranza, non conoscenza, non cultura e spesso non comprensione sostanziale dei fatti del mondo contemporaneo e tra-smettono, con assoluto convincimento della loro fondatezza, pseudo conoscenze[56].

Non si realizzano sufficienti investimenti nella

---

51 In https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499. Si veda anche, per il richiamo a questa figura professionale la Delibera n. 13 "*Lavoro: le linee guida del Garante per posta elettronica e internet [1387522]*" dell'1 marzo 2007, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/doc web/1387522.

52 Si veda il Considerando n. 149 del GDPR ove si sottolinea che *"l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia*". Questa, ricordiamo, per il rispetto dell'art 'art. 50 della "*Carta dei diritti fondamentali dell'Unione europea*", letto alla luce dell'art. 4, del protocollo n. 7 della "*Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*", firmata a Roma il 4 novembre 1950, enuncia tre criteri di riferimento per una corretta valutazione della singola fattispecie: "*Il primo consiste nella qualificazione giuridica dell'illecito nel diritto nazionale, il secondo nella natura dell'illecito e il terzo nel grado di severità della sanzione in cui l'interessato rischia di incorrere*" (*ex multis*, v. S. MARANI, "*Principio di ne bis in idem: la Corte di Giustizia ne delinea i limiti*", Corte giustizia Unione Europea, Grande Sezione, sentenza 20/03/2018 n° C-537/16, in http://www.altalex.com/documents/news/2018/03/21/ne-bis-in-idem-corte-di-giustizia.

53 Il bimbo e l'adolescente, come l'immigrato che chiede l'elemosina all'angolo di una qualsiasi strada delle grandi città italiane, e non solo, utilizzano uno *smartphone*, anche solo per gioco, distrazione abituale.

54 A volte sono anche posti all'interno del suo corpo per stimolazioni muscolari o neurali o per ragioni di monitoraggio clinico con comunicazione a soggetti terzi vigilanti.

55 *Nomofobia* e *vamping* sono le connesse nuove patologie da connessione "*sociale*" pressoché senza interruzione, di giorno nel primo caso, di notte nel secondo, e che affliggono non solo gli adolescenti, ma persone di tutte le età e di qualsiasi livello di istruzione.

56 C. GEERTZ, "*Mondo globale, mondi locali. Cultura e politica alla fine del ventesimo secolo"*, Il Mulino 1999, pag. 16, ove: *"Il modo in cui gli uomini intendono le cose e reagiscono ad esse il modo in cui se le figurano, le giudicano e reagiscono sfugge sempre di più alla nostra conoscenza […] Ciò di cui abbiamo bisogno sono nuovi modi di pensare capaci di frequentare particolarità, individualità, stranezze, discontinuità, contrasti e singolarità[…] Ciò di cui manchiamo sono gli accessi che sappiamo ricavare comunque da questi modi di essere da questa pluralità, il senso di un'unione che non è né globale, né uniforme, né originaria, né costante, ma non di meno reale*".
Queste argomentazioni sono fatte proprie da G. DEL GOBBO, "*Processo formativo tra potenziale di conoscenza e reti di saperi. Un contributo di riflessione sui processi di costruzione di conoscenza*", Firenze, University Press, 2007, pag. 90, ove sottolinea che "*in un momento storico in cui assistiamo ad una crescente circolarità di informazioni rischiamo di cadere in forme di pseudo conoscenza*".

conoscenza ed il capitale umano[57] perde di pregio in quanto non riesce più a distinguere il vero dal falso, il reale, il concreto fisico dall'immaginario (è sufficiente che vi sia un'informazione nel web, una comunicazione e/o un'immagine digitale, su *facebook, twitter, messanger, instagram* o altri *social network*, di qualsiasi densità essi siano, utilizzino o meno *Internet*).

La sua ignoranza non dipende dall'invecchiamento (lungo e progressivo) della popolazione possibile grazie ad un diverso tipo di alimentazione, al progresso della medicina e della chirurgia, all'utilizzo di macchine che alleviano la fatica fisica, ecc., ma anche da pigrizia, superficialità e discontinuità nell'**apprendimento**[58].

Superata la fase storica dell'ignoranza strutturale diffusa, quella dell'analfabetismo proprio dell'incapacità di leggere e scrivere, quella dell'incapacità totale di decifrare uno scritto, siamo ora a dovere fare, da molti anni, i conti con l'**analfabetismo funzionale inteso come incapacità di un individuo di usare in modo efficiente le abilità di lettura, scrittura e di calcolo nella vita quotidiana**[59].

L'"*OECD Survey of Adult Skills (PIAAC), Diagnostic report, 5 October 2017*[60]*, reveals that over 13 million adults ─ or 40% of Italy's adult population ─ have low numeracy and literacy skills. This is much higher than the share of low-skilled adults across OECD countries, who on average make up 27% of the population. It is also higher than what is observed in Germany and Poland, where the share of low-skilled adults comprises 23% and 29% of the population, respectively. Italy also has a relatively low share of first-time tertiary graduates at 35% ─ on par with countries like Hungary, Mexico and Luxembourg ─ compared to the OECD average of 49%. But, on the upside, Italian workers display relatively good 'readiness-to-learn and problem solving' skills, suggesting that more targeted education and training policies could help develop and make better use of skills*".

Il nostro Paese è anche "*ricco*" di **analfabeti digitali** (inclusi i c.d. "*nativi digitali*"), **soggetti che "*non distinguono una notizia da una pubblicità online, non considerano* minimamente l'attendibilità delle fonti delle notizie su Internet, sono facilmente ingannabili dai messaggi postati sui Social Network**"[61].

Non siamo solo di fronte ad una questione di anzianità della popolazione (afflitta anche da una naturale regressione della conoscenza originariamente conseguita attraverso la formazione scolastica), ma anche ad un grave difetto di formazione scolastica (di ogni ordine e grado) e di **formazione acquisita nelle comunità socio-ambientale** di costante frequentazione e interscambio di conoscenze ed attraverso la quale **si perde la cognizione della differenza tra mondo reale, quello fisico-psichico di natura essenzialmente biologica, mondo virtuale, spesso espressione di un mondo in cui frequentemente la maschera, lo rende ingannevole o immaginario**.

La questione della cultura socio-ambientale, non solo digitale[62], è di assoluto rilievo per la tutela efficiente ed efficace della *privacy*, travalica i confini sensibili del singolo individuo, si intreccia con il sistema globale e, pertanto, anche dell'azienda famiglia (e di ogni altra azienda di erogazione) e dell'azienda impresa, siano esse espressione di organizzazioni pubbliche o private.

La sostanziale carenza culturale, intuitivamente, in materia di intelligenza artificiale e nelle sue applicazioni anche ambientali per monitoraggi, di varia natura, di cose e persone (i c.d. sistemi *smart* di video- sorveglianza, comunicazione tra dispositivi, raccolta intelligente dei rifiuti, dei sistemi di manutenzione in remoto dei *computer*, di riscaldamento, di domotica, ai nuovi assistenti intelligenti - da Siri a Cortana a Google *home* -, ecc.) comporta, in una società umana connotata da gravi livelli di superficialità e sciatteria comportamentale ed incapacità funzionale (irrilevanti i titoli di studio dei singoli), un'estrema difficoltà nell'operare in concreto ai fini della prevenzione dei rischi non previsti.

---

57 Sull'inadeguatezza del capitale umano del nostro Paese il nostro riferimento, *ex multis*, è a I. VISCO," *Investire in conoscenza, partendo dai libri*", intervento del Governatore della Banca d'Italia al 35° Seminario di Perfezionamento della Scuola per Librai su *"Tradizione e innovazione in libreria, Giornata conclusiva: Dove nascono le storie?*" Venezia, Fondazione Cini, 26 gennaio 2018 ed ai suoi: "*Investire in conoscenza. Per la crescita economica*", Bologna, Il Mulino, 2009, cap. 3, e "*Il capitale umano per il XXI secolo*", Il Mulino, n. 1/2011, pp. 6-20.
Sullo stesso tema, il rinvio è a T. DE MAURO, "*Analfabeti d'Italia*", Internazionale, n. 734, 6 marzo 2008, http://internazionale.it ed al più recente E. MURGESE, "*Analfabeti funzionali, il dramma italiano: chi sono e perché il nostro Paese è tra i peggiori*", in L'Espresso, http://espresso.repubblica.it/inchieste/2017/03/07/ news/analfabeti-funzionali-il-dramma-italiano-chi-sono-e-perche-il-nostro-pa ese-e-tra-i-peggiori-1.296854 , ove: "*Come ricordava Tullio De Mauro, «la regressione rispetto ai livelli acquisiti nel percorso scolastico colpisce dappertutto gli adulti». «Occorre -, quindi, secondo lo studioso che più di tutti in questi ultimi anni ha continuato ad avvertire dei pericoli dell'analfabetismo, riflettere su stili di vita e assetti sociali che producono questi dislivelli di competenze e queste masse di deprivati tra gli adulti»*".

58 Si vedano i programmi dell'UE di "*lifelong learning*":" *The Lifelong Learning Programme (LLP) was designed to enable people, at any stage of their life, to take part in stimulating learning experiences, as well as developing education and training across Europe*" in (http://ec.europa.eu/education/lifelong-learning-programme_en).

59 UNESCO, *Handbook of Household Surveys*, Revised Edition, *Studies in Methods*, Series F, No. 31, United Nations, New York, 1984, par. 15.63, ove: " *a person is functionally illiterate who cannot engage in all those activities in which literacy is required for effective functioning of his group and community and also for enabling him to continue to use reading, writing and calculation for his own and the community's development*".

60 In http://www.oecd.org/skills/oecd-skills-strategy-for-italy-diagnostic-report-rome-2017.htm.

61 C. DI CRISTOFARO, "*Stiamo crescendo una generazione di «ignoranti digitali»?",* 15 dicembre 2016 in http://www.alleyoop.ilsole24 ore.com/ 2016/12/15/ stiamo-crescendo-una-generazione-di-ignoranti-digitali/. Si veda anche il Dossier del MIUR, Indagine OCSE, Pisa 2012,"*Studenti, computer e apprendimento: dati e riflessioni*", pagg. 5-8.
Non si può operare in modo adeguatamente tutelato nel mondo digitale se non si percepisce correttamente quello reale, meglio, quello realtà fisica in cui viviamo quali esseri biologici, con i relativi rischi, rischi che nel mondo digitale, quello della realtà virtuale, si moltiplicano all'inverosimile in forza di applicazioni tecnologiche ignote alla massa di coloro che, come persone fisiche, si pongono in relazione con persone ed organizzazioni utilizzando strumenti al cui uso concreto non sono stati preparati in modo adeguato.

62 Non si può operare in modo adeguatamente tutelato nel mondo digitale se non si percepisce correttamente quello reale, meglio, quello realtà fisica in cui viviamo quali esseri biologici, con i relativi rischi, rischi che nel mondo digitale, quello della realtà virtuale, si moltiplicano all'inverosimile in forza di applicazioni tecnologiche ignote alla massa di coloro che, come persone fisiche, si pongono in relazione con persone ed organizzazioni utilizzando strumenti al cui uso concreto non sono stati preparati in modo appropriato.

In estrema sintesi, per dirla con le parole di Antonello Soro, Presidente dell'Autorità garante per la protezione dei dati personali,

> "*ciò che, più di ogni altra misura, garantirà l'effettività dei diritti sanciti sarà la diffusione di quella «cultura*[63] *della privacy» necessaria per promuovere, a un tempo, sviluppo economico e libertà, efficienza amministrativa e dignità della persona*".

8. Conclusioni

Il Regolamento generale sulla protezione dei dati (General Data Protection Regulation), del 27 apri-le 2016, dei cui lineamenti fondamentali abbiamo trattato, rappresenta un dettato normativo da porsi in relazione alla disciplina legale dei rapporti tra le persone e le organizzazioni in uno scenario tecnologico di amplissima portata e che impone una necessaria riconsiderazione delle tutele della persona in un complesso rapporto tra diritti e doveri, tecnologie e sistemi di responsabilità.

Il frazionamento delle disposizioni legali esistenti ed un certo grado di disarmonia nei comportamenti dei singoli Paesi dell'Unione Europea hanno reso necessario fare chiarezza e stabilire norme comuni.

Un'attenzione particolare deve essere altresì posta al titolo del provvedimento sul quale molto si è scritto e detto con una visione contenuta, limitata a quella dei dati e delle informazioni relative alla persona fisica nell'intento della sua tutela.

Lo scenario deve essere ampliato. La protezione, anche nell'interesse delle organizzazioni, deve essere ridefinita, ma questo presuppone un diverso modo di concepire l'architettura delle organizzazioni e la diffusione di una cultura, generale e condivisa, della sicurezza nel mondo digitale, nel quale siamo immersi, del quale siamo parte integrante, pronti alle relazioni con la persona elettronica ed a un'integrazione tra intelligenza biologica e intelligenza artificiale.

Il percorso è lungo e le possenti forze di resistenza al cambiamento rischiano di determinare fratture sociali con la generazione di classi tecnocratiche dominanti grazie all'integrazione di soggetti, individuali e collettivi, e di gruppi sociopolitici, con le tecnologie digitali ed i sistemi di intelligenza artificiale, indirizzati verso una diversa concezione di persona e di *privacy* e dei suoi sistemi tecnologici e giuridici di tutela.

63 "*Vi spiego la cultura necessaria a proteggere i dati. Parola del Garante della Privacy*", Intervento di A. SORO, "*Formiche*", numero 132, gennaio 2018, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display / content/id/7422841 .

World Law and Economics Global Knowledge 1-2 (2018) 13-19

Robotica, intelligenza artificiale e responsabilità civile
La resposabilità civile della persona elettronica

Franco Pontani

Abstract

Lo scritto affronta un tema delicato, quello del rapporto tra persona umana e persona elettronica alla luce della sempre maggiore integrazione tra il naturale biologico, la sua ibridazione con componenti artificiali ed un futuro prossimo che deve essere oggetto di attenta valutazione preventiva. Questo non solo in considerazione della situazione in atto di rapidissima rivoluzione tecnologica e sostanzialmente priva di condivise regole etiche e giuridiche, ma in attesa di un'evitabile futura consapevolezza di consapevolezza di esistenza autonoma dei sistemi di intelligenza artificiale atti a generare problematiche di relazione sociale e di responsabilità di quei *robot* che hanno già raggiunto elevati livelli di autonomia di giudizio ed azione nei rapporti con altri *robot*, con l'ambiente e la società umana . L'Unione Europea ha assunto una posizione che merita attenzione e primi commenti.

BIBLIOGRAFIA E SITOGRAFIA

AMIGONI F., SCHIAFFONATI V., SOMALVICO M., *Intelligenza artificiale*, in Enciclopedia della Scienza e della Tecnica, Treccani, 2008, in http://www.treccani.it/enciclopedia/intelligenza-artificiale_%28Enciclope-dia-della-Scienza-e-della-Tecnica%29/; BAUR C., WEE D., *Manufacturing's next act*, June 2015, in https://www.mckinsey.com/business-functions/opera tions/our-insights/manufacturings-next-act; BOLDRINI N., *Indagine RISE (Research & Innovation for Smart Enterprise)*, Università degli Studi di Brescia, *Da Industria 4.0 a Impresa 4.0, dalle parole ai fatti*, 21 gennaio 2018, in https://www.internet4things.it/industry-4-0/indagine-rise-da-industria-4-0-a-impresa-4-0-dalle-parole-ai-fatti/; BONOMI C., *Tassare i robot è una scorciatoia senza sbocchi*, Il Sole24Ore, 23 marzo 2017; CARLUCCI AIELLO L., *Intelligenza artificiale*, in Enciclopedia Italiana, IX Appendice, 2015; CARMAN C.C., EVANS J., *On the epoch of the Antikythera mechanism and its eclipse predictor*, in *Archive for History of Exact Sciences*, Vol. 68, nº 6, 15 novembre 2014; CAROBENE A., *Intelligènza artificiale. Approfondimento*, in http://www.treccani.it/enciclopedia/intelligenza-artificiale/; CECCARELLI M. (a cura di), ROMDHANE L., ZEGHLOUL S., *Distinguished Figures, Mechanism and Machine Science Their Contributions and Legacies*, Part 2, Springer Dordrecht Heidelberg London, New York, 2010; FLORIDI L., *Infosfera*, in *Internet & Net Economy*, DI BARI V. (a cura di), Il Sole 24-Ore Libri, 2002; FONTANA G., *In viaggio con il padre dell'infosfera*, Il Sole24Ore, 20 maggio 2010; GALLINO L., *La società, perché cambia, come funziona. Un'introduzione sistemica alla sociologia*, Paravia, Torino, 1980; MACI L., *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare*, in *Economy Up*, 9 ottobre 2017, in https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare; MASINI C., *Lavoro e risparmio*, UTET, Torino, 1986; MELLO P., *Intelligenza artificiale*, Documentazione Interdisciplinare di Scienza e Fede, 2002, in http://disf.org /intelligenza-artificiale; REDAZIONE, Insieme è meglio, *Pastorelli: sui "Robot" Salvini è distratto, il progetto di legge c'è già*, 8 febbraio 2018; RIGUZZI F., *Introduzione all'intelligenza artificiale*, gennaio 2006, in https: //arxiv.org/pdf/1511.04352.pdf e in Terre di Confine, Anno 2, Numero 1, gennaio 2006, in http://www.terredi-confine.eu/introduzione-all-intelligenza-artificiale/, poi aggiornata (v.2) il 16 ottobre 2016, in https: //arxiv.org/abs/1511.04352, Cornell University Library; RODOTÀ S., *Uno statuto giuridico globale della persona elettronica*, testo del discorso tenuto, sul tema *"Un mondo, una Privacy"*, l'11 ottobre 2001, alla sessione conclusiva della Conferenza internazionale sulla protezione dei dati, Parigi, 24-26 settembre 2001, in http://www.interlex.it/675/rodota5.htm; SAVELLI F., *La prima fabbrica 4.0 di McKinsey*, in *Corriere Economia*, 11/12 agosto 2016; SELBER J.C., in AA.VV., *Telemicrosurgery: Robot Assisted Microsurgery*, Springer - Verlag France, 2013; TREMOLADA L., *La strana idea di tassare i robot*, Il Sole24Ore, 21 febbraio 2017; Voce *Robòt*, in Vocabolario Treccani, in http://www.treccani.it/vocabolario/robot/; Voce *Robot*, in Enciclopedia Treccani, in http://www.treccani.it/enciclopedia/robot/; Voce *Robotica*, in Enciclopedia Treccani in http://www.treccani.it/enciclopedia/robotica/.

SOMMARIO

1. Premessa

L'evoluzione tecnologica con la quale la società si confronta da almeno 10 anni ha assunto ritmi di accelerazione e di integrazione interdisciplinare senza precedenti.

La rapidità di mutamento coinvolge diverse aree dell'industria di produzione di beni e servizi e la loro circolazione nel sistema globale, fisico e virtuale.

Ciò richiede un costante monitoraggio del rapporto che si realizza tra l'utilizzo di strumenti tecnologicamente avanzati (non autonomi od autonomi nel loro operare), ad ausilio ed affiancamento dell'uomo nelle sue molteplici attività (anche in sempre più marcata autonomia o totale sostituzione dell'uomo), e la necessità di concepire in nuovi modi l'organizzazione del lavoro.

È il momento della *lean organization*, di una diversa qualificazione del capitale umano, di un diverso modo di fare formazione.

È evidente che strumenti diversi e modalità differenti del loro utilizzo possono comportare problemi di varia natura e generare diversi e nuovi livelli di responsabilità individuale e collettiva.

Questo, inoltre, accade in una società che, dal punto di vista delle conoscenze e dei saperi, individuali e di gruppo, è ancora *"inadeguata"* rispetto alle nuove necessità anche per carenze, talvolta gravi, nella formazione scolastica, culturale e universitaria, ancora lenta nel realizzare ineludibili integrazioni interdisciplinari.

Ai punti che seguono in sintesi si rappresenterà un percorso e si formuleranno considerazioni e valutazioni in tema di rischio e responsabilità conseguenti all'uso di applicazioni tecnologiche che vedranno una sempre più marcata applicazione della c.d. *"intelligenza artificiale"* in sistemi dinamici complessi ed ultracomplessi[1].

2. La robotica. Nozione (sommaria) ed evoluzione

La robotica ha per oggetto lo studio e la realizzazione di *robot* e le loro applicazioni pratiche nelle attività di produzione industriale e di ricerca scientifica e tecnologica[2]. Ai *robot* ci si è spesso riferiti denominandoli anche *"automi*[3] *meccanici"* per la loro originaria natura di macchine semoventi, non elettroniche, utilizzate per il supporto all'uomo in lavori faticosi[4].

Con l'evoluzione tecnologica la meccanica diviene *"meccatronica"* (dalla combinazione dei termini *"meccanica"* ed *"elettronica"*), disciplina che studia le interazioni con l'elettronica e l'informatica (dalla combinazione dei termini *"informazione"* e *"automatica"*). Ciò ha reso possibile, tramite l'informazione automatizzata attraverso l'elettronica, una sempre maggiore automazione e precisione dei sistemi di produzione ed ha contribuito alla semplificazione del lavoro e, in parte, alla sostituzione del lavoro dell'uomo.

La meccatronica si occupa, in particolare, di sistemi di controllo del movimento, noti anche come *Motion Control*. Tra i suoi principali campi di applicazione vi sono quelli nella robotica.

I *robot* sono apparecchiature in movimento o che gestiscono processi nei quali il movimento (quello più accurato possibile) trova nell'informatica la sua possibilità di maggiore precisione e versatilità per cui l'utilizzo avviene in campi sempre più svariati, superando quello della meccatronica di cui la robotica è parte naturale.

Nella robotica confluiscono apporti di molte discipline sia di natura umanistica, come la linguistica, sia di natura scientifica come biologia, fisiologia, psicologia, elettronica, fisica, informatica, matematica e meccanica.

Ma la robotica si evolve e l'apparecchiatura automatica (a diversi livelli di autonomia) si integra con l'elettronica e con i programmi informatici (istruzioni prescrittive di comportamento fondate su informazioni di natura cognitiva[5]), e si transita ai *bot*, che si pongono in relazione fra loro, in comunicazione anche automatica, tra loro e con il mondo circostante, in modo diretto e remoto, con sistemi di rete complessi ed interconnessi.

Quindi i sistemi divengono sempre più integrati in relazione con la società, con l'ambiente fisico in generale, con il mondo animale, vegetale, con l'uomo e le sue componenti organiche a vario livello dimensionale e di funzionamento. Diventano, pertanto. sempre più complessi da realizzare e da controllare, con il rischio di operare in campi od aree non ancora conosciuti a fondo, con immaginabili conseguenze.

L'evoluzione dell'informatica ha condotto anche alla realizzazione di *software* che generano *software*, a strumenti, a macchine che apprendono attraverso sensori sempre più sofisticati e che possono, teoricamente, evolversi acquisendo sempre maggiore autonomia. A questo punto si parla di intelligenza artificiale e di relazioni della stessa con il sistema globale vivente, con intuitive conseguenze.

3. L'intelligenza artificiale. Nozione (generale) e scenari evolutivi

Con il progredire sempre più rapido della ricerca scientifica e delle sue applicazioni concrete (moltissime quelle sperimentali in corso) risulta difficile formulare una definizione condivisa di intelligenza artificiale delle macchine. Gli indirizzi di pensiero scientifico in materia si sono divisi nei due filoni della IA *"debole"* e della IA *"forte"*: il primo ritiene che i sistemi robotici

---

1 *"Un sistema è un insieme i cui elementi sono avvinti da relazioni di interdipendenza"* (cioè di connessione reciproca). Un sistema si definisce complesso quando è *"altamente elaborato e riccamente interconnesso, senza per questo superare la possibilità di una descrizione completa"*; è ultracomplesso quando è *"così complicato da non poter essere descritto in modo preciso e dettagliato"*. V. C. MASINI, *Lavoro e risparmio*, UTET, Torino, 1986, pp.29-39. Un sistema dinamico ha la caratteristica di evolvere o modificarsi nel tempo, in particolare se è di tipo *"aperto"* cioè che ha interazioni con il mondo esterno e scambia con lo stesso energia, materia, informazioni.

2 Voce *Robotica*, in Enciclopedia Treccani in http://www.treccani.it/enciclopedia/robotica/.

3 Il termine *"automa"* deriva dal greco αὐτόματος, *automatos*, *"che agisce di propria volontà"*. La sua definizione, tuttavia, non collima con l'utilizzazione del termine nel contesto colloquiale, in quanto in questo, risulta riferibile a soggetto che non pensa ma si comporta in modo automatico.

4 Il termine *Robot*, dal cèco *Robot ‹ròbot›*, designa un *"apparato meccanico* […] *programmabile, impiegato nell'industria, in sostituzione dell'uomo, per eseguire automaticamente e autonomamente lavorazioni e operazioni ripetitive, o complesse, pesanti e pericolose"* (Voce *Robòt*, in Vocabolario Treccani, in http://www.treccani. it/vocabolario/robot/. La funzione di detto *"apparato"* è quella di *"Manipolatore riprogrammabile, multiscopo progettato per muovere oggetti, parti, attrezzi, o apparecchiature specializzate attraverso vari movimenti, programmati per l'esecuzione di una varietà di compiti"* (Voce *Robot*, in Enciclopedia Treccani, in http://www. treccani.it/enciclopedia/robot/). Occorre anche precisare che la nozione di *"programmazione"* è riconducibile sia alla meccanica, sia ai sistemi elettromeccanici ed ancora all'elettronica ed all'informatica e non è incompatibile con la nozione di *"automa meccanico"*. Basti pensare alla *"macchina di Anticytera"* (C.C. CARMAN, J. EVANS, *On the epoch of the Antikythera mechanism and its eclipse predictor*, in *Archive for History of Exact Sciences*, Vol. 68, nº 6, 15 novembre 2014, pp. 693-774), un autentico calcolatore meccanico risalente, presumibilmente, al 250 A.C., o all'automa programmabile del 1206 D.C. di Abū al-'Iz Ibn Ismā'īl ibn al-Razāz al-Jazarī [anche in M. CECCARELLI (a cura di), L. ROMDHANE, S. ZEGHLOUL, *Distinguished Figures, Mechanism and Machine Science Their Contributions and Legacies*, Part 2, Springer Dordrecht Heidelberg London, New York, 2010 pp. 1-21] al quale viene attribuito il primo progetto documentato di automa programmabile, in https://www.ebuliz.com/. Per una sintetica, ma non necessariamente esaustiva sintesi di testimonianze di costruzione di automi e *robot*, v. https://www.history.com/news/history-lists/7-early-robots-and-automatons, e J.C. SELBER, in AA.VV., *Telemicrosurgery: Robot Assisted Microsurgery*, Springer - Verlag France, 2013, p. 19-30, in particolare p. 20.

5 Si qualificano come *"informazioni cognitive quelle che dicono cosa è avvenuto, cosa sta avvenendo o cosa avverrà entro un sistema o nel suo ambiente"* (L. GALLINO, *La società, perché cambia, come funziona. Un'introduzione sistemica alla sociologia*, Paravia, Torino, 1980, pp. 26-27).

possano pervenire solo alla simulazione di alcuni processi cognitivi umani, mentre il secondo indirizzo esprime il convincimento che i sistemi robotici conseguiranno un'intelligenza propria, autonoma e indipendente, pari od anche superiore a quella umana[6].

Le definizioni sino ad oggi formulate appaiono sempre ancora generiche e tendono a rifarsi sempre a definizioni dell'intelligenza umana. Non fanno emergere, in modo specifico, i limiti dell'artificiale in relazione al conseguimento di una consapevolezza dello stesso artificiale di essere, di esistere, di fare parte un *"qualcosa"*. Pertanto, allo stato, se ne possono considerare solo le attitudini emulative del funzionamento del cervello umano[7].

Si tratta di una scienza, ancora giovane, *"che affronta il problema di come rappresentare, manipolare e costruire conoscenza circa fatti, azioni e leggi di causalità. Da un punto di vista metodologico, i ricercatori di intelligenza artificiale hanno l'obiettivo di costruire programmi per l'elaboratore che realizzino alcune attività intellettuali proprie dell'uomo, congiuntamente al tentativo di spiegare i principî basilari dell'intelligenza"*[8].

I *"vantaggi"* generalmente percepiti dell'intelligenza artificiale al servizio della società e del sistema *"ambiente"*, nella più ampia accezione del termine, sono riconducibili all'integrazione tra discipline scientifiche diverse con una velocità di trattamento e, pertanto di elaborazione ed analisi, anche statistica, dei *big data*, cui consegue la possibilità di ampliare le interazioni tra uomo e macchina e tra macchine, la capacità di integrare i sensi percettivi degli esseri viventi (sistemi di realtà aumentata), di ridurre determinate categorie di rischio grazie a sistemi cognitivi più approfonditi ed integrati della realtà fenomenica, di indagare meglio e più a fondo per trovare soluzioni a problemi finora apparivano di difficile od impossibile soluzione a causa della numerosità delle informazioni disponibili od acquisibili, ecc..

In considerazione del fatto che siamo in presenza di una scienza giovane, che deve ancora sperimentare molto, la sua evoluzione deve considerarsi *"praticamente senza limiti"*, per le scoperte scientifiche che, grazie ad essa e alle sue applicazioni, si potranno realizzare in moltissimi campi.

4. L'impresa 4.0

Nell'ambito delle applicazioni di maggior rilievo e impatto pressoché immediato, nate dal connubio tra robotica ed intelligenza artificiale, vi sono quelle relative al mondo dell'impresa di produzione, della finanza, della comunicazione, del commercio.

È nata l'**impresa 4.0** a testimoniare della quarta rivoluzione industriale[9] **(Industria 4.0)**, grazie all'utilizzo sempre più diffuso delle nuove tecnologie informatiche (*"intelligenti"*).

Tale industria viene principalmente connotata dai seguenti indirizzi di sviluppo: 1) la gestione dei dati e connettività, tramite gli strumenti dei *big data*, l'*internet* delle cose (*Internet Of Things*, IOT) e la tecnologia *cloud*; 2) gli *analitycs*, che realizzano un'analisi avanzata dei dati, e l'*intelligence*, che automatizza l'attività umana; 3) l'interazione uomo-macchina, che si esprime mediante interfaccia *touch screen*; 4) il transito dal mondo virtuale a quello reale, grazie alle stampanti 3D, i *robot* collaborativi e il risparmio energetico[10].

Dalla tecnologia applicata ai processi industriali si transita ad una implicita fase successiva, ad un nuovo modo di fare impresa, per cui il concetto e paradigma di riferimento non si fondano più solo sulle tecnologie, ma sul modo di lavorare delle persone nelle imprese, ove svolge un ruolo fondamentale la formazione, e in modo specifico quella universitaria[11].

L'adozione di questo nuovo concetto e di questo nuovo paradigma impone profonde modifiche strutturali delle organizzazioni di impresa e dei suoi impatti sulle persone, sulla società e sull'ambiente. Ne conseguono una differente modalità di mappatura dei rischi ed una riconsiderazione dei sistemi di prevenzione, di tutela e di costante mappatura dei rischi globali, anche in relazione alla *cyber security* e alla difesa nei sistemi competitivi che ricorrono alle *cyberwar*.

Infine, occorre ridefinire i rapporti, anche etici, sul fondamento del principio di responsabilità con

---

[6] F. RIGUZZI, *Introduzione all'intelligenza artificiale*, gennaio 2006, in https://arxiv.org/pdf/1511.04352.pdf e in Terre di Confine, Anno 2, Numero 1, gennaio 2006, in http://www.terrediconfine.eu /introduzione-all-intelligenza-artificiale/, poi aggiornata (v.2) il 16 ottobre 2016, in https://arxiv.org/abs/1511.04352, Cornell University Library.

[7] Per una ricognizione storica, il rinvio, *ex multis*, è a P. MELLO, *Intelligenza artificiale*, Documentazione Interdisciplinare di Scienza e Fede, 2002, in http://disf.org/intelligenza-artificiale. Per una definizione v. A. CAROBENE, *Intelligènza artificiale. Approfondimento*, in http://www.treccani.it/enciclopedia/intelligenza-artificiale/ e L. CARLUCCI AIELLO, *Intelligenza artificiale*, in Enciclopedia Italiana, IX Appendice, 2015.

[8] F. AMIGONI, V. SCHIAFFONATI, M. SOMALVICO, *Intelligenza artificiale*, in Enciclopedia della Scienza e della Tecnica, Trecani, 2008, in http://www.treccani.it/enciclopedia/intelligenza-artificiale_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/.

[9] Le precedenti rivoluzioni a cui si fa riferimento sono quelle: *"del 1784 con la nascita della macchina a vapore e di conseguenza con lo sfruttamento della potenza di acqua e vapore per meccanizzare la produzione; del 1870 con il via alla produzione di massa attraverso l'uso sempre più diffuso dell'elettricità, l'avvento del motore a scoppio e l'aumento dell'utilizzo del petrolio come nuova fonte energetica; del 1970 con la nascita dell'informatica, dalla quale è scaturita l'era digitale destinata ad incrementare i livelli di automazione avvalendosi di sistemi elettronici e dell'IT (Information Technology)"*; L. MACI, *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare*, in *Economy Up*, 9 ottobre 2017, in https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare.
La prima esperienza italiana è della McKinsey come testimoniato da F. SAVELLI, *La prima fabbrica 4.0 di McKinsey*, in *Corriere Economia*, 11/12 agosto 2016, ove vengono individuate le quattro direttrici di sviluppo ed investimento di quella che possiamo qualificare come la *"nuova industria"*, ed ancor prima, da C. BAUR, D. WEE, *Manufacturing's next act*, June 2015, in https://www.mckin sey.com/business-functions/operations/our-insights/manufacturings -next-act.

[10] In https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare/, cit..

[11] N. BOLDRINI, *Indagine RISE (Research & Innovation for Smart Enterprise)*, Università degli Studi di Brescia, *Da Industria 4.0 a Impresa 4.0, dalle parole ai fatti*, 21 gennaio 2018, in https://www.internet4things.it/industry-4-0/indagine-rise-da-industria-4-0-a-impresa-4-0-dalle-parole-ai-fatti/.

individuazione dei soggetti ai quali le responsabilità devono essere legalmente attribuite.

5. Il *robot "intelligente"* e la sua *"personificazione"*

Lo scenario evolutivo rappresentato vede l'emergere rilevante del ruolo della robotica e dell'intelligenza artificiale in tutti i campi: nella *"nuova impresa"* digitale, nell'informazione e nella comunicazione, e nella società che risulta sempre più influenzata, nei suoi comportamenti e nelle sue attese, dai sistemi robotici e dalle applicazioni di intelligenza artificiale, anche di tipo indossabile od integrabili nell'organismo vivente. In questo scenario la questione della responsabilità civile conseguente a danni derivanti dall'utilizzo di tali tecnologie diviene oggetto di una necessaria riconsiderazione non solo in termini etici, ma anche giuridici.

In due documenti dell'Unione europea (specificatamente, nella bozza di mozione[12] sulla *"personalità elettronica"* presentata da Mady Delvaux, nell'ambito di un *gruppo di lavoro per le questioni legali relative allo sviluppo della robotica e dell'intelligenza artificiale* nell'Unione con specifico riferimento agli aspetti legali civili[13] e poi nella Relazione del 27 gennaio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica[14] *"integrata"* dai pareri di diverse Commissioni) il *"robot intelligente"*, cioè dotato di *"intelligenza artificiale"*, viene qualificato come soggetto per il quale bisogna prevedere uno specifico *status* di *"persona elettronica"*.

Nella bozza di mozione [par. 31, lett. f)] in relazione al tema della responsabilità, si richiama l'attenzione della Commissione sulla necessità di esplorare le implicazioni di natura legale connesse ai *robot* intelligenti:

> *"creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the* ***status of electronic persons with specific rights and obligations****, including that of making good any damage they may cause, and applying* ***electronic personality*** *to cases where robots make smart autonomous decisions or otherwise interact with third parties independently".*

Nella Relazione del gennaio 2017, recante raccomandazioni alla Commissione dell'Unione in un'ottica di lungo periodo e in uno scenario complesso connotato dalla rappresentazione dei casi di maggior rilievo attinenti all'impiego di sistemi robotici, la Commissione giuridica [par. 59, lett. f)] formula l'invito di esaminare e valutare:

> *"l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi".*

Nel contesto tuttavia emerge l'assenza, in sede europea, di una definizione comune e condivisa di *"robot intelligente"*, anche se (nell'Allegato alla Proposta di risoluzione - Definizione e classificazione dei *"robot intelligenti"*) ne vengono enunciate le sue *"caratteristiche"* fondamentali: *1. capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati; 2. capacità di apprendimento attraverso l'esperienza e l'interazione; 3. forma del supporto fisico; 4. capacità di adeguare il suo comportamento e le sue azioni all'ambiente.*

La questione dell'attribuzione al *"robot intelligente"* di uno *"status di persona"*, ha anche generato un interessante dibattito, non sul tema in sé, che non ha registrato particolari e significativi interventi, ma su una questione che, indirettamente, mostra come la proposta di una disciplina in materia del *"robot persona"*, dotato di *"personalità elettronica"*, in sostanza non sia così fantascientifica come potrebbe apparire. Si tratta della qualificazione del *robot* come soggetto autonomo d'imposta, un soggetto con un suo reddito ed una sua cittadinanza, una sua coscienza e responsabilità, oggettive e soggettive, un contribuente[15]. Questo ha intuitive conseguenze non solo giuridiche e sociali, anche in un contesto internazionale, ma primariamente filosofiche e con possibili implicazioni persino di natura religiosa (il *"robot intelligente"* e consapevole di essere che si interroga sul perché e sul senso della sua esistenza e sul rapporto con il suo creatore-costruttore).

La materia non è, tuttavia, qui oggetto di approfondimento in relazione alle questioni esistenziali etiche e giuridiche conseguenti all'eventuale attribuzione ai *robot* di tale *status* giuridico.

In questa sede si desidera solo precisare e sottolineare che la *"persona elettronica"* di cui si parla non è la stessa di cui l'insigne giurista prof. Stefano Rodotà, presidente dell'Autorità della *privacy*, si occupò nel passato quando nel 2001, in relazione alla tutela della *privacy*, tenne un discorso sul tema di una necessaria tutela dell'identità elettronica della persona fisica[16] (quindi non del *robot* con lo *"status"* giuridico di *"persona vivente artificiale"*).

---

[12] Draft Report (31.5.2016) *with recommendations to the Commission on Civil Law Rules on Robotics* [2015/2103(INL)], Committee on Legal Affairs.

[13] Quindi con esclusione di qualsiasi proposta in materia penale.

[14] Documento di seduta n. A8-0005/2017, in http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//IT.

[15] L. TREMOLADA, *La strana idea di tassare i robot*, Il Sole24Ore, 21 febbraio 2017, C. BONOMI, *Tassare i robot è una scorciatoia senza sbocchi*, Il Sole24Ore, 23 marzo 2017, solo per citare alcune battute nel contesto del dibattito.
Nello scenario politico si veda una Proposta di legge, dell'On. Pastorelli ed altri (Camera dei Deputati, 3 agosto 2017, n. 4621) in tema di modifica della disciplina delle aliquote di *imposta sui redditi delle imprese realizzati mediante sistemi di intelligenza artificiale* ed un conseguente dibattito politico, attivo anche nel 2018 (REDAZIONE, Insieme è meglio, *Pastorelli: sui "Robot" Salvini è distratto, il progetto di legge c'è già*, 8 febbraio 2018), il tutto con la prevalenza di una certa confusione in materia di q*uantum* di imposta e soggettività del tributo.

[16] S. RODOTÀ, *Uno statuto giuridico globale della persona elettronica*, testo del discorso tenuto, sul tema *"Un mondo, una Privacy"*, l'11 ottobre 2001, alla sessione conclusiva della Conferenza internazionale sulla protezione dei dati, svoltasi a Parigi dal 24 al 26 settembre 2001, in http://www.interlex.it/675/rodota5.htm.

Noi ci occuperemo, invece, del *robot* intelligente inteso solo come macchina dotata di particolari caratteristiche.

6. La responsabilità del *"costruttore"* per difetti del *"prodotto"*

L'evoluzione tecnologica in atto sta determinando, come già in precedenza esposto, l'immissione sul mercato di *"prodotti"* sempre più sofisticati i cui effetti dannosi conseguenti al loro utilizzo si possono manifestare anche a lunga distanza nel tempo, con un'autentica difficoltà probatoria del danno sul fondamento del nesso di causalità.

In relazione alla responsabilità del *"costruttore"* del bene, cioè dell'impresa (industriale) che lo realizza e lo rende destinabile al mercato, si devono considerare varie condizioni, incluse quelle della natura e della compatibilità funzionale delle singole componenti (fisiche e non) del *"prodotto"* in relazione alla sua destinazione utile ed indicata dal *"produttore"*. Quando i *"prodotti"* sono tecnologicamente complessi, con l'impiego di componenti materiali (*hardware*) e immateriali (*software*), solo appropriate procedure di controllo e di collaudo prima dell'immissione del *"prodotto"* sul mercato e anche da parte dell'utilizzatore professionale, possono fornire un'adeguata attesa di assenza di difetti o di irrilevanza funzionale degli stessi.

La problematica ha trovato una sua prima disciplina in sede europea, non con specifico riferimento ai *robot*, innanzitutto con la Direttiva n. 85/374/CEE, in materia di responsabilità per danno da prodotti difettosi, recepita in Italia con il D.P.R. 24 maggio 1988, n. 224, e poi con la Direttiva n. 1999/34/CE, modificatrice della precedente e recepita con il D.Lgs. 2 febbraio 2001, n. 25.

Quando si tratta di sistemi robotici diversamente sofisticati nelle componenti informatiche che ne rendono utile l'impiego, le varie responsabilità e la loro *"attribuzione"* e *"distribuzione"* a soggetti diversi, in una sorta di *"catena"* o *"rete complessa"* di relazioni, risulta sempre più complessa, con il necessario ricorso a consulenze tecniche di particolare impegno e difficoltà.

In particolare ciò accade quando i *"prodotti"* da verificare in presenza di lamentati difetti e conseguenti danni, sono in grado di porsi in relazione autonoma con altri *"prodotti"*, e non di essere solo *"istruiti"* e *"formati"* dal *"produttore-costruttore"* (o da terzi per suo conto e su specifiche tecniche[17] assegnate), ma sono anche in grado di apprendere, anche da fonti non sempre verificabili con certezza, nell'ambito di un'*infosfera*[18] che, comunque, modifica costantemente e rapidamente il mondo della conoscenza e della comunicazione in modo ancora non adeguatamente conosciuto e regolato.

La relazione della Commissione Giuridica UE sottolinea, con riferimento a scenari pratico-applicativi diversi (mezzi di trasporto autonomi, veicoli autonomi, droni a pilotaggio remoto, *robot* impiegati per l'assistenza, *robot* medici per interventi riparativi e migliorativi del corpo umano, *robot* destinati all'educazione ed al lavoro), la sussistenza di impatti di natura sociale ed ambientale, cui conseguono o possono conseguire responsabilità per danni generati.

La responsabilità prefigurata è di natura oggettiva, fondata sulla prova del danno e sull'individuazione del nesso di causalità (par. 54), ma deve tener conto, come detto, del rapporto tra comportamento e livello di autonomia del *robot*.

Questa autonomia viene qualificata come *"la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna; […] tale autonomia è di natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente"* (Par. AA dei considerando).

Di rilievo appaiono le seguenti sottolineature della Commissione Giuridica UE:

1) (par. AB), *"più i robot sono autonomi, meno possono essere considerati come meri strumenti nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore, ecc.); […] ciò, a sua volta, pone il quesito se le regole ordinarie in materia di responsabilità siano sufficienti o se ciò renda necessari nuovi principi e regole volte a chiarire la responsabilità legale dei vari attori per azioni e omissioni imputabili ai robot, qualora le cause non possano essere ricondotte a un soggetto umano specifico, e se le azioni o le omissioni legate ai robot che hanno causato danni avrebbero potuto essere evitate"*;

2) (par. AD), *"nell'attuale quadro giuridico, i robot non possono essere considerati responsabili in proprio* (in quanto non *"ancora"* provvisti di uno *"status giuridico di persone elettroniche responsabili"*) *per atti o omissioni che causano danni a terzi; [...] le norme esistenti in materia di responsabilità coprono i casi in cui la causa di un'azione o di un'omissione del robot può essere fatta risalire ad uno specifico agente umano, ad esempio il fabbricante, l'operatore, il proprietario o l'utilizzatore, e laddove tale agente avrebbe potuto prevedere ed evitare il comportamento nocivo del robot; che, inoltre, i fabbricanti, gli operatori, i proprietari o gli utilizzatori potrebbero essere considerati oggettivamente responsabili per gli atti o le omissioni di un robot"*;

3) (par. AH), *"per quanto riguarda la responsabilità extracontrattuale, la Direttiva 85/374/CEE del Consiglio copre solamente i danni causati dai difetti di fabbricazione di un robot*

---

[17] Per *"specifica tecnica"* si intende la *"specificazione contenuta in un documento che definisce le caratteristiche richieste di un prodotto, quali i livelli di qualità o di proprietà di utilizzazione, la sicurezza, le dimensioni, comprese le prescrizioni applicabili a un prodotto per quanto concerne la terminologia, i simboli, le prove e i metodi di prova, l'imballaggio, la marchiatura e l'etichettatura, nonché le procedure di valutazione della conformità [omissis]"* (art.1.3 della Direttiva n. 98/34/CE, Direttiva del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, del 22 giugno 1998, come modificata dalla Direttiva n. 1998/48/CE del 20 luglio 1998).

[18] G. FONTANA, *In viaggio con il padre dell'infosfera* [L. FLORIDI, *Infosfera*, in *Internet & Net Economy*, V. DI BARI (a cura di), Il Sole 24-Ore Libri, 2002], Il Sole24Ore, 20 maggio 2010, ove: *"l'infosfera è la globalità dello spazio delle informazioni, perciò include sia il cyberspazio (Internet, telefonia digitale, ecc.), sia i mass media classici (biblioteche, archivi, emeroteche, ecc.)"*.

e a condizione che la persona danneggiata sia in grado di dimostrare il danno effettivo, il difetto nel prodotto e la connessione causale tra difetto e danno e che pertanto la responsabilità oggettiva o la responsabilità senza colpa potrebbero non essere sufficienti";

4) (par. AI), *"l'attuale quadro giuridico non [è] sufficiente a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile"*.

Appare evidente la *"scollatura"* tra disciplina giuridica e concreta applicazione delle tecnologie della robotica che utilizzano diversi livelli di sofisticazione dell'intelligenza artificiale.

Inoltre, dal quadro emerge come possa essere difficile individuare in modo chiaro e indiscutibile, in diversi casi (ragionevolmente sempre più numerosi), a quale soggetto debba imputarsi la responsabilità, ed il conseguente danno da risarcire, o come responsabilità e danni possano o debbano essere distribuiti tra soggetti diversi in modo economicamente ponderato secondo il concorso al danno di ogni partecipante alla costruzione di tale *"prodotto"* e dei soggetti preposti al controllo e collaudo del prodotto *"finito"*.

Ciò è anche più difficile anche per l'inadeguata formazione degli utilizzatori e degli stessi operatori che utilizzano questi tipi di *robot*.

La natura della *"macchina robot"*, che presuppone l'esistenza di un sistema integrato di parti meccaniche (*hardware*) e di componenti programmate (*software*) comporta l'esistenza di una pluralità di soggetti interessati al risarcimento del danno conseguente all'impiego di uno strumento molto complesso.

La responsabilità, oltre a quella dei compartecipi alla sua *"costruzione/produzione/fabbricazione"*, non è solo quella degli operatori, ma anche dell'*"utilizzatore"* o, meglio, come vedremo, di una diversa gamma di soggetti *"utilizzatori"*, che possono essere anche gli stessi *"operatori"*.

7. La responsabilità dell'*"utilizzatore"*

Come si è visto esistono più compartecipi alla qualificazione di *"costruttore del prodotto"* e quindi più compartecipi, con variegate intensità di concorso alla sua realizzazione finita e funzionale; altrettanto può dirsi per l'*"utilizzatore"*.

Il documento della Commissione giuridica dell'UE oggetto del nostro esame non chiarisce esattamente la natura dell'*"utilizzatore"*, che appare diversa da quella dell'*"operatore"*, lasciando intendere che ci sia una distinzione tra *"utilizzatori"* ed *"operatori"*, tra *"utilizzatori"*, *"operatori"* e *"proprietari"* e, ancora, tra *"utilizzatori"* del *"prodotto tecnologico"* ed *"utilizzatori finali della tecnologia"*, identificando questi negli *"ingegneri robotici"* (punto 10 dei Suggerimenti alla Commissione UE).

Appare, invero, che gli *"ingegneri robotici"*, utilizzatori della tecnologia, si debbano considerare come concorrenti responsabili al processo di progettazione e costruzione dei *robot intelligenti*.

Invece, realizzato il *"prodotto"* ritenuto privo di difetti, ancorché adeguatamente collaudato in relazione alla sua destinazione funzionale, appare che vi possa essere una responsabilità autonoma, da valutare in relazione alle singole circostanze comportamentali di uso del *"prodotto"*.

Il consumatore (inteso come *"qualsiasi persona fisica che, nei contratti oggetto della […] direttiva, agisca per fini che non rientrano nel quadro della sua attività commerciale, industriale, artigianale o professionale" ex* art. 2 della Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011, di modifica, sostituzione di precedenti direttive in materia, recepita con il D.Lgs. 21 febbraio 2014, n. 21) dovrebbe trovare la sua tutela attraverso possibili integrazioni della normativa di cui al Codice del Consumo (D.Lgs. 6 settembre 2005, n. 206 e succ. modd., che hanno recepito nella normativa nazionale le direttive comunitarie).

Negli altri casi si pongono questioni relative a:

1) la concessione in uso, dal proprietario all'utilizzatore, di prodotti consapevolmente difettosi o non funzionalmente adatti allo scopo cui verranno destinati dall'utilizzatore, di cui il proprietario sia consapevole della divergenza con le specifiche fornite dal costruttore-produttore;
2) l'utilizzo consapevole diverso da quello cui il prodotto doveva o poteva essere destinato (anche con riferimento a condizioni ambientali) secondo le indicazioni del proprietario;
3) l'utilizzo dell'operatore in modo difforme dalle istruzioni ricevute per negligenza, insufficiente preparazione nell'uso del prodotto, dolo, ecc., con eventuale chiamata in causa del soggetto e/o dell'ente preposto alla formazione e/o istruzione dell'operatore;
4) il comportamento dell'utilizzatore comunque non conforme alle specifiche tecniche, enunciate con chiarezza, del prodotto;
5) altre problematiche riferibili alle variabili circostanze di utilizzo.

In presenza di comportamenti *"autonomi"* del *"robot intelligente"*, dettati dalle istruzioni fornite e correlati vincoli imposti, ma modificati a causa delle interrelazioni con altri *robot* o per acquisizione di istruzioni e modifiche di vincoli imposti da interazioni con l'ambiente e con l'*infosfera* nell'ambito del sistema di autoapprendimento non guidato ed imprevedibile, la questione che si pone, in presenza di danno, è se questo sia, nelle circostanze, riconducibile a difetti che potevano essere diagnosticati anteriormente all'inizio dell'utilizzo, o periodicamente da parte del produttore-costruttore, in presenza di un sistema di costante autodiagnostica della macchina intelligente ed entro quali limiti di ragionevolezza dato che non tutti gli scenari sono prevedibili.

Da ciò consegue l'indirizzo (indicato nel codice etico-deontologico degli ingegneri robotici di cui alla Proposta di risoluzione qui in esame) di un approccio fondato su determinati precetti (tra i quali):

1) *"il funzionamento di un sistema robotico dovrebbe sempre basarsi su un rigoroso processo di valutazione dei rischi, che dovrebbe essere improntato ai principi di proporzionalità e di precauzione"*;
2) *"l'attuale ritmo dell'automazione e della digitalizzazione del lavoro e dei servizi rende imperativo migliorare le conoscenze e le competenze digitali, onde garantire un elevato livello di occupazione e combattere il crescente analfabetismo digitale"*;
3) *"ridurre il rischio di errore umano"*;
4) *"qualsiasi politica sulla robotica [*deve*] affrontare le questioni etiche e relative alla protezione dei dati, compresi i dati di terzi e i dati personali, nonché alla responsabilità civile, all'istruzione e alla formazione e alla sicurezza informatica"*.

Nella realtà attuale siamo in presenza di un sistema di produzione di beni e di modalità di impiego degli stessi connotati da mutamenti continui e non per distinti, separati scatti di evoluzione, cioè per passi temporalmente definiti.

La regolamentazione giuridica delle responsabilità per la tutela ed il risarcimento del danno da fatto illecito non può statuire condizioni di non punibilità dei comportamenti per difetto di disciplina. Il sistema normativo legale deve procedere in modo tempestivo e lungimirante.

Il legislatore deve operare in modo tale da considerare e prevedere i fattori di rischio connessi a queste nuove tecnologie e da identificare i soggetti da tutelare.

La tutela di cui si tratta deve essere prevista anche nei confronti dei lavoratori delle imprese ed enti che utilizzano detti *"strumenti"*, o che con gli stessi condividono attività ed ambienti e, in ogni caso, di tutti i soggetti che non rientrano delle categorie sopra indicate.

Il nuovo assetto normativo è urgente, è da considerare in un'ottica transfrontaliera (meglio, di relazioni globali). Secondo gli indirizzi della Commissione giuridica (e non solo), dovrebbe essere:

1) *"fondato su una valutazione approfondita della Commissione che stabilisca se applicare l'approccio della responsabilità oggettiva o della gestione dei rischi"*;
2) integrato *"da un regime assicurativo obbligatorio, che potrebbe basarsi sull'obbligo del produttore di stipulare una copertura assicurativa per i robot autonomi che produce"*.

Numerosi e di particolare interesse sono i pareri delle Commissioni Trasporti e Turismo, Libertà Civili, Giustizia e Affari Interni, Occupazione e Affari Sociali, Ambiente, Sanità Pubblica e Sicurezza Alimentare, Industria, Ricerca ed Energia, Mercato Interno e Protezione dei Consumatori, allegati alla Proposta di risoluzione esaminata. Da essi, in parte, si è tratto spunto nella presente esposizione.

8. Conclusioni

Dalla Commissione giuridica dell'Unione europea ed in particolare dalle conclusioni del *"gruppo di lavoro per le questioni legali relative allo sviluppo della robotica e dell'intelligenza artificiale"* emerge un quadro *"preoccupato"* in termini di evoluzione senza adeguato controllo.

La Commissione europea formula l'auspicio di applicazione di principi e regole di natura etica, della promozione della formazione allo scopo di comprimere gli effetti del *gap* da analfabetismo informatico, di un sistema di individuazione di soggetti responsabili, di cautele di progettazione.

La Commissione si pone, poi, interrogativi sull'autonomia decisionale dei *robot* intelligenti, macchine che possono apprendere, comunicare, interrelarsi tra loro, modificarsi al punto tale da prefigurare la possibilità di imporre uno *status giuridico di persona* al frutto, il risultato della creazione elettronica.

Tutto questo porta a dover predisporre tempestivamente strumenti giuridici atti a stabilire un sistema di responsabilità civili, per il momento attribuibili a persone fisiche e non ai *robot personificati* con l'attribuzione di uno speciale ed innaturale *status di persona*.

Si è in presenza di un campo assolutamente nuovo che non può essere ignorato, e di un attuale sistema di individuazione delle responsabilità civili in materia, che, allo stato, appare assolutamente inadeguato.

This page is left intentionally blank

Pontani e Associati S.p.A.
Cap. Soc. 120.000 (centoventimila) int. vers. - REA Milano 1047300 - R.I./C.F./P.I. 04847510155
Sede Legale, Direzione e Amministrazione: 20121 Milano - Piazza Castello n. 5 - Tel. 02-36682148
Fax 02-36687506 * Direttore Responsabile: Dott. Franco Pontani
Registered by the Cancelleria del Tribunale di Milano n. 5 del 9 gennaio 2015
E-mail: info@pontanieassociati.com