Rivista elettronica di Diritto, Economia, Management

Numero 3 - 2022 - Supplemento 1

Intelligenza artificiale e Nuove Forme di Discriminazione

atti del Convegno a cura di Maria Novella Campagnoli e Massimo Farina

Inquadra il QR-CODE per il download degli altri numeri della Rivista

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOEDU®

ISSN 2039-4926

N. 3 - 2022 - Supplemento 1 · pp. 13-24

I.A. principi e tutele in materia di privacy

Gianluigi Ciacci[1]

Abstract [IT]: Lo sviluppo repentino ed esponenziale dei sistemi di Intelligenza Artificiale, e della correlata attenzione "diffusa" per la stessa, conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi), ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze: non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso; impedire che tale progresso avvenga in danno dei suoi utenti. Dicotomia che raggiunge una forte criticità, da una parte, nel momento in cui dal suo sviluppo dipendono enormi interessi economici e, dall'altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 2016/679, finalizzata proprio a prevenire, o comunque limitare, tale danno. La pregnante disciplina in materia di protezione dei dati personali, infatti, prevede una serie di principi e disposizioni di difficile, se non impossibile, applicazione ai sistemi di Intelligenza Artificiale: si pensi, ad esempio, alla necessità di rispettare la minimizzazione e trasparenza nel trattamento dei dati personali (art. 5, par. 1, del Regolamento), rispetto ad una realtà tecnologica che in generale ha la necessità di essere alimentata da ingenti quantità di informazioni (i c.d. *big data*) per ottenere migliori risultati, e le cui modalità di funzionamento, nonché gli stessi risultati dei processi elaborativi basati sull'I.A., sono, e spesso devono essere, "oscuri". Per risolvere l'indicata dicotomia la scelta non riguarda solo il tema contingente, ma quello più ampio relativo al rispetto o meno della legalità anche nel mondo digitale.

Abstract [EN]: The sudden and exponential development of Artificial Intelligence systems, and the related "widespread" attention for the same, also a consequence of the multiplication of its applications in the everyday life of users (think, for example, of virtual assistants in cell phones or in home devices), has given rise to a debate on the need to strike a balance between two opposing needs: not to slow down, or even block, the progress of the sector, and thus the positive consequences of the same; to prevent that this progress occurs to the detriment of its users. A dichotomy that reaches a strong criticality, on the one hand, when enormous economic interests depend on its development and, on the other hand, when the harm to users concerns their personal data: in the latter case mainly due to the presence of strong

[1] Docente presso l'Università LUISS Guido Carli.

legislation, represented by EU Regulation 2016/679, aimed precisely at preventing, or at least limiting, such harm. The pregnant data protection regulations, in fact, provide for a series of principles and provisions that are difficult, if not impossible, to apply to Artificial Intelligence systems: one thinks, for example, of the need to respect minimization and transparency in the processing of personal data (Art. 5(1) of the Regulation), with respect to a technological reality that in general needs to be fed by huge amounts of information (so-called big data) in order to achieve better results, and whose modes of operation, as well as the very results of the processing processes based on A.I, are, and often must be, "obscure." In order to resolve the indicated dichotomy, the choice is not only about the contingent issue, but the broader one related to whether or not legality is also respected in the digital world.

Keywords [IT]: privacy – big data – intelligenza artificiale – legalità – cultura.

Keywords [EN]: privacy - big data - artificial intelligence - legality - culture.

1. Introduzione

Nell'evoluzione degli studi sull'Informatica Giuridica di frequente l'attenzione degli esperti della materia è stata catalizzata dall'avvento di fenomeni tecnologici che hanno sollevato rilevanti, e interessanti, problemi giuridici: dalla nascita dei contratti informatici negli anni ottanta, alla tutela dei programmi per elaboratore ed al valore giuridico del documento elettronico/firma digitale degli anni Novanta; successivamente l'avvento della rete Internet, dei social network, e poi la tecnologia blockchain, la moneta elettronica, gli smart contracts, ed infine proprio l'Intelligenza Artificiale.

Quest'ultima, non potendomi dilungare nel riportare le varie definizioni, e nel dettagliare i suoi contenuti (che verranno sicuramente trattati dagli altri relatori), certamente è un fenomeno di rilevante, e crescente, interesse, in repentino sviluppo e con importanti, e complesse, implicazioni giuridiche: che quindi, nell'attirare l'attenzione degli studiosi di informatica giuridica, e non solo (l'attualità del tema infatti coinvolge sempre più anche la dottrina "tradizionale": aspetto molto utile nell'ottica della oramai improrogabile necessità di aumentare la diffusione della cultura sulle nuove tecnologie anche nel mondo del diritto), la sta portando ad essere anche di grande … "moda".

A parte però gli elementi positivi del "successo" dell'Intelligenza Artificiale, si deve rilevare un rischio in tale situazione ? Probabilmente sì, quello rappresentato dalla concreta possibilità di distrarsi con aspetti secondari del fenomeno (si pensi ad

esempio al tema della guida autonoma, e della connessa responsabilità: sicuramente molto interessante e importante, ma per lungo tempo è sembrato rappresentare il solo, o comunque principale, problema giuridico da approfondire e risolvere). Un "successo" che spesso "condiziona" anche chi se ne occupa professionalmente e/o a livello istituzionale: si possono fare a tale proposito due esempi.
Con riferimento al primo, riporto un passaggio di una interessante monografia pubblicata un paio di anni fa, che abbiamo presentato in LUISS il 27 ottobre 2020 (A. Longo – G. Scorza, *L'impatto sulle nostre vite, diritti e libertà*, Mondadori Università, 2021, pp. XII-244). Gli autori, nel descrivere ed introdurre il tema dell'intelligenza artificiale, riportano l'evoluzione storica del suo sviluppo, con l'indicazione delle principali date che hanno caratterizzato i passaggi più rilevanti di tale evoluzione; l'aspetto curioso è rappresentato dall'idea di associare agli episodi "reali" quelli collegati a produzioni letterarie o cinematografiche realizzate più o meno negli stessi periodi: quasi a dimostrare la stretta correlazione, in questo settore, tra realtà tecnologica e divulgazione. Nella tabella che segue riporto alcuni esempi tratti dal volume (pp. 9-31):

1939 Atanasoff-Berry Computer (ABC)	1942 Asimov, le 3 leggi della robotica
1950 test di Turing	
1959 machine learning	
1966 Shakey the Robot	1968 "2001 Odissea nello spazio"
1970 WABOT 1	1977 "Star Wars"
1995 chatbot Alice	1984 "Electric Dreams"
1997 Deep Blue	2001 "AI - Artificial Intelligence"
2000 ASIMO	2004 "Io, robot"
2011 Watson	2013 "Her (Lei)"

Ma la commistione che sto cercando di evidenziare, non ultimo allo scopo di sottolineare la necessità di non farsi distrarre dagli aspetti "di moda" dell'importante tema, più divulgativi che scientifici, non si limita ad interventi non istituzionali o della dottrina (non solo accademica, ma anche nella stampa d'opinione). Il secondo esempio riguarda infatti una fonte ufficiale, la "*Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*", che nel punto A dell'introduzione riporta
"A. *considerando che, dal mostro di Frankenstein ideato da Mary Shelley al mito classico di Pigmalione, passando per la storia del Golem di Praga e il robot di Karel C apek, che ha coniato la parola, gli esseri umani hanno fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane*".
Testo che permette di capire come il rischio della prevalenza dell'Intelligenza Artificiale "divulgativa" (mostri, Golem, robot, ...) possa portare a trascurare la necessità

di un serio approfondimento giuridico delle varie ed ulteriori (rispetto alla responsabilità da guida autonoma) problematiche.
Volendo però vedere il "bicchiere mezzo pieno", non si deve ignorare, a causa del rischio evidenziato, l'opportunità creata dal forte interesse per questa realtà, rappresentata dalla nuova domanda di conoscenza legata alla necessità di comprendere l'I.A.: che porta al moltiplicarsi di eventi, di pubblicazioni non solo divulgative, ma anche tecniche, e con riferimento anche ai diversi campi applicativi (prospettiva degli ultimi mesi, che sempre più hanno portato ad un approfondimento più "maturo" dei problemi giuridici dell'intelligenza artificiale). Domanda di conoscenza che assume una grande importanza, soprattutto nel nostro Paese, dove la carenza di competenze nelle nuove tecnologie ha sempre rappresentato uno dei suoi grandi problemi, ancor di più se si pensa alla mancata percezione della necessità di un approccio culturale alle stesse. Carenza oggi sempre più grave.
Così, lo sviluppo di un'attenzione "diffusa" per l'I.A., conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi), oltre a portarla al di fuori della discussione tra esperti, ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze:

– non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso (e poi sì, anche l'enorme business da essa resa possibile direttamente, per il valore in sé dell'I.A., e indirettamente, per la ricchezza prodotta dalle sue applicazioni);
– impedire che tale progresso avvenga in danno dei suoi utenti.

Dicotomia che raggiunge una forte criticità, da una parte, nel momento in cui dal suo sviluppo dipendono enormi interessi economici ("alzando la posta in gioco"), e, dall'altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 2016/679, finalizzata proprio a prevenire, o comunque limitare, tale danno.
Prima di affrontare il fondamento dell'indicata dicotomia, e di provare a cercare le possibili soluzioni, occorre in premessa analizzare una realtà strettamente legata a quella dell'intelligenza artificiale, il fenomeno dei c.d. "*big data*".

2. I c.d. Big Data e l'Intelligenza Artificiale

Quando ci si occupa delle nuove tecnologie, e non solo, è oramai costante il richiamo alla c.d. "società dell'informazione", e all'importanza fondamentale acquisita dai dati ("il nuovo petrolio").
L'informazione è infatti diventata il motore dell'economia, e l'evoluzione negli anni delle tecnologie dell'informazione e della comunicazione ha portato ad una sua trasformazione in "informazione automatica", e quindi "informatica".

L'ulteriore evoluzione degli ultimi anni ha portato un cambiamento nelle modalità di creazione, acquisizione, gestione, comunicazione, ..., delle informazioni. La tecnologia ha infatti modificato il Volume, la Velocità, la Varietà, (la Veridicità), il Valore economico dei dati (le famose "V") e la possibilità di loro utilizzo, analisi e sviluppo, in una realtà di autoalimentazione che genera quotidianamente miliardi di informazioni. Realizzando la realtà dei c.d. "Big Data" che vengono definiti (punto A dei considerando della "*Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto*") come le "*ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare*".
Non potendo approfondire in queste poche pagine la realtà dei Big Data, ci basti richiamare il fatto che essi si pongono in stretta correlazione con l'Intelligenza Artificiale: da un lato, ne "alimentano" l'apprendimento (ad esempio nei sistemi di *machine learning*), mentre dall'altro rappresentano il risultato dell'applicazione dei relativi algoritmi.
Se questo è il contesto, se i dati hanno assunto questa importanza, allora è diventato fondamentale proteggere il loro valore, insieme alla necessità sempre più sentita di sviluppare l'Intelligenza Artificiale. Ma se poi i dati di cui si parla sono … "personali", cioè sono riferiti (o riferibili, anche indirettamente) ad individui, non basta più proteggere il loro *valore*, e allo stesso tempo non si può pensare solo a diffondere l'utilizzo dell'I.A., sostenendo il relativo settore economico; diventa invece prioritariamente necessario tutelare *i soggetti* a cui si riferiscono i dati oggetto di questa nuova tecnologia, la loro dignità e libertà individuale. Necessità di tutela per raggiungere la quale è nata la normativa europea a protezione dei dati personali, rappresentata da ultimo (dopo la Direttiva 95/45/CEE degli anni Novanta) proprio dal Regolamento UE 2016/679.

3. Big Data, Intelligenza Artificiale e protezione dei dati personali

Nell'affrontare il tema della "privacy", più correttamente della protezione dei dati personali, soprattutto con riferimento al nostro Paese, si entra in contatto con un'anomalia "paradigmatica": principalmente creata dall'idea generalizzata che vede la relativa disciplina come assolutamente inutile, burocratica, anzi, addirittura dannosa per chi vuole oggi fare impresa ("se c'è la privacy non si può fare niente"), qualcosa da cui difendersi. Conseguenza di tale anomalia è stata la forte carenza negli anni di una generalizzata "cultura" della protezione dei dati personali, la disattenzione

politica al problema, lo scarso livello di adeguamento alla legge delle strutture dei vari titolari, privati ed anche pubblici.
Come detto, la situazione è migliorata con l'avvento nel maggio del 2018 del Regolamento 2016/679, il c.d. G.D.P.R.: di cui tutti parlano, molti si attivano per poterlo rispettare, ma alla fine non così tanti riescono ad approfondirne i diversi aspetti per arrivare a conoscerlo.
Ad ogni modo, l'ingente importo delle sanzioni, l'introduzione di un sistema basato sulla responsabilizzazione del titolare (c.d. *accountability*), una serie di scelte... "strategiche" nella costruzione della disciplina normativa (ad esempio, l'introduzione della figura e del ruolo del Responsabile per la Protezione dei Dati Personali, comunemente DPO, dell'obbligo di tenuta di un Registro dei trattamenti come momento di "autoconsapevolezza" del titolare, l'obbligo di denuncia dei c.d. *data breach*, l'introduzione del principio di *accountability* alla base del nuovo approccio sistematico della disciplina,...), hanno trasformato il fallimento del sistema di tutela degli anni '90, avente fonte nella Direttiva 95/45/CEE, in un successo. Questo principalmente per la natura "sostanzialista" Regolamento UE 2016/679, il cui sistema di tutela non si risolve solo nel rispetto formale degli obblighi, come in quello precedente, ma nella costruzione di un'effettiva, ed efficace, protezione delle informazioni personali degli individui: si è passati cioè da una logica "di adempimento" (il mero rispetto di obblighi precostituiti ed uguali per tutti, semplicemente rispettati dai titolari del trattamento, senza curarsi del risultato dell'adeguamento al loro disposto) a quella di sistema (dove prevale l'efficacia del sistema, basato come detto sulla responsabilizzazione, sull'*accountability* dei titolari).
Ancora, il cambiamento ha riguardato proprio l'oggetto della disciplina, la sua finalità: in particolare

- prima (Direttiva 95/46/CE) si voleva assicurare la protezione dei dati personali e la loro libera circolazione;
- ora il Regolamento 2016/679 inquadra invece la protezione dei dati personali quale diritto fondamentale e inviolabile della persona, ritiene prioritario rafforzare la fiducia degli interessati sulla tutela forte delle informazioni, stabilendo un quadro normativo adeguato allo sviluppo dell'economica digitale.

Cambiamento di impostazione che riporta centrale proprio l'importanza della tutela delle informazioni relative agli individui, come già previsto in due fonti di primaria importanza per l'Europa: fonti costantemente richiamate nell'affrontare il tema della protezione dei dati personali, ma che poi devono effettivamente essere tenute presenti nell'analizzare, valutare e disciplinare le attività sulle informazioni relative agli individui, e quindi anche i nuovi fenomeni tecnologici.
La prima è la Carta dei diritti fondamentali della UE, il cui art. 7 (intitolato "*Rispetto della vita privata e della vita familiare*"), testualmente dispone

- "*ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*"

mentre l'art. 8 (intitolato proprio "*Protezione dei dati di carattere personale*"), sancisce

– "1. *ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*; 2. *tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*; 3. *il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*"

La seconda fonte è il Trattato sul funzionamento della UE, il cui art. 16 prevede al par. 1 che

– "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*",

e al par. 2

– "*Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti*".

4. Gli aspetti della disciplina in materia di protezione dei dati personali di rilievo per le attività di trattamento collegate all'I.A.

Ma tornando al Regolamento 2016/679, ricordiamo velocemente il suo oggetto ("… *protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*", art. 1, par. 2), e procediamo a schematizzare alcuni suoi aspetti che hanno un diretto rilievo per la tutela dei dati personali coinvolti in processi di Intelligenza Artificiale. In particolare, occorre ricordare:

– l'ambito di applicazione territoriale del Regolamento, che aggiunge alla regola generale dello stabilimento (art. 3, par. 1: la normativa sulla protezione dei dati si applica a chi è stabilito nello Spazio Economico Europeo), quella innovativa del c.d. "target" (art. 3, par. 2: ovunque sia stabilito il titolare del trattamento, se utilizza dati di interessati che si trovano nell'Unione, in presenza di due condizioni previste dalla norma, dovrà applicare il Regolamento), che estende la sua applicabilità anche a sistemi di I.A. non utilizzati in Europa, o comunque riconducibili a titolari extra europei;
– i principi generali del trattamento, e nella specie quelli di liceità/correttezza/trasparenza (art. 5 par. 1, lett. *a*), limitazione della finalità (par. 1, lett. *b*), minimizzazione (par. 1, lett. *c*), limitazione conservazione (par. 1, lett. *e*); e poi, in generale, quello di *accountability* (art. 5, par. 2) e quelli dell'art. 25 (*protection data by*

design e *by default*);
- l'individuazione delle c.d. basi giuridiche del trattamento, necessaria per "giustificare" l'utilizzo dei dati personali, in applicazione degli artt. 6 (per i dati personali "comuni") e 9 (per i dati personali "particolari");
- infine, tra gli obblighi che il titolare del trattamento deve osservare quando utilizza sistemi di Intelligenza Artificiale, a maggior ragione se operanti con "*big data*", ricordiamo, oltre a quello del punto precedente, quello di informativa (artt. 13 e 14 del Regolamento) e quello di rendere possibile, effettivo ed agevole, l'esercizio dei diritti riconosciuti all'interessato, cioè del soggetto a cui i dati trattati si riferiscono.

A parte gli indicati elementi della disciplina del Regolamento UE 2016/679 da tenere presenti nell'analisi delle criticità sollevate dall'applicazione della stessa all'Intelligenza Artificiale, occorre poi riportare quanto viene disposto dall'art. 22 di tale fonte, intitolato "*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*": l'unica norma del Regolamento che si riferisce direttamente ad una possibile applicazione dell'intelligenza artificiale, ma, più in generale, al momento una delle prime disposizioni sul tema *tout court*.

Il suo titolo individua il settore dell'I.A. di interesse, quello cioè che riguarda le decisioni prese da sistemi algoritmici con riferimento ad un individuo: ad esempio, per la selezione dei *curricula* al fine dell'individuazione di risorse lavorative da assumere in un'azienda, o in applicazioni più specifiche, come per la decisione sulla libertà vigilata dei detenuti raggiunta attraverso l'intervento del sistema di intelligenza artificiale Compas utilizzato dalla Corte di La Crosse in Wisconsin USA. In particolare il disposto del suo primo paragrafo prevede:

"*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".

Quindi, proprio a tutela dei diritti e delle libertà fondamentali, della dignità delle persone fisiche, si prevede la possibilità per l'interessato di rifiutare l'applicazione esclusiva di un sistema automatizzato nelle determinazioni che lo riguardano. Disposizione che ha poi alcune eccezioni nel paragrafo 2 della norma, nella specie quando la decisione
- sia necessaria per la conclusione o l'esecuzione di un contratto
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento,
- si basi sul consenso esplicito dell'interessato.

Eccezioni che, per la loro estensione (si pensi al problema dell'effettiva efficacia del consenso, in generale e nel caso concreto), sembrano svuotare di qualsiasi utilità l'art. 22 del Regolamento, ma che comunque sono equilibrate dall'applicazione di un'ulteriore regola generale a garanzia della persona coinvolta (il suo par. 3):

"*il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano*

da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione",
e che comunque hanno a loro volta un'eccezione, stabilita dall'ultimo paragrafo dell'art. 22 (che le esclude in ogni caso in cui si tratti di "categorie particolari di dati personali"). Ma, a parte la disciplina dei processi decisionali automatizzati appena indicata, le disposizioni con cui il Regolamento 2016/679 ha strutturato la protezione dei dati personali sono applicabili alle attività di trattamento di tali dati svolte attraverso sistemi di I.A.?

5. Big Data, Intelligenza Artificiale e protezione dei dati personali: problemi e possibili soluzioni

La risposta al quesito è sicuramente affermativa, anche se poi altrettanto sicuramente si deve rilevare che le caratteristiche del "sistema GDPR" sollevano, come detto, diversi problemi per la sua effettiva operabilità rispetto alla realtà dell'I.A. e dei *big data*.
Premesso che il Regolamento UE 2016/679 deve essere osservato da qualunque titolare che utilizzi le informazioni personali di interessati che si trovano nell'Unione, "*con o senza l'ausilio di sistemi automatizzati*" (e quindi anche nella realtà tecnologica in esame), vediamo quali difficoltà si incontrano nell'applicare gli aspetti della disciplina normativa richiamati nel precedente paragrafo. Schematicamente,

- per quanto riguarda il rispetto dei principali generali del trattamento, le criticità maggiori si realizzano per quello di "*trasparenza*" (il trattamento deve avvenire in maniera chiara per l'interessato, principio da cui deriva l'obbligo di informativa, su cui si veda oltre), a causa della necessità di segretezza per consentire una prima tutela degli algoritmi di intelligenza artificiale, a fronte delle difficoltà per realizzare una loro effettiva protezione giuridica quale proprietà intellettuale; ma anche per quelli di "*minimizzazione*" e di "*finalità*" (secondo i quali si devono utilizzare solo i dati personali strettamente necessari per il raggiungimento dello scopo del trattamento, che non possono poi essere impiegati per scopi diversi), di impossibile applicazione se il sistema di I.A., in particolare di quelli basati sul *machine learning*, necessiti del maggior numero di dati possibile per poter funzionare, con sviluppi spesso imprevedibili; ed infine per quello di "*limitazione della conservazione*", anche in questo caso diametralmente opposto all'esigenza dei *big data*, come detto numerosissimi e comunque "per sempre".
- con riferimento all'individuazione della corretta base giuridica del trattamento, in linea di massima consensuale, la difficoltà deriverebbe dalla possibilità concreta di rispettare il disposto normativo, non ultimo a livello di organizzazione pratica dell'adempimento: quella necessaria per raccogliere il consenso degli interessati coinvolti nel processo di intelligenza artificiale, di cui non si ha alcuna conoscen-

za, e poi per gestirlo nel tempo (si pensi alle eventuali richieste di revoca, da rendere effettive andando a cancellare i relativi dati personali nell'insieme complessivo delle diverse banche dati).
– strettamente connessi a quanto appena detto sarebbero infine il tema dell'adempimento dell'obbligo di informativa e quello di organizzazione dell'effettiva possibilità di esercizio dei diritti da parte dell'interessato: temi che non posso affrontare in questa breve relazione, ma le cui difficoltà sono intuibili.

Come evidenziato da diversa dottrina, ulteriori problematiche sono legate alla tipologia di trattamento dati posti in essere in tali realtà. Quella ad esempio causata dal fatto che in genere le informazioni risalgono a una lunga catena di acquisizioni, e solo alla fine vengono aggregate ed esaminate/utilizzate da titolari che possono non coincidere con coloro che li hanno raccolti; ancora, il fatto che spesso l'intervento di sistemi di I.A. sulla massa di dati portano a creare nuove informazioni impreviste, e imprevedibili, all'inizio della raccolta: realizzando ad un'indeterminatezza soggettiva che non si concilia con la stessa impostazione del Regolamento UE 2016/679. E, tra l'altro, i titolari di questi sistemi sono in genere le aziende "over the top" di difficile "gestione" per portarle al rispetto della normativa europea.

Come risolvere questi problemi? Rinunciare alla possibilità di proteggere i dati personali coinvolti in sistemi di intelligenza artificiale? Abdicazione che però porterebbe, alla luce dell'evoluzione tecnologica, ad eliminare del tutto la tutela di un diritto fondamentale dell'individuo, quello alla protezione dei suoi dati personali?

Prima di tentare di ipotizzare alcune soluzioni al problema, occorrerebbe procedere ad un'attenta analisi sul se e sul come viene oggi richiamata la disciplina sulla protezione dei dati personali nelle diverse fonti in materia di intelligenza artificiale. Si scoprirebbe infatti che quasi tutte prevedono indicazioni ben precise sul tema: ribadendo e sottolineando l'importanza del rispetto dei diritti fondamentali dell'individuo, in particolare quello alla protezione dei suoi dati personali.

Non potendo approfondire in queste brevi note l'esame delle varie fonti, mi limiterò a prendere come esempio la "*Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale*": numerose sono in essa le norme sul punto, ad iniziare dal paragrafo 4.2 intitolato "Dati personali e riservatezza", ed in particolare il suo art. 126 in cui si "*ribadisce che il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, quali sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali e dall'articolo 16 del trattato sul funzionamento dell'Unione europea si applicano a tutti i settori della robotica e dell'intelligenza artificiale e che il quadro giuridico dell'Unione per la protezione dei dati deve essere pienamente rispettato*", e si "*evidenzia che i progettisti di sistemi robotici e intelligenza artificiale sono responsabili di sviluppare prodotti che siano sicuri e adeguati agli scopi previsti e di applicare le procedure per il trattamento dei dati rispettando la legislazione esistente e garantendo la riservatezza*".

Ma si può fare riferimento anche all'art. 140, norma che introduce un altro tema, quello della cooperazione tra Commissione, Stati membri e mondo accademico, allo

scopo di
"*rafforzare la condivisione delle conoscenze e promuovere l'istruzione e la formazione*
- *per i progettisti, relativamente alle implicazioni etiche, alla sicurezza e al rispetto dei diritti fondamentali, e*
- *per i consumatori, per quanto riguarda l'utilizzo della robotica e dell'intelligenza artificiale, con una particolare enfasi sulla sicurezza e la riservatezza dei dati*".

Cooperazione di cui il presente convegno rappresenta a pieno titolo un primo esempio applicativo.

La lettura della fonte appena riportata può far raggiungere un primo punto fermo: a fronte di un apparato normativo che si sta costruendo per regolamentare usi e sviluppi dell'I.A., che prende in grande considerazione la protezione dei dati personali, il contrasto sembrerebbe porsi non tanto e non solo nella dicotomia "applico/non applico", ma anche nella più ampia scelta "rispetto/non rispetto" la legge. E allora, anche da questo punto di vista, non si può certo ritenere ammissibile la rinuncia a tale protezione, la rinuncia alla legalità.

Proviamo allora ad immaginare le possibili soluzioni, che indichiamo in tre differenti ambiti:

- dal punto di vista dei "player" del settore, cioè da un lato i fornitori di sistemi di Intelligenza Artificiale, dall'altro gli utilizzatori di tali sistemi (comunque tutti "titolari del trattamento" se vengono applicati ad informazioni relative agli individui, direttamente o indirettamente identificabili), ad adeguarsi correttamente al sistema della protezione dei dati personali introdotto dal Regolamento UE 2016/679;
- sviluppare il più possibile una tutela "dal basso", cioè posta in essere dagli stessi interessati, che a loro volta sono utenti delle nuove tecnologie, e in maniera più o meno consapevole cedono i loro dati ai player citati: tutela che deve partire da una corretta formazione e informazione degli interessati (non quindi non possono più essere solo "tecno-entusiasti", ma anche "tecno-consapevoli"), in generale sulla realtà digitale in cui vivono, ma in particolare sulla realtà del trattamento dei dati personali e sulla loro tutela;
- potenziare il più possibile la tutela "dall'alto", quindi a livello normativo (non solo affermazioni generali di principio, ma regole più dettagliate e certe) ma in particolare potenziando l'Autorità Garante (che deve portare all'adeguamento al Regolamento anche i più importanti player, punto 1, e consapevoli il maggior numero possibile di interessati, punto 2), nella possibilità concreta di operare.

Utopia?

Sicuramente le soluzioni proposte sono ambiziose, e allo stesso tempo, riguardando la … "privacy" (e tutte le difficoltà correlate di cui si è detto), di difficile realizzazione, e comunque non in tempi brevi.

Ma occorre capire che non si può non decidere, soprattutto a fronte della repentina evoluzione di sistemi I.A. sempre più potenti ed invasivi della nostra sfera privata, accorciando il più possibile i tempi per giungere alla soluzione del contrasto tra

sviluppo dell'intelligenza artificiale e protezione dei dati: avendo ben chiaro che la scelta in realtà si pone su un livello più ampio, in particolare tra la limitazione, o addirittura la rinuncia a un diritto fondamentale, per l'importanza (economica) del settore, ed invece un salto "culturale" che deve portare al successo al 100% del sistema di protezione dei dati personali, anche rispetto alle innovative (e di moda) applicazioni di intelligenza artificiale.