La borsa di dottorato è stata cofinanziata con risorse del
Programma Operativo Nazionale Ricerca e Innovazione 2014-2020 (CCI 2014IT16M2OP005),
Fondo Sociale Europeo, Azione I.1 "Dottorati Innovativi con caratterizzazione Industriale"

UNIONE EUROPEA
Fondo Sociale Europeo

Ministero dell'Università e della Ricerca

PON RICERCA E INNOVAZIONE

A Methodology of Total Audience Management Compliant with GDPR

Inviato a parziale adempimento degli obblighi previsti per il conseguimento del titolo in
Dottore in Filosofia

Tutor

Ch.mo Prof. Roberto Tagliaferri

Dottorando

dott. Amleto Soldani

Scuola di Big Data Management

Coordinatore

Ch.mo Prof. Valerio Antonelli

Febbraio, 2022

INDICE

Introduzione

Nel corso degli ultimi anni, con l'implementazione delle tecnologie di intelligenza artificiale e lo sviluppo delle capacità di elaborazione dei dati, si è assistito ad un incremento costante dell'analisi dei dati disponibili e, quindi, della loro ricerca e aggregazione. Avere più dati vuol dire non solo disporre di una maggiore quantità di informazioni, ma, e sempre di più, avere la possibilità di implementare nuove tecnologie in grado di leggerli, correlarli e, tramite meccanismi inferenziali sempre più sofisticati, dedurre nuove informazioni, diverse da quelle di partenza. Questo meccanismo sembra non avere limiti, pertanto le aziende di ogni settore (in modo specifico quello commerciale e quelle, in generale, che offrono servizi nel mercato B2C) si sono impegnate per avere la possibilità di raccogliere ogni tipo di dato, memorizzarlo e analizzarlo nei modi più diversi. Ciò ha avuto conseguenze di vario tipo: alcune sono passate quasi in secondo piano, come l'implementazione di sistemi di preferenza abbastanza sofisticati da suggerire all'utente contenuti e/o prodotti sulla base delle proprie preferenze, facendogli risparmiare tempo prezioso e consentendogli anche di conoscere prodotti prima sconosciuti, altre invece sono state notate e sono divenute fonte di preoccupazione, come le decisioni automatizzate che hanno portato al rifiuto alla stipula di un contratto di lavoro o di assicurazione o di concessione di nuovo credito. È diventato quindi evidente come i processi decisionali automatizzati potessero essere strumenti tanto potenti quanto pericolosi: consentono alle imprese grandi risparmi di tempo e di costi, come anche l'offerta di prodotti prima impensabili o troppo complessi per essere offerti (si pensi a contratti di credito che valutano la solvibilità del richiedente in pochi secondi, sulla base di informazioni estratte automaticamente da molteplici database, pertanto oggettive), ma al contempo richiedono una quantità di informazioni spesso di carattere personale, come le preferenze di spesa, e talvolta sensibile, come il reddito, senza che la persona debba obbligatoriamente esserne informata. Sulla base di questi aspetti il legislatore europeo si è attivato prima e meglio di qualsiasi

altro legislatore mondiale: è riuscito ad analizzare ciò che stava accadendo, a trovare abbastanza velocemente i punti di incontro necessari fra i vari membri dell'Unione e a scrivere e promulgare una norma ritenuta una pietra miliare della *privacy* delle persone fisiche.

Il regolamento UE 2016/679, anche conosciuto come *General Data Protection Regulation*, va ben oltre la necessità di stabilire una regolamentazione dei processi decisionali automatizzati – pur essendo, in tal senso, una norma dal carattere dirompente – arrivando a definire l'intero perimetro della *privacy* di un cittadino UE, di come questa possa essere definita e trattata, su quali soggetti sono imposti i vincoli previsti dalla norma e quali soggetti devono vigilare su questi affinché le norme siano rispettate effettivamente. Nel presente elaborato si provvede a definire un inquadramento di entrambe le discipline, sia dal punto di vista giuridico, per quel che concerne la norma in parola, sia informatico, per quanto concerne le tecnologie prevalentemente utilizzate nell'ambito dell'intelligenza artificiale, nella costante applicazione di un approccio multidisciplinare che tenda ad avvicinare i due mondi e a evidenziare le sfide davanti alle quali questi si trovano. Si provvede, poi, all'esame di alcune applicazioni pratiche delle tecnologie delineate nel mondo economico-aziendale. L'elaborato si conclude con la disamina di una fattispecie concreta analizzata durante il corso di dottorato presso l'azienda partner "Tuko production s.r.l."; questa, nel valutare lo sviluppo di un *software* basato su intelligenza artificiale, si è posta alcune *quaestiones juris* circa la compatibilità del primo con la normativa vigente, in particolar modo con riguardo alla protezione della *privacy*. L'elaborato, sulla base dell'inquadramento delineato, fornisce l'inquadramento giuridico e chiarisce i punti sulla base dei quali è possibile sviluppare il *software* pensato dall'azienda.

Capitolo I

GDPR e Intelligenza Artificiale

SOMMARIO: Sezione 1: GDPR. - 1. Concetto di dati personali. - 2. Base legittima di trattamento dei dati. - 3. Big Data, algoritmi e intelligenza artificiale. - Sezione 2: Intelligenza Artificiale. - 1. Dell'intelligenza artificiale. - 2. *Machine Learning* e *Deep Learning*. - 3. Breve introduzione al *k-means clustering*. - 4. Compliance *by default* e *by design*.

Sezione 1

Big Data: l'adattamento giuridico alla fattispecie tecnologica

1. *Concetto di dati personali*

I dati personali di un individuo sono costituiti, sostanzialmente, da ogni e qualsiasi informazione che lo riguarda. Per individuo si intende una persona fisica identificata o, comunque, identificabile. Detto individuo è definito l'"interessato". Il titolare del trattamento[1] è il soggetto deputato alla raccolta e alla gestione dei suddetti dati personali ed è tenuto a identificare l'interessato con tutti i mezzi dei quali è ragionevole avvalersi, direttamente o indirettamente. Ciò consente di fare alcune prime riflessioni sulla circostanza che non esiste, evidentemente, un'unica metodologia valida per qualsiasi persona il titolare del trattamento si trovi di fronte; gli strumenti utilizzati, e quindi l'identificazione in questo caso, variano a seconda delle situazioni soggettive e oggettive e devono essere individuate volta per volta. Una diversa considerazione possibile è che se il dato non è riconducibile ad una persona fisica individuata o individuabile, ovvero è anonimo, non è oggetto di regolamentazione sulla base del *General Data Protection Regulation*[2] (in seguito, GDPR). Un'altra limitazione della normativa considerata è che questa non

[1] Per trattamento si intende qualunque operazione – anche senza l'impiego di attrezzatura informatica – riguardante *"la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, 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"*, art. 4 Regolamento 679/2016, c.d. "*General Data Protection Regulation*".

[2] *"Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca."*, considerando 26, Regolamento 679/2016.

si applica alle persone decedute[3] o alle persone giuridiche, dato che l'art. 1 contempla espressamente le sole persone fisiche.

Ciò detto, non si vuole in questa sede affermare che le persone giuridiche siano prive di qualsiasi tutela: si ricorda, per completezza di informazione, che la Convenzione 108 modernizzata dà la possibilità alle parti aderenti di prevedere una estensione di alcuni diritti alle persone giuridiche e che la direttiva *e-privacy*, inerente la tutela della vita privata e della corrispondenza, vede un progetto di regolamento tuttora in fase di approvazione che estende la tutela alle persone giuridiche. Come si è detto, qualsiasi dato riferibile a una persona fisica è considerabile "dato personale"[4]; ciò è vero a prescindere dalla natura dell'informazione. Ad esempio, nella documentazione attestante l'esito di un colloquio di lavoro potrebbero essere presenti dati di natura oggettiva (il candidato possiede una laurea magistrale) piuttosto che soggettiva (il valutatore ritiene che il candidato sia polemico): entrambi sono riferiti a una persona fisica individuata o, comunque, individuabile, pertanto sono parimenti oggetto di tutela ai sensi del GDPR. Nemmeno la circostanza che i dati personali siano di natura privata o pubblica sortisce l'effetto di una diversa tutela[5]. I dati sono da considerarsi personali anche se l'identificazione è possibile in via potenziale: se, ovvero, attraverso di essi sia possibile estrarre informazioni in modo tale che la suddetta identificazione diventi possibile. L'articolo 4 del GDPR in merito stabilisce che 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". In un parere del gruppo di lavoro articolo 29 si osserva, peraltro, che "senza neanche cercare il nome e l'indirizzo di un

[3] Considerando 27, *ibidem.*

[4] Già in proposito la Convenzione 108 del 28/01/1981 prevedeva, all'art. 2, che fosse considerabile dato personale "*ogni informazione concernente una persona fisica identificata o identificabile"*, proponendo di fatto una definizione il più possibile onnicomprensiva.

[5] Si veda Corte EDU, Amann c. Svizzera, n. 27798/95, 16 febbraio 2000, punto 65.

soggetto è possibile categorizzarlo sulla base di criteri socioeconomici, fisiologici, filosofici o di altro tipo, e attribuirgli alcune decisioni, tanto più che il punto di contatto (il computer) non richiede più necessariamente che ne sia svelata l'identità in senso stretto"[6]. Anche il modo con il quale i dati personali sono archiviati o utilizzati è ininfluente rispetto alla necessità di rispettare la normativa: che si parli di dati personali o di immagini contenuti in comunicazioni scritte o orali[7], di immagini tratte da sistemi a circuito chiuso[8] o di semplici suoni[9]. Sulla base di quanto si è detto, risulta di tutta evidenza quanta importanza rivesta la riconducibilità di un'informazione a un singolo individuo: l'individuabilità di un soggetto risulta essere la pietra sulla quale è basato in ottima parte il disposto normativo.

La *ratio* di tale scelta è piuttosto evidente: ciò che si vuole disciplinare non è, *sic et simpliciter*, l'uso di dati personali, quanto l'identità di un determinato individuo, al fine di proteggere il suo diritto alla riservatezza. Questa considerazione ha portato ad approfondire le modalità che consentono di spezzare il legame fra i dati e il soggetto al quale sono riferiti: l'anonimizzazione e la pseudonimizzazione. Il problema dell'identificabilità del soggetto al quale si riferiscono i dati si può porre almeno in due momenti differenti: quando i dati vengono raccolti, qualora sia possibile farlo senza doverlo obbligatoriamente identificare, e quando questi devono essere in qualche modo "dismessi" dal titolare del trattamento, secondo il principio della limitazione della conservazione[10], che sostanzialmente stabilisce che egli debba procedere a ciò ogni qual volta non abbia più bisogno dei dati, o questi non servano più al loro scopo iniziale. Anonimizzare

[6] Gruppo di lavoro articolo 29 per la protezione dei dati, parere 4/2007 sul concetto di dati personali, WP 136, 20 giugno 2007, pag. 15.

[7] Corte EDU, Von Hannover c. Germania, n. 59320/00, 24 giugno 2004; Corte EDU, Sciacca c. Italia, n. 50774/99, 11 gennaio 2005; CJUE, C-212/13, František Ryneš c. Úřad pro ochranu osobních údajů, 11 dicembre 2014.

[8] Corte EDU, Peck c. Regno Unito, n. 44647/98, 28 gennaio 2003; Corte EDU, Köpke c. Germania (dec.), n. 420/07, 5 ottobre 2010; GEPD (2010), *The EDPS video-surveillance guidelines* [linee guida EDPS sulla videosorveglianza], 17 marzo 2010.

[9] Corte EDU, P.G. e J.H. c. Regno Unito, n. 44787/98, 25 settembre 2001, punti 59 e 60; Corte EDU, Wisse c. Francia, n. 71611/01, 20 dicembre 2005 (versione in lingua francese).

[10] Si veda l'articolo 5, paragrafo 4, lettera e) del Regolamento 679/2016; si veda anche l'articolo 5, paragrafo 4 lettera e) della Convenzione n. 108 modernizzata.

i dati significa, sostanzialmente, rimuovere da un set di dati personali qualsiasi elemento che consenta di ricollegarli all'interessato, così da non consentirne l'identificazione. Ciò deve essere fatto non solo con riferimento alle informazioni che direttamente potrebbero identificarlo, ma anche con quelle che potrebbero essere utilizzate indirettamente per ottenere lo stesso scopo. Tale obiettivo risulta tanto più alto quanto maggiore è la quantità di dati utilizzati. Il legislatore europeo, peraltro, nel tentativo di descrivere una metodologia di approccio piuttosto che un comportamento negativo da sanzionare, evita di addentrarsi in livelli di dettaglio che inevitabilmente finirebbero per depotenziare la portata del regolamento 679/2016, stabilendo talvolta principi che non sono per niente scontati da rispettare[11]: nel considerare "tutti i mezzi … di cui il titolare … può ragionevolmente avvalersi per identificare detta persona fisica" il legislatore, di fatto, pone una serie di problemi nomofilattici che non possono che essere risolti caso per caso. Non aiuta, anzi forse peggiora anche la situazione, l'ulteriore successiva specificazione circa la necessità di "prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto" delle tecnologie disponibili e degli sviluppi tecnologici. Queste considerazioni acquistano maggiore chiarezza se si considera che anche il gruppo di lavoro articolo 29, in un suo considerando[12], nell'analizzare diverse tecniche di anonimizzazione utilizzate[13] perviene alla conclusione che in determinate situazioni queste possano non bastare per rendere l'identificazione effettivamente impossibile, di fatto prospettando situazioni nelle quali il titolare

[11] *"I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici",* considerando 26, GDPR.

[12] Parere 05/2014 sulle tecniche di anonimizzazione, WP216, 10 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[13] *Noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity and t-closeness.*

del trattamento sia costretto a cancellare i dati in suo possesso per rispettare la norma.

La seconda metodologia summenzionata, ovvero la pseudonimizzazione, è definita dalla norma[14] come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile". Non si tratta, pertanto, di rimuovere – come nel caso dell'anonimizzazione – alcuni dati per rendere impossibile l'identificazione, quanto di fare in modo che questa rimanga possibile sulla base di informazioni accessibili solo al titolare del trattamento su richiesta di un soggetto legittimato. Si pone, evidentemente, un problema in più rispetto all'anonimizzazione: mentre quest'ultima pone la difficoltà di individuare tutti i dati che, direttamente o indirettamente, rendono identificabile un interessato, con la pseudonimizzazione questi stessi dati devono essere spostati in un set diverso, o comunque vanno applicate determinate *policy* di protezione all'accesso per far sì che sia solo il titolare del trattamento a poterli consultare. In altre parole, la pseudonimizzazione non solleva il titolare del trattamento dal rispetto degli obblighi previsti dal GDPR in materia di protezione dei dati personali, ma può essere una metodologia da applicare per ridurre i rischi legati alla sicurezza delle infrastrutture informatiche[15]. Vi sono alcune tipologie di dati che hanno meritato una particolare attenzione da parte del legislatore europeo[16], ovvero: dati personali che rivelano l'origine razziale o etnica, che rivelano le opinioni politiche, le convinzioni religiose o di altro tipo comprese le convinzioni filosofiche, dati personali che rivelano l'appartenenza sindacale, dati genetici e dati biometrici trattati al fine di

[14] Articolo 4, paragrafo 5 del GDPR.

[15] Su questo aspetto si veda anche il punto 18 della relazione esplicativa della Convenzione n. 108 modernizzata.

[16] Articolo 9, GDPR; articolo 6, convenzione 108 modernizzata.

identificare una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona[17].

2. *Base legittima di trattamento dei dati*

Affinché vi possa essere il rispetto della normativa a protezione della *privacy* è necessario che il trattamento dei dati personali avvenga, preliminarmente, sulla base di due principi fondamentali: i dati devono essere "trattati in modo lecito, corretto e trasparente"[18] e vi deve essere conformità rispetto ad uno dei legittimi presupposti per il trattamento, sia che i dati siano personali non sensibili (vd. Art. 6 GDPR), sia che siano sensibili (vd. Art. 9). La base legittima più utilizzata e, in un certo senso, più sottovalutata è il consenso dell'interessato. La possibilità di utilizzarlo è prevista in più fonti giuridiche[19]; per rimanere nell'ambito del GDPR, si deve fare riferimento ad una serie di disposizioni.

In particolare, all'articolo 4 è riscontrabile la definizione di consenso e le caratteristiche necessarie affinché sia valido; all'articolo 6 si prevede che esso sia utilizzabile come base legittima; all'articolo 7 sono descritte in dettaglio le condizioni per ottenere un valido consenso e all'articolo 8 si stabiliscono le norme particolari per il consenso dei minori con riferimento ai servizi della società dell'informazione.

Le caratteristiche principali del consenso sono quattro: esso deve essere libero, informato, specifico e inequivocabile. Il consenso è libero quando non vi sono coercizioni in tal senso, ovvero "soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni, coercizioni o

[17] Si veda in merito CGUE, C-101/01, processo penale a carico di Bodil Lindqvist, 6 novembre 2003, punto 51.

[18] Articolo 5, GDPR.

[19] Cfr. Articolo 5, paragrafo 2 della Convenzione 108 modernizzata; Consiglio d'Europa, Comitato dei Ministri (2010), *raccomandazione CM/Rec(2010)13 del Comitato dei Ministri agli Stati membri sulla protezione delle persone con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, 23 novembre 2010, articolo 3.4, lettera b).

conseguenze negative significative nel caso in cui" l'interessato non lo manifesti[20]. In particolare, "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto"[21]: ciò significa evidentemente che la coercizione può anche non essere operata in fase di manifestazione del consenso, ben potendo concretizzarsi in una mancata utilità in caso lo si revochi. L'evidente conseguenza dell'affermazione precedente consiste nell'impossibilità, in alcune occasioni, di considerare il consenso fornito dall'interessato una base legittima del trattamento, perché esso non può intendersi fornito liberamente. Si pensi, ad esempio, alla necessità di fornire tutta una serie di dati personali per effettuare la registrazione ad un sito online di un Ente pubblico: indipendentemente dal fatto che tale registrazione sia facoltativa, se questa dà accesso a una serie di servizi di indiscutibile importanza, come ad esempio la possibilità di pagare le tasse comunali online o di effettuare un estratto debitorio a una certa data, o ancora di prenotare l'accesso fisico ai locali comunali, è sicuramente improprio definire "libero" il consenso fornito, dato che altrimenti l'interessato viene escluso da servizi decisamente importanti. In alcuni casi vi possono essere condizioni insite nel rapporto fra interessato e titolare del trattamento che rendono il consenso, se non automaticamente inadatto ad essere considerato base legittima, comunque di per sé oggetto di particolare attenzione. Si pensi ai rapporti nei quali vi è un vincolo di subordinazione: risulta evidente che la disparità di posizione fra titolare del trattamento e interessato può rendere il consenso una base inadatta ai fini del rispetto delle disposizioni del GDPR[22]. Con i suddetti esempi non si vuole affermare che il consenso, quando vi sia un interesse

[20] Si veda Gruppo di lavoro articolo 29, parere 15/2011 sulla definizione di consenso, WP 187, Bruxelles, 13 luglio 2011, pag. 12.

[21] Articolo 7, paragrafo 4, GDPR.

[22] Gruppo di lavoro articolo 29, parere 8/2001 sul trattamento dei dati personali nell'ambito dei rapporti di lavoro, WP 48, Bruxelles, 13 settembre 2001; Gruppo di lavoro articolo 29, Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995, WP 114, Bruxelles, 25 novembre 2005; Gruppo di lavoro articolo 29, parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, Bruxelles, 8 giugno 2017.

di un certo tipo o un qualsiasi vincolo di subordinazione, non possa mai essere una base legittima, ma che va valutato caso per caso: se si considera una variante del primo esempio, dove invece che servizi pubblici vi è l'utilizzo di una carta carburante che, tramite registrazione – e quindi la comunicazione di dati personali – concede un piccolo sconto all'utilizzatore, non si può certo escludere per questo che il consenso possa essere una base legittima, dato che il vantaggio che deriva all'interessato/utilizzatore della carta non è tale da condizionare, di per sé stesso, la scelta di quest'ultimo, che pertanto rimane libera.

Il secondo aspetto fondamentale del consenso è l'informazione dell'interessato, la quale deve essere adeguata, deve cioè contenere una informazione precisa e sufficientemente comprensibile dell'elemento rispetto al quale il consenso stesso viene richiesto; l'interessato, infatti, "deve ricevere, in modo chiaro e comprensibile, informazioni precise e complete su tutti gli aspetti rilevanti [...], come la natura dei dati trattati, le finalità del trattamento, i destinatari di eventuali trasferimenti e i diritti" dello stesso[23].

Elemento indispensabile perché l'interessato possa definirsi adeguatamente informato è senz'altro la specificazione delle conseguenze che il mancato consenso comporta[24]. Per essere chiara, ovvero comprensibile, l'informazione deve avvenire facendo attenzione al linguaggio utilizzato e ai tecnicismi utilizzati, in considerazione del pubblico medio al quale l'informazione stessa viene indirizzata[25].

Il consenso deve, inoltre, essere inequivocabile, ovvero non deve esservi alcun dubbio circa l'intenzione dell'interessato di volerlo effettivamente fornire. Normalmente, quindi, ciò richiede che l'interessato compia una specifica azione di un qualche genere; è possibile, però, che ciò avvenga in modo implicito. Si pensi, ad esempio, ad un titolare del trattamento che, in fase di registrazione,

[23] Gruppo di lavoro articolo 29, Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), WP 131, Bruxelles, 15 febbraio 2007.

[24] Si consideri che l'interessato deve capire "*cosa significa il fatto di prestare il proprio consenso e la misura dello stesso*", relazione esplicativa della Convenzione 108 modernizzata.

[25] Gruppo di lavoro articolo 29, parere 15/2011 sulla definizione di consenso, WP 187, Bruxelles, 13 luglio 2011, pag. 19.

informi l'interessato del fatto che l'utilizzo stesso di determinati servizi comporta espressione del consenso al trattamento dei dati. Risulta di tutta evidenza che, a seconda dei dati raccolti e dei servizi erogati, ciò potrebbe non bastare per considerare il consenso espresso in modo inequivocabile[26]. Nel caso dei minori, poi, il consenso diventa una base legittima ancora più fragile, dato che non sempre il soggetto di minore età può considerarsi effettivamente in grado di comprendere quali autorizzazioni sta concedendo al titolare del trattamento, quali sono i suoi diritti, quali sono le conseguenze, in generale, della scelta che sta per compiere. Per i minori, quindi, la norma affronta l'appropriatezza del consenso come base legittima con particolare attenzione[27], prevedendo, all'articolo 8, che il trattamento sarà lecito "soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale" quando ad esprimere il consenso sia un soggetto di età inferiore ai 16 anni[28]. Naturalmente nel contesto considerato il linguaggio utilizzato assume peculiare importanza, infatti la norma, benché con un considerando[29], prevede che questo debba essere semplice e chiaro, tale per il quale un minore possa capirlo "facilmente".

Una seconda e diversa base legittima consiste nella necessarietà del trattamento dei dati ai fini dell'esecuzione di un contratto; tale circostanza, in particolare, è prevista all'articolo 6 paragrafo 1 lettera b) del GDPR[30]. Una terza possibilità di avere una base legittima del trattamento è data da una previsione di legge che insiste sul titolare del trattamento[31]; tale circostanza può verificarsi sia se il titolare

---

[26] *"Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento."*, considerando 42, GDPR.

[27] Dato che essi *"possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali"*, considerando 38, GDPR.

[28] Anche se lo stesso articolo prevede che gli Stati possano abbassare questo limite, comunque non al di sotto dei 13 anni.

[29] Si veda Considerando 58, GDPR.

[30] *"Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso".* In proposito si vedano anche la relazione esplicativa della Convenzione n. 108 modernizzata, punto 46; Consiglio d'Europa, Comitato dei Ministri (2010), *raccomandazione CM/Rec(2010)13 del Comitato dei Ministri agli Stati membri sulla protezione delle persone con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, 23 novembre 2010, articolo 3.4, lettera b).

[31] Articolo 6, paragrafo 1, lettera c), GDPR.

del trattamento sia un soggetto pubblico, sia che sia un soggetto privato. È già stato fatto, in questa sede, un esempio riguardante il datore di lavoro e il lavoratore: il primo ha senz'altro un obbligo legale a trattare alcuni dati personali, inerenti alla fiscalità e alla previdenza, del secondo, dato che qualora non lo facesse verrebbe meno ad obblighi di legge di altra natura.

Più in generale, quando la base legittima del trattamento è data da una previsione di legge, dovrebbe essere quest'ultima a identificare il titolare del trattamento, i dati oggetto del trattamento stesso, le limitazioni, il periodo di memorizzazione e comunque tutti gli elementi utili a definire e dettagliare quanto possibile la base legittima stessa. Anche questa base legittima conosce alcuni limiti: per esempio, deve essere obbligatoriamente conforme agli articoli 7 e 8 della Carta Europea dei Diritti Fondamentali e all'articolo 8 della Convenzione Europea dei Diritti dell'Uomo. "La salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica"[32] costituiscono una quarta possibilità di base legittima di trattamento. A differenza delle basi legittime precedentemente esposte, quella in parola ha un carattere residuale, poiché può essere considerata valida quando il trattamento "non può essere manifestamente fondato su un'altra base giuridica"[33]. Un'ulteriore base legittima dei dati è costituita dall'interesse pubblico e dall'esercizio di pubblici poteri, prevista dall'articolo 6, paragrafo 1, lettera e) del GDPR, qualora il trattamento dei dati di un individuo sia necessario "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento"[34]. Anche in questo caso valgono le stesse osservazioni di cui sopra in merito alla necessarietà del rispetto di alcune condizioni quando la base legittima del trattamento è costituita da un obbligo legale. L'ultima base legittima per il trattamento dei dati è costituita dall'interesse legittimo del terzo, ai sensi dell'articolo 6, paragrafo 1, lettera f) del GDPR, che si sostanzia nella possibilità di trattare legittimamente dati personali di

[32] Articolo 6, paragrafo 1, lettera d), GDPR.
[33] Considerando 46, GDPR.
[34] Considerando 45, GDPR.

un individuo ogni qual volta ciò sia "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi – ad eccezione delle autorità pubbliche nell'esercizio dei loro compiti – cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela"[35]. L'interesse legittimo, pertanto, può essere sia del terzo che dell'interessato. Questa base legittima è probabilmente quella che va valutata caso per caso, per verificare l'effettiva legittimità del trattamento e il mancato prevaricamento dell'interesse al trattamento dei dati rispetto al diritto di riservatezza tutelato dalla norma in commento. Affinché possa essere utilizzata la base legittima in parola è necessario che si avverino, sostanzialmente, tre condizioni: l'effettiva esistenza di un interesse legittimo, la necessarietà del trattamento dei dati personali per il perseguimento di quest'ultimo e la non prevalenza dei diritti e delle libertà fondamentali dell'interessato su quelli del titolare del trattamento o del terzo[36].

Come si diceva anche all'inizio del presente paragrafo, quanto detto vale in generale in tutti i casi di trattamento di dati personali; circa il trattamento di dati sensibili vanno fatte ulteriori precisazioni. L'articolo 9 del GDPR, infatti, prevede l'applicabilità di un regime dettagliato ogni qual volta siano trattati dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale, nonché per il trattamento di dati genetici e dati biometrici intesi a identificare in modo univoco una persona fisica, e dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona: in via generale, il trattamento dei suddetti è vietato. Il divieto è stemperato da un elenco esaustivo di eccezioni riportato all'articolo 9 paragrafo 2, dove sono elencate situazioni in cui l'interessato acconsente esplicitamente al trattamento dei

[35] Articolo 7, paragrafo 1, lettera f), Direttiva 95/46; articolo 6, paragrafo 1, lettera f), GDPR; considerando 47, GDPR.

[36] Cfr. CGUE, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA «Rīgas satiksme», 4 maggio 2017, https://curia.europa.eu/juris/document/document.jsf;jsessionid=4512EFC773F60B2910D899406556C29E?text=&docid=190322&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=3528070, la quale, benché si pronunci in realtà sull'art. 7 della Direttiva 95/46, svolge osservazioni assolutamente compatibili con la normativa vigente.

dati, oppure il trattamento è effettuato da un organismo che non persegue scopi di lucro e riveste carattere politico, filosofico, religioso o sindacale nel corso di attività legittime e riguarda solo i suoi (ex) membri o persone che hanno contatti regolari con esso per tali scopi, oppure ancora il trattamento riguarda dati personali esplicitamente resi pubblici dall'interessato.

Un'ulteriore eccezione è data dalla circostanza nella quale il trattamento sia necessario per adempiere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato nel contesto dell'occupazione, della sicurezza sociale e della protezione sociale, o per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica (quando l'interessato non può prestare il proprio consenso), oppure ancora per rivendicare, esercitare o difendere un diritto per via giudiziaria o quando i tribunali esercitano le loro funzioni giurisdizionali, o per finalità di medicina preventiva o di medicina del lavoro: per la «valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità», oppure a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, quando vi siano motivi di interesse pubblico nel settore della sanità pubblica o comunque quando vi siano motivi di interesse pubblico rilevante.

Quando i dati trattati rientrano nelle fattispecie di cui sopra il titolare del trattamento può procedere anche sulla base del consenso dell'interessato, con la importante differenza che questo deve obbligatoriamente essere espresso e che il diritto UE e quello degli Stati Membri possono prevedere l'esclusione di questa possibilità in determinati casi e per determinate fattispecie.

3. *Big Data, algoritmi e intelligenza artificiale*

Di big data si sente parlare ormai in maniera quasi incessante, a vari livelli di approfondimento e in molteplici campi del sapere. Sono almeno due i fattori che

hanno contribuito, in massima parte, a delineare il panorama nel quale ci troviamo attualmente: l'incremento della capacità computazionale, anche tramite il drastico miglioramento delle tecnologie di costruzione dei componenti *hardware*, e la crescita esponenziale della rete internet, sia in termini di velocità ed efficienza delle connessioni, sia in termini di tipologia di dati trasmessi. Fino a venti anni fa, infatti, la comunicazione era strutturata tramite interfacce sostanzialmente semplici, che consentivano limitate interazioni e, comunque, lo scambio di informazioni a senso unico: nella maggioranza dei casi tramite internet avveniva una comunicazione simile a quella della radio o della televisione, ovvero un unico soggetto parla a una molteplicità di soggetti. Vi era, in altre parole, una distinzione ancora abbastanza marcata su chi produceva contenuti e chi ne fruiva.

In due decadi questo concetto è stato completamente accantonato: oggi chiunque può essere contemporaneamente produttore e fruitore, senza dover sostenere costi d'impianto di una qualche reale importanza e, di fatto, avendo la possibilità di immettere in una rete interconnessa con miliardi di dispositivi le proprie opinioni, impressioni, convinzioni… in altre parole, i propri dati personali[37]. Tale circostanza, accompagnata al fatto che sempre più dispositivi sono stati resi "intelligenti" (comandabili da remoto) e interconnessi (pensiamo ai sensori d'inquinamento di una grande città, oggi sicuramente connessi in qualche modo tramite internet), ha comportato un enorme aumento della quantità di dati disponibili in formati comprensibili ad elaboratori informatici.

[37] Peraltro l'interconnessione dei sistemi collegati ad una rete, consentendo di valicare i confini nazionali ed europei, ha comportato inevitabilmente tensioni e incomprensioni fra sistemi giuridici differenti. In merito, basti pensare che *"negli ultimi anni Europa e Stati Uniti d'America si sono resi protagonisti di uno scontro, contrassegnato spesso da toni particolarmente aspri, sul tema della data privacy. L'Europa ha agito sia sul piano politico sia sul piano giuridico – ma direi anche culturale – per consolidare la posizione volta ad affermare il principio che al trattamento dei dati personali degli europei occorre applicare il diritto europeo. Ciò anche in base alla convinzione (certo non infondata) che il livello di protezione dei dati personali adottato in Europa è assai più elevato rispetto agli altri. A questa impostazione gli Stati Uniti hanno risposto con una visione totalmente diversa, in cui gli interessi – economici e non solo – americani hanno un peso maggiore rispetto alle tutele giuridiche europee. […]. Ciò ha comportato il risultato che negli Stati Uniti il diritto alla protezione dei dati personali non soltanto non è un diritto "fondamentale", ma configura una posizione giuridica soggettiva "isolata", in cui l'individuo sembra schiacciato da interessi di attori che godono di una protezione – politica e giuridica – superiore."*, S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, 2017, Torino, p. 49.

In aggiunta a tutto quanto detto finora va considerato che, ormai, le tecnologie di intelligenza artificiale sono alla portata di tutti e consentono di elaborare una mole di dati impensabile fino anche solo a un decennio fa. Le analisi comportano la scoperta di correlazioni e la possibilità di effettuare, con un grado di sicurezza sempre più alto, inferenza su dati noti per addivenire a dati non noti i quali, con grande facilità, sono classificabili come dati personali, se non come dati sensibili.

Le tecnologie in parola, peraltro, sono utilizzate non solo per analizzare i dati al fine di perseguire uno scopo dichiarato di profilazione, quanto per erogare servizi che altrimenti non sarebbero possibili con lo stesso grado di elasticità: pensiamo agli assistenti vocali presenti da lungo tempo su tutti gli *smartphone*, oggi in rapida diffusione anche su dispositivi domestici (come Alexa, per fare un esempio). La funzione dell'assistente vocale è possibile solo grazie a un *software* basato su algoritmi di intelligenza artificiale che analizza costantemente tutto quello che gli viene proposto, sia in termini di input diretto (*query* che vengono poste in linguaggio naturale) sia indiretto (rumori ambientali in genere, nell'attesa di ricevere il comando vocale di attivazione).

Risulta di tutta evidenza, a questo punto, come l'attuale panorama dei servizi dell'informazione costituisca un'enorme sfida per il legislatore, nella ricerca dell'adeguato bilanciamento – ammesso che esista – fra il diritto alla riservatezza riconosciuto a qualsiasi essere umano e il miglioramento continuo della tecnologia basata su intelligenza artificiale, riconosciuta come il prossimo miglioramento epocale che la specie umana conoscerà, in parte già in corso. Da parte del legislatore europeo, il concetto di big data incorpora in sé "la crescente capacità tecnologica di raccogliere, trattare ed estrarre conoscenze nuove e predittive a partire da grandi volumi, varietà e velocità dei dati"[38].

[38] Si vedano in merito Consiglio d'Europa, Comitato consultivo della Convenzione 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 gennaio 2017, pag. 2; Commissione europea, *comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, verso una florida economia basata sui dati*, COM (2014) 442 final, Bruxelles, 2 luglio 2014, pag. 4; International Telecommunications Union (2015), *raccomandazione Y.3600. Big Data – Cloud computing based requirements and capabilities.*

La definizione è volutamente molto ampia: non comprende solo la raccolta e la memorizzazione, ma anche l'analisi e l'estrazione di nuove informazioni, anche a livello inferenziale, ovvero predittivo, nella consapevolezza che qualsiasi sia la finalità iniziale il dato raccolto può essere oggetto di ulteriore elaborazione e, anche tramite la combinazione con dati sempre nuovi, fornire informazioni sempre diverse al soggetto che si occupa di effettuare la raccolta. Tale ampiezza è necessaria sulla base della metodologia di funzionamento della tecnologia utilizzata: algoritmi di intelligenza artificiale. In termini semplificati, tali software non seguono un linguaggio di programmazione che preveda rigidamente cosa fare a seconda dell'input ricevuto; al contrario, il linguaggio di programmazione è loro necessario per capire come trattare le informazioni ricevute e correlarle l'una con l'altra.

Per questo motivo, alcuni dispostivi possono percepire ciò che li circonda, comprendere l'ambiente nel quale operano e agire in tempo reale[39]. Tutto ciò si può riassumere sostenendo che il software "imita" funzioni cognitive, come l'apprendimento e la risoluzione di problemi, normalmente associate a persone fisiche[40]. Quando si parla dei rischi associati a tale tecnologia, spesso ci si riferisce alle cosiddette tre "v": volume, velocità e varietà dei dati trattati, dato che al crescere di queste caratteristiche crescono anche i rischi insiti nell'uso della tecnologia stessa.

In particolare, oggetto di attenzione da parte del legislatore sono i processi decisionali automatizzati e la profilazione; i primi possono indurre a prendere decisioni che possono avere ricadute su persone e/o su gruppi di esse (si pensi ai software di intelligenza artificiale utilizzati in fase di selezione del personale), la seconda può essere utilizzata per comprendere le caratteristiche personali di un individuo e tenerne conto a vari scopi (ad esempio la pubblicità personalizzata,

[39] Si pensi all'autopilota di alcune vetture oggi in commercio: senza una comprensione in tempo reale di ciò che circonda la vettura, qualsiasi decisione di guida sarebbe impossibile.

[40] S. Russel e P. Norvig, *Artificial Intelligence: A Modern Approach (seconda ed.)*, 2003, Upper Saddle River, New Jersey, pagg. 27, 32–58, 968–972; S. Russel e P. Norvig, *Artificial Intelligence: A Modern Approach (terza ed.)*, 2009, Upper Saddle River, New Jersey, pag. 2.

accesso o meno a particolari categorie di servizi e/o al credito). Il pericolo che queste attività vengono svolte da soggetti che ne fanno un uso improprio è concreto e reale, poiché esse possono comportare violazioni significative dei diritti fondamentali, anche al di là del diritto alla vita privata. Il GDPR dedica particolare attenzione alle tecniche suesposte; l'articolo 22[41], infatti, riconosce il diritto di un individuo a non essere profilato o soggetto a processi decisionali automatizzate e, comunque, al paragrafo 3 riconosce "almeno" il diritto di ottenere l'intervento umano.

Con l'uso di intelligenze artificiali, peraltro, vi sono elementi di criticità ulteriori da prendere in considerazione: chi è effettivamente il titolare del trattamento e in che modo questo può essere ritenuto responsabile di una determinata decisione, chi è il proprietario dei dati raccolti con le metodologie in parola oppure definire le responsabilità precise di tutti gli attori coinvolti. Se, ad esempio, il software di IA viene considerato un prodotto diventa molto complesso attribuire responsabilità ai sensi della normativa *privacy*, dato che questa comprende responsabilità di tipo personale e non per i danni causati da un prodotto.

Da tempo, sulla base di queste considerazioni, si sta cercando di comprendere come rivedere le norme in tema di responsabilità quando sono utilizzati sistemi di intelligenza artificiale. Rispetto ai principi statuiti nel GDPR, ve ne sono alcuni più in inconciliabili di altri con le tecnologie in parola: il principio di legittimità, di minimizzazione, di limitazione delle finalità, di trasparenza e di esattezza. Riguardo al primo si è già detto: può essere complesso verificare se chi utilizza i dati abbia effettivamente una base legittima per il trattamento. Riguardo al principio di minimizzazione e di limitazione delle finalità, il problema è estremamente simile e riguarda il modo in cui gli algoritmi di intelligenza

[41] I dati e le procedure automatizzate sono da sempre oggetto di attenzione da parte del legislatore comunitario, in realtà. In questa sede si ritiene opportuno ricordare l'art. 5 della Convenzione 108, il quale stabiliva che "*I dati a carattere personale oggetto di elaborazione automatica devono essere: a) ottenuti ed elaborati lealmente e legalmente; b) registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini; c) adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati; d) esatti e, se necessario, aggiornati; e) conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati".*

artificiale utilizzano i dati e prendono decisioni sulla base di essi: cancellare dati acquisiti, o essere sicuri delle finalità per le quali i dati vengono trattati sono attività in aperto contrasto con funzionamento stesso delle tecnologie in analisi, che potrebbero arrivare a diventare inutili qualora applicassero i principi summenzionati in modo rigoroso.

Riguardo poi alla trasparenza, se è vero che un software di intelligenza artificiale non esegue una serie di valutazioni sulla base di una programmazione preimpostata risulta di immediata evidenza come potrebbe essere molto complesso motivare le circostanze che hanno portato un software a prendere una decisione piuttosto che un'altra. Il principio di esattezza dei dati risulta praticabile con la stessa difficoltà dei principi summenzionati, se si considera che gli algoritmi collazionano informazioni da sorgenti diverse, la cui affidabilità è impossibile da verificare il più delle volte. Al fine di imporre a qualsiasi titolare un trattamento corretto e trasparente dei dati raccolti, il GDPR ha previsto che debbano essere fornite informazioni adeguate[42] circa "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"[43], salvo poi vanificare in parte questa disposizione prevedendo un esonero qualora "comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato"[44].

[42] Storicamente, i diritti dell'interessato a conoscere le modalità con le quali sono trattati i suoi dati personali sono sempre stati rilevanti; si pensi all'art. 8 della Convenzione 108, che stabiliva che ogni persona doveva avere la possibilità di *"a. conoscere l'esistenza di una collezione automatizzata di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale o la sede principale del responsabile della collezione; b. ottenere a ragionevoli intervalli e senza eccessivo ritardo o spesa la conferma dell'esistenza o meno, nella collezione automatizzata, di dati a carattere personale che la riguardano e la comunicazione di tali dati in forma intellegibile; c. ottenere, all'occorrenza, la rettifica di tali dati o la loro cancellazione qualora essi siano stati elaborati in violazione delle disposizioni di diritto interno che danno attuazione ai principi fondamentali enunciati negli articoli 5 e 6 della presente Convenzione; d. disporre di un ricorso se non viene dato seguito ad una domanda di conferma o, a seconda dei casi, di comunicazione, di rettifica o di cancellazione ai sensi delle lettere be e c del presente articolo"*.

[43] Articolo 13, paragrafo 2, lettera f), GDPR.

[44] Articolo 14, paragrafo 5, lettera b), GDPR.

Su questo aspetto si è pronunciato anche il gruppo di lavoro articolo 29, prevedendo che in ogni caso la complessità del trattamento non dovrebbe, di per sé, esonerare il titolare del trattamento dal fornire spiegazioni adeguate[45]. La stessa esenzione non si applica ai diritti di accesso, rettifica e cancellazione[46], anche se il titolare del trattamento può essere esonerato dal notificare la cancellazione o la rettifica dei dati all'interessato qualora "si riveli impossibile o implichi uno sforzo sproporzionato"[47]. All'interessato è riconosciuto il diritto di opposizione, al quale il titolare del trattamento può evitare di dare attuazione qualora vi sia un legittimo interesse d'ordine superiore (e comunque mai quando la finalità del titolare è il marketing diretto).

[45] Gruppo di lavoro articolo 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 2017, pag. 14.

[46] In particolare il diritto di cancellazione è assurto spesso agli onori di cronaca, anche per fatti estremamente gravi e spiacevoli, come quello di Tiziana Cantone occorso nel 2015; in generale, comunque, "*il dibattito sul diritto all'oblio può offrire un importante contributo alla riflessione sulla vulnerabilità di donne uomini bambini che, sempre più immersi in un mondo virtuale, rischiano di pagare un prezzo altissimo e assolutamente reale a causa di condotte (proprie o altrui) a volte ingenue, altre volte lucidissime, a volte soltanto idiote, altre volte anche violente"*, S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, op. cit., p. 52.

[47] Articolo 19, GDPR.

Sezione 2
IA: la nuova frontiera

1. *Dell'intelligenza artificiale*

Il termine "intelligenza artificiale" è piuttosto difficile da definire. Alcune volte, ad esempio, le persone lo usano per indicare cose che sono difficili da fare per un computer, come ad esempio comprendere un linguaggio parlato, rispetto ad altri compiti che esse sono più abituate a vederlo svolgere, come ad esempio svolgere calcoli complessi. Più di recente, con il crescere dell'interesse circa l'argomento in parola, le aziende spesso cercano di descrivere i propri nuovi prodotti associandovi in vario modo il termine "AI", sebbene talvolta indichino funzionalità svolgibili da qualsiasi computer. Una definizione molto semplicistica di "intelligenza artificiale" può essere la seguente: l'IA è ciò che rende possibile ad una macchina agire in modo tale da sembrare intelligente[48].

In realtà, facendo un passo indietro, si è cominciato a parlare di sistemi intelligenti già nel 1950, ad opera dello scienziato Alan Turing. Naturalmente egli sapeva che non è possibile definire con esattezza cosa si intende per "intelligenza": per questo motivo, quindi, ideò ciò che conosciamo come "Test di Turing". Quest'ultimo si considera superato se un essere umano non possa dire con certezza, entro un tempo limite di cinque minuti, se stia o meno parlando con un sistema automatico o con una persona in carne e ossa. Turing non poteva certo immaginare di parlare con un computer utilizzando il linguaggio naturale nel 1950, perciò utilizzava una telescrivente (ad oggi diremmo che "chattava" con il computer).

In effetti, nel documento nel quale Turing descrive il suo test egli cerca di affrontare tutte le principali convinzioni sulla base delle quali, per le persone dell'epoca, era impossibile che un computer potesse essere intelligente, affrontando una notevole varietà di campi, da posizioni teologiche a questioni

[48] *Artificial Intelligence: implications for business strategy*, T. Malone, MIT-CSAIL, 2017, https://www.csail.mit.edu/.

matematiche. Forse, se lo avesse conosciuto, avrebbe utilizzato un termine coniato dal matematico Marvin Minsky: "*suitcase word"*[49], con esso volendosi riferire a parole che sono come grandi "valigie" nelle quali si possono mettere molteplici significati, dotandole di così tanti concetti tutti contemporaneamente presenti che è difficile darne una definizione precisa. Ciò che probabilmente Turing cercava di dimostrare era che l'intelligenza artificiale, intendendo qui la capacità di un computer di simulare un certo tipo di ragionamento, è una cosa molto seria e concreta, per niente impossibile a priori.

E in effetti dieci anni dopo lo scritto di Turing vennero fondati laboratori importanti da Marvin Minsky, John McCarthy, Allen Newell e Herb Simon. L'approccio di McCarthy, nel suo laboratorio in Stanford, era basato sulla logica matematica. Spese la sua intera vita a cercare di piegare la logica alla sua volontà. Newell e Simon si concentrarono, invece, nel cercare di formalizzare il modo di pensare dell'essere umano. Essi svilupparono alcuni sistemi capaci di risolvere semplici puzzle, di risolvere alcuni problemi in modo che consideravano simile a quello che sarebbe stato adottato da un essere umano. Minsky, invece, evitò di concentrarsi su un singolo approccio, poiché riteneva che fosse necessario adottarne molteplici, che contemplassero diversi punti di vista[50] .

In altri termini si può affermare che mentre Turing ha tentato di dimostrare che l'intelligenza artificiale è una cosa possibile, Minsky è stato colui il quale ha trovato un primo approccio sul come strutturare il problema; del resto, entrambi sono accreditati come i veri pionieri del campo dell'intelligenza artificiale. Nei primi anni sessanta, James Slagle scrisse un programma in grado di risolvere problemi di calcolo integrale in forma chiusa; il risultato fu davvero notevole e consentì di effettuare alcune prime importanti considerazioni. Slagle, infatti, adottò una tecnica chiamata "*problem reduction"*: prendere un problema molto complesso e dividerlo in pezzi più piccoli – e più semplici.

---

[49] M. Minsky, *The Emotion Machine: Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind*, 2007, New York, p. 59.

[50] M. Minsky*, Steps towards artificial intelligence,* Proceedings of the IRE, 1961, Volume 49, Numero 1, pag. 8-30.

Detto approccio venne utilizzato più e più volte: all'inizio degli anni settanta vi erano programmi in grado di interpretare immagini e di imparare da esempi di test. Uno in particolare fu addirittura in grado di rispondere ad una domanda che gli venne posta, in modo simile a come oggi fanno Siri o Alexa[51]. Il punto desumibile dal discorso fatto finora è il seguente: se un problema è ben rappresentato, è ben compreso e strutturato tanto da riuscire a definire uno schema per la sua risoluzione, allora si è ben più che a metà dell'opera.

L'intelligenza artificiale ha a che fare con modelli di pensiero, di percezione e di azione, volendo qui intendere con "modello" una formalizzazione di ciò che si conosce e si vuole riprodurre. Con un modello è possibile comprendere, spiegare, predire e controllare ciò che si vuole, ciò che è il fine ultimo della ricerca scientifica. La rappresentazione di un problema è quindi costituita da una serie di convenzioni, di regole che descrivono ciò che si analizza. A titolo esemplificativo, l'algebra imparata a scuola e usata per risolvere i problemi ivi affrontati niente altro è che una rappresentazione dei problemi stessi, un modo di ricondurre la possibilità di risolverli a una serie di regole. L'intelligenza artificiale è basata su una serie di tecniche finalizzate a schematizzare le azioni di pensare, di percepire e di agire.

Il punto nodale della schematizzazione è che tramite essa è possibile rendersi conto dei vincoli i quali, venendo affrontati, rendono possibile la realizzazione dei modelli. La combinazione di questi modelli è ciò che costituisce un'architettura, ovvero una struttura complessa capace di affrontare problemi complessi. L'intelligenza artificiale, quindi, può essere considerata come qualcosa che si basa su architetture come sopra definite. Negli anni ottanta sopraggiunse il cosiddetto *"AI Winter"*: a causa di aspettative molto alte a fronte di risultati piuttosto deludenti l'interesse per la tecnologia in parola calò considerevolmente.

Anche se molte *startup* finirono per non decollare, vi fu anche qualche successo. L'interesse per l'intelligenza artificiale ha conosciuto una reviviscenza

[51] *Artificial intelligence: implications for business strategy*, P. Winston, MIT-CSAIL, 2017, https://www.csail.mit.edu/.

negli anni duemila, quando sono state messe in commercio alcune tecnologie di successo (come Siri, nel 2010) e vi sono stati alcuni eventi mediatici che hanno avuto una forte risonanza (come la vittoria di Watson nel 2011 nel programma *Jeopardy*). Da questo successo mediatico e dalla combinazione di vari fattori colossi come IBM, Google, Facebook, Amazon e Microsoft hanno cominciato a investire tutti ingenti quantità di capitali e di *know-how* nello sviluppo dell'intelligenza artificiale, scatenando la terza ondata che stiamo vivendo. La combinazione di enormi capacità di calcolo e della disponibilità di una quantità pressoché illimitata di dati ha potuto consentire lo sviluppo di una nuova tipologia di algoritmi statistici, ai quali oggi ci si riferisce con il termine onnicomprensivo di *Machine Learning*.

2. *Machine Learning* e *Deep Learning*

Il *machine learning* è una tecnica di programmazione informatica che ha, come obiettivo, la definizione di metodologie finalizzate a consentire ad un computer, fornitigli una serie di input, di imparare a ricondurli a determinati output non preventivamente determinati. L'approccio alla programmazione adottato da tale disciplina è assolutamente innovativo: se infatti fino ad oggi scrivere un software voleva sostanzialmente dire fornire al computer una serie di istruzioni, più o meno complesse, affinché, data una serie di input preventivamente definiti, fossero prestabilite anche le operazioni da compiere per fornire una serie di output, con il *machine learning* l'obiettivo non è tanto definire tutti gli input possibili, quanto dare alla macchina un modo che le consenta di simulare un processo cognitivo per metterla in grado di rispondere a una serie non predefinita di input con output pertinenti.

Tale approccio è reso possibile dall'unione di algoritmi statistici differenziati a seconda della modalità di ragionamento che si vuole che la macchina simuli[52]. Una

[52] *"Machine learning is essentially a form of applied statistics with increased emphasis on the use of computers to statistically estimate complicated functions and a decreased emphasis on proving confidence*

definizione piuttosto nota di *machine learning* è la seguente: "si dice che un *software* impari dall'esperienza "E" con riferimento a una determinata tipologia di compiti "T" e di misurazione della performance "P", se detta performance nello svolgere i compiti in "T", misurata come "P", aumenta con esperienza "E""[53].

Affinché ciò sia possibile, dopo aver impostato la macchina affinché funzioni secondo i parametri desiderati è necessario un periodo di apprendimento, per diversi motivi: ad esempio in questa fase (cd. *Testing*) gli algoritmi utilizzati cambiano, volta per volta, alcuni parametri interni, per cercare il miglior funzionamento possibile rispetto al *task* assegnato; peraltro, la fase in parola è necessaria, talvolta, per verificare che l'algoritmo abbia effettivamente le *performance* attese e funzioni come previsto. Con i termini *supervised* e *unsupervised* si descrivono, rispettivamente, tecniche di apprendimento differenti: nella prima, l'algoritmo lavora sulla base di un set di dati (*training set*) preventivamente identificato per imparare a identificarne un altro, mentre nella seconda la preventiva identificazione manca.

L'identificazione, normalmente, viene fatta da un essere umano, ma non mancano oggi tecnologie di intelligenza artificiale che sono costruite per identificare *dataset* che fungeranno poi da *training set* per altre intelligenze artificiali. Entrambe le metodologie procedono analizzando la struttura dei dati, per identificare uno schema (*pattern*) che li definisca, ricondurlo ad una tipologia nota e ricercarlo successivamente nei dati da identificare autonomamente. Le tecniche di apprendimento in parola non sono definite in modo rigido, in realtà: servono per consentire una prima identificazione degli algoritmi, ad esempio per consentire agli operatori una più veloce comprensione dell'algoritmo del quale stanno valutando l'utilizzo.

---

intervals around these functions…", I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, 2016, Boston, p. 89.

[53] *"A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E.",* T. Mitchell, *Machine Learning*, 1997, New York, pag. 870-877.

L'utilizzo di una tecnica di apprendimento piuttosto che di un'altra non è, peraltro, mutuamente esclusivo: uno stesso problema può essere affrontato diversamente, a seconda di come lo si imposta. Ciò potrebbe essere utile per dividere un problema eccessivamente complesso in tanti sotto-problemi dei quali è nota la metodologia di risoluzione, oppure che richiedono una capacità di calcolo inferiore rispetto alla soluzione del problema principale. Vi sono diversi compiti che possono essere risolti da tecnologie di *machine learning*; a seconda del compito da risolvere si definisce la tipologia di algoritmo, o la combinazione di algoritmi, da adottare. Un tipo di compito piuttosto diffuso può essere quello della classificazione: al software viene chiesto di identificare un determinato *dataset* in input, riconducendolo ad una determinata categoria *k*.

Un esempio dell'applicazione del compito in parola è dato dal riconoscimento del contenuto di un'immagine: il software, sulla base di un vettore di dati costituito dal valore attribuito alla luminosità dei pixel componenti la stessa, riconduce tramite una funzione matematica l'immagine ad una delle categorie da esso conosciute. Vi possono essere casi nei quali la classificazione deve essere fatta con dati di input non completi: in questo caso l'algoritmo deve imparare un *set* di funzioni, cosicché potrà applicare quella più pertinente a seconda del dato mancante. Tale metodologia può essere molto utile, ad esempio, nell'ambito medico, dato che per ottenere alcuni dati potrebbe essere necessario lo svolgimento di alcuni esami invasivi.

Un compito molto simile alla classificazione è sicuramente la clusterizzazione, ovvero il raggruppamento in *cluster* (grappoli, letteralmente) di una serie di dati ricevuti in input. La similitudine è evidente: sia il primo che il secondo metodo sono finalizzati a riunire in uno stesso gruppo (che sia una classe o un *cluster*) dati ricevuti in input sulla base di caratteristiche simili. La differenza più importante, però, è che mentre il primo compito effettua questa distinzione raggruppando i dati in classi note a priori, il secondo individua la quantità e la tipologia dei *cluster* procedendo a raggruppare i dati che ritiene essere maggiormente simili l'uno con l'altro. Questa differenza di funzionamento è un esempio evidente di compiti che

sono considerati di *supervised* (il primo) e di *unsupervised learning*; sulla base del compito, si sceglierà l'algoritmo opportuno, che quindi sarà categorizzabile allo stesso modo.

Un diverso tipo di compito è dato dalla regressione: da un determinato tipo di input, il software deve fornire un numero come output. Tale è lo scenario nel quale deve essere predetto il valore di un titolo finanziario, ad esempio, dato l'andamento del mercato dei titoli di borsa. Un altro tipo di compito è dato dalla trascrizione: ad un software viene chiesto di ricondurre ad un set di dati strutturato una serie di input relativamente destrutturati, come ad esempio può essere la trascrizione in un file di testo di un discorso in lingua naturale. Un diverso compito può essere quello della traduzione automatica: l'algoritmo deve ricondurre un set di dati espresso in un determinato linguaggio (ad esempio l'inglese) ad un altro linguaggio (ad esempio l'italiano). Sia la trascrizione che la traduzione automatica sono poi riconducibili ad una più ampia categoria di compiti, chiamata output strutturato: vi rientrano tutti i compiti che richiedono ad un algoritmo di restituire come output un vettore contenente elementi strettamente interconnessi. Un esempio può essere la formazione di una frase di senso compiuto a partire da un'immagine data in input.

Un altro ancora può essere quello dell'identificazione di anomalie: si chiede di identificare, fra una serie di elementi, se ve ne sia uno – e nel caso, quale esso sia – che non sembra poter essere ricompreso nella serie in analisi. Un esempio è sicuramente l'identificazione di una spesa anomala rispetto ad un insieme di spese addebitate su una stessa carta di credito. Un altro possibile compito è quello della sintesi e/o del campionamento: ad un software viene chiesto di generare un output simile, ma sempre diverso, rispetto ad un altro dato come input. Tale funzione può essere utile, ad esempio, nei videogiochi, dove può essere noioso e inefficiente generare ogni singolo pixel quando si devono gestire fondali di dimensioni considerevoli.

Vi possono essere poi: l'imputazione di valori mancanti, la quale è necessaria quando un software deve identificare un valore ignoto (o perduto) all'interno di un

set di valori noti; la pulizia dal rumore, quando viene chiesto ad un software di ricondurre un certo tipo di input corrotto a quello che doveva essere in origine (o avrebbe dovuto essere, secondo il calcolo di una probabilità condizionata); la stima di densità, quando l'oggetto della richiesta è l'identificazione di una funzione di probabilità con la quale determinati dati si distribuiscono in uno spazio definito.

3. Breve introduzione al *k-means clustering*

Si è già avuto modo di introdurre il compito noto come clusterizzazione: al software di intelligenza artificiale viene richiesto di raggruppare, a seconda delle similitudini che riscontrerà nei dati, in *k* cluster il *dataset* in input. Le similitudini dei dati non sono note, anzi, sono proprio l'oggetto di approfondimento che la clusterizzazione cerca di mettere in rilievo. L'algoritmo "*K-Means"* serve proprio a definire un *K* numero di raggruppamenti nei quali è possibile collocare i dati ricevuti in input, ovvero, in altre parole, a segmentare un *dataset* disomogeneo in *K cluster* contenenti dati omogenei.

Ci possono essere vari scopi che motivano l'utilizzo dell'algoritmo in parola: un esempio può essere la necessità di analizzare grandi mole di dati per cercare similitudini altrimenti molto difficili da rilevare diversamente (soprattutto in situazioni nelle quali vi è la costante generazione di nuove informazioni), oppure la generazione di *K* sottoinsiemi di dati omogenei sui quali sarà possibile applicare algoritmi di classificazione che sarebbero, altrimenti, troppo onerosi da gestire. L'algoritmo in parola è conosciuto per essere estremamente efficiente e piuttosto veloce nell'esecuzione; un primo elemento al quale è necessario porre attenzione, però, è il numero di *cluster* in cui si ritiene di dover dividere i dati.

Come si è detto, *K* è il numero di cluster: l'algoritmo, sostanzialmente, dividerà i dati proprio in *K cluster*. Detto parametro è quindi un numero intero, predefinito

dall'utente, a meno delle considerazioni che saranno fatte appresso. Scegliere K=1, pertanto, significa non effettuare alcun raggruppamento: l'algoritmo si limiterà a prendere in input un *dataset* e a raggrupparlo in un unico *cluster* contenente esattamente il numero di dati contenuto nel *dataset* originario.

Del resto, posto che n sia il numero dei componenti del *dataset* di input, scegliere K=n pure non ha alcun senso, perché l'algoritmo genererà tanti *cluster* quanti componenti. Le appena descritte circostanze sono sicuramente estreme, sia nel senso che rappresentano i casi limite possibili nell'utilizzo dell'algoritmo in parola, sia nel senso che nessuno avrebbe alcuna convenienza ad operare simili scelte, ma fanno emergere il tratto più delicato dell'utilizzo dell'algoritmo in parola: la scelta di K. Quando la struttura dei dati in ingresso è nota o, sulla base di alcuni elementi, comunque desumibile, la scelta potrebbe essere meno complessa di quello che si potrebbe immaginare, ma ciò non sempre è vero e, comunque, determinate osservazioni potrebbero condurre a risultati piuttosto diversi, se non ingannevoli.

Per ovviare a questo aspetto (talvolta) problematico, è possibile utilizzare metodi agglomerativi (anche detti *bottom-up*) o divisivi (*top-down*), che differiscono a seconda della logica utilizzata per dividere i dati in input, a partire dalle singole unità e procedendo via via per aggregazioni contenenti sempre più elementi, oppure in senso inverso, partendo dall'intero *dataset* per fermarsi al numero di *cluster* definibile come ottimale. Come prima attività l'algoritmo forma il cosiddetto "spazio dei record", ovvero uno spazio geometrico nel quale ad ogni elemento del *dataset* vengono assegnate delle coordinate.

Se agli elementi di un *dataset* sono associate diverse caratteristiche, lo spazio dei record avrà tante dimensioni quante sono le caratteristiche associate a ogni singolo elemento. Il valore di ogni caratteristica sarà trasformato in una coordinata dell'elemento del *dataset*. Si è detto che l'algoritmo ha come obiettivo la ricerca delle somiglianze degli elementi all'interno di un *dataset*: matematicamente ciò avviene misurando la distanza che vi è tra i punti presenti nello spazio dei record.

Affinché ciò sia possibile, però, le coordinate devono essere confrontabili, ovvero devono essere misurate in grandezze omogenee; per garantire che ciò accada, l'algoritmo trasforma tutti i campi del *dataset* in numeri e procede a normalizzarli, ottenendo così la comparabilità necessaria. Un esempio può essere utile per visualizzare semplicemente quanto suesposto. Prendiamo tre soggetti, Prospero, Otello e Lear, e il peso e l'altezza di ognuno di essi:

Prospero: Altezza = 180 cm; Peso = 80 kg.

Otello: Altezza = 160 cm; Peso = 70 kg.

Lear: Altezza = 190 cm; Peso = 120 kg.

I valori sopra descritti possono essere riportati sotto forma di vettori: Prospero (180,80), Otello (160,70) e Lear (190,120). Riportandoci alle descrizioni di cui sopra, le tre persone sono gli elementi del *dataset* e il peso e l'altezza sono le caratteristiche associate ad ognuna di esse. In questo caso, quindi, lo spazio dei record avrà un aspetto bidimensionale e potrà essere rappresentato su un asse cartesiano.

Una volta rappresentati gli elementi come punti in uno spazio è possibile misurarne la distanza; per farlo, vi sono diverse metodologie, come ad esempio la distanza euclidea, la distanza Manhattan e la distanza di Hamming. L'algoritmo di cui questo paragrafo fornisce una breve analisi è basato sul concetto di centroidi:

punti nello spazio che rappresentano un *cluster* e che corrispondono al punto medio degli elementi ricompresi in esso. Naturalmente non è detto che come centroide venga obbligatoriamente preso un elemento ricompreso nel *dataset* in input, per cui è sicuramente possibile che i punti utilizzati come centroidi siano in realtà punti del tutto nuovi rispetto a quelli dedotti dal *dataset* in input, anche se a volte si vuole intenzionalmente che essi siano scelti fra elementi presi a caso dal *dataset*, come si vedrà in seguito.

Un altro aspetto rilevante è che l'algoritmo in parola è di tipo iterativo: esso compie una serie di operazioni ripetute, sempre uguali, finché non ottiene il risultato voluto. In termini discorsivi, le fasi che vengono ripetute sono le seguenti:

- assegnazione di ogni elemento del *dataset* al *cluster* che contiene il centroide avente la distanza minore rispetto alle coordinate dell'elemento considerato;
- (ri)calcolo del punto medio degli elementi associati al *cluster* e sua elezione come (nuovo) centroide.

Le fasi suddette saranno ripetute fino al raggiungimento di *K cluster*. Può essere assai arduo individuare il corretto numero di *cluster* da cui partire; per ovviare a questo problema esistono diverse modalità di inizializzazione dell'algoritmo fra le quali ricordiamo il *forgy method,* che prende alcuni elementi dal *dataset*, oppure quello del *random partition*, che seleziona casualmente i componenti del *dataset* e li divide in *cluster* da considerare inizialmente.

Un metodo di inizializzazione che ha riscosso molto successo è quello del *K-Means++*, ideato nel 2007 da David Arthur e Sergei Vassilvitskii, il quale cerca di fornire centroidi di partenza quanto più sparpagliati possibile. L'inizializzazione procede come segue:

- scelta a caso del primo centroide fra gli elementi del *dataset*;
- per ogni elemento non posizionato viene calcolata la distanza dal centroide esistente più vicino;
- scelta di un nuovo elemento nel *dataset* che abbia una probabilità proporzionale al quadrato della distanza ed eleggerlo a centroide.

4. Compliance *by default* e *by design*

Il rispetto della normativa sulla privacy è declinato in diversi modi, variabili a seconda della genesi che il sistema considerato ha conosciuto in termini di progettazione delle regole di funzionamento dello stesso. Da quanto si è detto, risulta chiaro che è piuttosto difficile evitare che un software basato su un algoritmo di intelligenza artificiale possa, con assoluta certezza, garantire il non accadimento di un determinato evento come quello della profilazione. Avere, pertanto, un'ottica rispettosa della normativa inerente la *privacy* fin dalle prime fasi di concepimento di un software è sicuramente un elemento di successo molto importante, perché può garantire il non accadimento di determinate analisi dati e/o correlazioni di essi che potrebbero difficilmente essere *compliant* con la normativa di riferimento.

Ciò può essere vero anche a prescindere dalla tipologia di dati trattati, perché attiene alla modalità con la quale questi vengono elaborati, incrociati, analizzati o comunque utilizzati dall'utente. Tale metodologia di approccio è definita *privacy by design*[54]. Nell'approfondire il concetto di *privacy by design* risulta evidente che ciò che differisce rispetto agli approcci adottati in passato non inerisce alle tipologie di strumenti di protezione dei dati utilizzati per garantire la conformità al disposto normativo, quanto alle modalità con le quali questi stessi strumenti sono utilizzati.

Tale concetto è espresso piuttosto chiaramente nella norma europea: l'art. 25[55] del GDPR, infatti, nel parlare di "protezione dei dati fin dalla progettazione"

---

[54] *"The term "Privacy by Design", or its variation "Data Protection by Design", has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions and addressing organisational procedures and business models as well. Although the concept has found its way into legislation as the proposed European General Data Protection Regulation, its concrete implementation remains unclear at the present moment."*, European Union Agency for Network and Information Security (ENISA), *Privacy and Data Protection by Design – from policy to engineering*, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

[55] *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare*

chiarisce come gli strumenti tecnici sono gli stessi previsti nella norma in generale (pseudonimizzazione, minimizzazione, e comunque l'utilizzo di misure tecniche e organizzative adeguate, con tutte le difficoltà interpretative che l'utilizzo del suddetto termine comporta). Il concetto di *privacy by default* non è di certo contrapposto a quello precedentemente esposto, bensì ne costituisce la logica conseguenza al fine di adeguare sistemi già esistenti a logiche normative successive alla loro implementazione.

È sempre la norma suddetta a definire il perimetro del concetto in parola, stabilendo la finalità (non rendere accessibili dati personali a un numero indefinito di persone fisiche) e l'oggetto di attenzione (quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità). La metodologia con la quale il concetto stesso è realizzato è esattamente identica, operativamente parlando, a quella già identificata nella definizione del precedente concetto (l'uso di misure tecniche e organizzative adeguate), a dimostrazione del fatto che non è necessario definire in via normativa la metodologia da seguire passo per passo, quanto lo è garantire il rispetto dei criteri di base della norma stessa.

Potrebbe sembrare, a prima vista, che il concetto stesso di *privacy by design* sia piuttosto pleonastico: sembra ovvio, infatti, che qualsiasi progettista di un sistema o di un *software* dovrebbe tenere conto, fra i vari aspetti, del necessario rispetto della normativa vigente. Ciò su cui il legislatore europeo, con l'emanazione del GDPR, e una certa parte della dottrina del settore in precedenza volevano porre l'attenzione è proprio l'esigenza di affrontare determinate esigenze e darvi una risposta nella fase di progettazione di un sistema, piuttosto che a processo ultimato. In passato, infatti, vi era un deciso disallineamento fra il mondo della progettazione software e quello della *privacy compliance*[56], reso più marcato dalla mancanza di

i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati", art. 25, GDPR.

[56] *"We observed that privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realise privacy by design. While the research community is very active and growing, and*

strumenti che rendessero semplice o, comunque, possibile senza l'utilizzo di un'ingente capacità computazionale il rispetto della privacy fin dalla progettazione.

Per ovviare a questo problema esistono diverse soluzioni, tutte complementari, la cui implementazione è sicuramente non scontata e sono, ad esempio:

1- Il supporto allo sviluppo di nuovi meccanismi di incentivazione per la creazione di soluzioni *privacy-friendly* da parte dei legislatori nazionali, delle agenzie e dei soggetti deputati alla definizione di *standard* operativi;

2- L'adozione di un processo multidisciplinare, per quanto possibile, da parte delle comunità di ricerca nello sviluppo di metodologie *privacy compliant*. Questa soluzione sarebbe sicuramente più efficace se supportata dalle agenzie governative eroganti fondi di ricerca;

3- La collaborazione fra comunità di ricerca e le società di sviluppo *software* per la realizzazione di strumenti che rendano intuitivo e semplice il rispetto della normativa *privacy* in fase di progettazione di un qualsiasi *software*;

4- La diffusione dell'utilizzo di *key server*[57] e di *anonymising relays*[58] nell'implementazione di progetti infrastrutturali, soprattutto se cofinanziati con fondi pubblici;

5- L'inclusione di aspetti legati al rispetto della *privacy* nei processi di formalizzazione di standard tecnici da parte delle agenzie internazionali a ciò deputate;

6- La realizzazione, da parte delle suddette agenzie, di strumenti di interoperabilità fra *tools* di *privacy compliance*.

---

constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice. This gap has to be bridged to achieve successful privacy-friendly design of systems and services and evolve the present state of the art. Further, enforcement of compliance with the regulatory privacy and data protection framework has to become more effective, i.e., better incentives for compliance as well as serious sanctions for non-compliance are needed. Also, privacy-by-design can very much be promoted by suitable standards that should incorporate privacy and data protection features as a general rule", ENISA, *Privacy and Data Protection by Design*, op. cit.

[57] Nell'ambito della crittografia pubblica, si tratta di server che conservano e restituiscono, a chi le chiede, le chiavi pubbliche precaricate dai rispettivi titolari. Un esempio di *key server* è rinvenibile al link seguente: https://keyserver.ubuntu.com/.

[58] Terminale di anonimizzazione, sostanzialmente un dispositivo o un software che riceve un messaggio, lo rende anonimo e lo ritrasmette.

Il processo di realizzazione di un *software* è sicuramente non lineare. Volendoci riferire al modello più classico di sviluppo, ovvero il modello a cascata[59], le fasi di sviluppo sono sei: sviluppo del *concept*, analisi, definizione del *design*, realizzazione, fase di *testing* e valutazione del prodotto finale. In particolare, nelle prime due fasi, per ottenere un *software* che sia *compliant by design*, è fondamentale adottare schemi di definizione del *design* che rendano più semplice la definizione della struttura del programma in fase di ideazione[60].

In ambito *privacy* vi sono alcuni *design patterns*, anche se non sono numerosissimi[61]; in questa sede si ritiene sia opportuno segnalare il lavoro svolto dalla *Berkeley School of Information*, la quale ha pubblicato, tramite il sito https://privacypatterns.org/patterns/, una raccolta sistematica di *design patterns* che affrontano una varietà di casistiche. In combinazione con queste vi sono i sistemi di *Privacy-enhancing technologies*[62] (PETs), che consistono in *tools* che possono essere utilizzati per la risoluzione di specifiche necessità[63].

Le strategie adottate nei *design patterns* possono essere schematizzate come segue:

1- Minimizzazione: la raccolta dati deve essere ristretta quanto più possibile all'indispensabile;

---

[59] A. Adel, A. Bahattab, *A comparison between three SDLC models waterfall model, spiral model, and Incremental/Iterative model,* International Journal of Computer Science Issues (IJCSI), 2015, 12.1, pag. 106.

[60] A design pattern *"provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context"*, E. Gamma, R. Helm, R. Johnson, J. Vlissides, *Design Patterns - Elements of Reusable Object-Oriented Software*, 1995, Boston.

[61] Si veda, sul punto, M. Hafiz., *A collection of privacy design patterns,* Proceedings of the 2006 conference on Pattern languages of programs, 2006, New York, pp. 7:1–7:13; S. Pearson, A. Benameur, *Decision support for design for privacy: A system focused on privacy by policy*, *Privacy and Identity Management for Life*, IFIP International Federation for Information Processing, 2011, volume 352 of IFIP AICT, pag. 283–296.

[62] *"Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."*, G. W. van Blarkom, J. J. Borking, and P. Verhaar., *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents*, College bescherming persoonsgegevens, 2003, capitolo 3, L'Aia, Paesi Bassi, pag. 33–54.

[63] A titolo esemplificativo in questa sede si ritiene opportuno citare *Idemix*, una suite di protocolli crittografici; per info, si veda https://hyperledger-fabric.readthedocs.io/en/release-2.2/idemix.html.

2- Occultamento: i dati personali, come anche le relazioni fra essi, non devono essere visibili da parte di qualsiasi utente;

3- Separazione: i dati personali vanno processati quanto più separatamente possibile, in modo da impedire o rendere molto difficile il ritrovamento di dati appartenenti a una stessa persona in un unico luogo di memorizzazione o processo di analisi;

4- Aggregazione: i dati personali vanno processati al più alto livello di aggregazione possibile, col minor livello di dettaglio possibile, tenuto conto delle informazioni delle quali è necessario tener conto;

5- Informazione: il soggetto al quale i dati personali si riferiscono deve essere adeguatamente informato riguardo alla circostanza che i suddetti siano raccolti e siano oggetto di analisi;

6- Controllo: il soggetto di cui sopra deve mantenere il controllo sui propri dati personali, sia nella fase di analisi che rispetto a quanti dati sono conservati e come ciò avviene;

7- Coercizione: l'effettiva adozione di una *privacy policy* conforme alla normativa in vigore dovrebbe essere obbligatoria per il soggetto che intende realizzare un *software*;

8- Dimostrabilità: il soggetto che raccoglie dati personali è tenuto a dimostrare l'effettivo rispetto della *privacy policy* di cui al punto precedente.

Risulta evidente che le suesposte strategie sono sostanzialmente identiche ai principi sui quali si basa la normativa europea sulla *privacy*. Un breve cenno merita, infine, la discussione portata avanti sia a livello dottrinale che normativo per l'ottenimento di un'*AI* affidabile (ovvero la cosiddetta *trustworthiness*). La *ratio* del GDPR è quella di riconoscere all'interessato che fornisce i propri dati e si vede soggetto a valutazioni che possono incidere anche pesantemente sulla propria vita (si pensi alle valutazioni creditizie o alle assicurazioni sulla vita) il diritto a vedersi spiegate le motivazioni alla base della decisione che lo riguarda.

Ciò è ottenibile in vario modo, e alcune delle soluzioni possibili sono già state enunciate; tuttavia, si parla sempre più insistentemente oltre che di *privacy by*

design di *thrustworthiness by design*[64], per affermare la necessità – sempre più impellente – di avere processi decisionali automatizzati che siano pienamente spiegabili dal sistema che li produce. Ciò, ovviamente, introduce maggiore complessità, poiché oltre ai sistemi di analisi vanno realizzati sistemi di *reporting* che siano effettivamente in grado di adattarsi ai primi e di seguirne le logiche e ci si sta interrogando in che modo sia opportuno fare ciò[65], ma è sempre più chiara la necessità di un cambio di approccio che consenta una maggiore trasparenza e leggibilità dei processi computazionali alla base delle tecnologie di intelligenza artificiale.

[64] Per una efficace disamina si veda R. Hamon, H. Junklewitz, I. Sanchez, G. Malgieri, P. De Hert, *Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, Ieee Computational Intelligence Magazine, 2022, Volume 17 – numero 1, pag. 72-85.

[65] "*Accordingly, in such situations, a DPIA should be necessary: the data controller should describe the data processing, assess the necessity and proportionality of it, analyze risks for data subjects (e.g., risks of discrimination, violation of the right to health, to freedom of thought, of movement, attack to their digital identity, etc.), and seek for the data subjects' opinion on the data processing. This procedure will also imply the description of the logic of the AI-based system, as well as the assessment of its impact on the fundamental rights and freedoms relevant for the application and the ways of mitigating it. Making this report public (at least in some parts), would also significantly help to reach a better level of transparency and justification of AI applications."*, R. Hamon, H. Junklewitz, I. Sanchez, G. Malgieri, P. De Hert, *Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, op. cit.

Capitolo II

Human-machine systems

SOMMARIO: 1. - Intelligenza artificiale ed essere umano nel sistema azienda. - 2. Paradigmi del cambiamento: il *Natural Language Processing*. - 3. Paradigmi del cambiamento: il *Machine Learning*. - 4. Paradigmi del cambiamento: la robotica.

1. *Intelligenza artificiale ed essere umano nel sistema azienda*

Per molto tempo l'obiettivo di una parte della ricerca scientifica è stato, e forse è tuttora, trovare un modo di rendere gli elaboratori informatici più veloci, più capaci di memorizzare informazioni, più performanti in ogni senso; solo di recente, però, con l'avvento di tecnologie di intelligenza artificiale, ci si è posti il problema di rendere questi stessi elaboratori più intelligenti. L'intelligenza, però, non è qualcosa di declinabile solo rispetto a singole persone: in generale, e forse soprattutto in ambito aziendale, si può parlare di intelligenza di gruppi di individui. Di fatto, possiamo definire "intelligenza collettiva" un gruppo di individui che agisce collettivamente in modi che sembrano intelligenti[66].

In altre parole, eserciti, aziende, Paesi, famiglie potrebbero essere tutti esempi di gruppi di persone che lavorano insieme in modi che, almeno il più delle volte, sembrano intelligenti. Negli ultimi anni è stato possibile osservare declinazioni di intelligenza collettiva che non si erano mai viste prima tramite l'implementazione e l'utilizzo di nuove tecnologie. Si pensi a Google, per esempio, la quale ha sistematizzato gli indirizzi delle pagine web create da milioni di persone in tutto il mondo in modo tale che chiunque possa effettuare una ricerca e trovarle semplicemente utilizzando parole chiave, o addirittura una frase di senso compiuto, ottenendo risultati incredibilmente intelligenti.

Oppure si pensi a Wikipedia, tramite la quale migliaia di persone di tutto il mondo hanno potuto creare collettivamente una enciclopedia di alta qualità, quasi

[66] *Artificial Intelligence: implications for business strategy*, T. Malone, 2017, op. cit.

senza nessuna supervisione e, nella maggior parte dei casi, senza nemmeno che fosse necessario pagarle. Questi esempi di intelligenza collettiva ottenuta tramite l'utilizzo di sistemi tecnologici non sono, probabilmente, la fine, ma l'inizio.

La domanda che ci si dovrebbe porre, pertanto, è: ci può essere un modo di combinare computer e persone in modo tale che, insieme, possano agire in modo più intelligente di qualsiasi persona, gruppo di persone o di computer abbia mai fatto finora? Ci sono almeno due possibili risposte a questa domanda: la prima può essere quella di collegare persone l'una all'altra in nuovi modi, in modo tale che queste possano collaborare più efficientemente come gruppo. La seconda, però, è sicuramente quella di combinare persone e computer dotati di intelligenza artificiale.

Nel primo capitolo si è già avuto modo di comprendere meglio il concetto di "intelligenza artificiale" e di approfondire quali compiti questa può svolgere e in che modo ciò può avvenire, ma da un punto di vista economico-gestionale ci si dovrebbe interrogare circa la possibilità di organizzare il lavoro in un'azienda combinando le persone che vi lavorano all'interno e le tecnologie che essa stessa decide di utilizzare all'interno dei propri processi produttivi. A tale combinazione ci si riferisce con il termine di sistemi uomo-macchina (*human-computer systems)*, e l'oggetto del presente capitolo inerisce le modalità con le quali è possibile ricercare l'ottimizzazione di questi sistemi tramite diverse soluzioni di combinazione degli elementi che ne fanno parte.

Le prime due domande alle quali rispondere, nel perseguimento dell'oggetto di ricerca, sono le seguenti: in un sistema del genere quali compiti dovrebbero essere affidati ai computer e quali altri agli esseri umani che ne fanno parte? Inoltre, come si potrebbe prevedere un miglioramento continuo di questi sistemi nel corso del tempo? Per rispondere, è opportuno svolgere alcune osservazioni. Un buon obiettivo è lasciare che le macchine facciano ciò che riescono a fare meglio delle persone, e viceversa. Ad esempio, i computer sono molto più capaci delle persone nel memorizzare grandi quantità di informazioni, come le persone sono

normalmente più capaci dei computer nell'interagire con altre persone tenendo conto del contesto nel quale si trovano.

Ciò evidentemente significa che non è né possibile né corretto sostituire le persone con i computer a prescindere dal compito che va svolto, bensì è necessario ricercare un'organizzazione che consenta a tutti di lavorare al meglio. Si pensi ad esempio al servizio di ricerca Google: in un certo senso, potrebbe essere considerato il sistema di intelligenza artificiale più usato al mondo, a seconda di cosa si intenda per intelligenza artificiale. Questo servizio, però, sarebbe del tutto inutile se non ci fossero persone che creano un contenuto, che è poi l'oggetto di ricerca del sistema summenzionato. Peraltro, l'introduzione del servizio di ricerca di Google ha consentito di ampliare enormemente la quantità di contenuto ricercabile, consentendo la creazione di nuovi posti di lavoro dedicati alla creazione di contenuto, alla ricerca di esso e alla pubblicità in generale.

Un altro esempio può essere il sistema di sicurezza informatica del Computer Science and Artificial Intelligence Laboratory (CSAIL) del Massachussets Institute of Technology (MIT): ai computer è demandato il compito di rilevare attività insolita nella rete proprietaria, mentre alle persone quello di analizzare il tipo di attività rilevata e identificare ciò che è effettivamente da considerare un pericolo e ciò che invece è frutto di un errore di rilevazione. Secondo le rilevazioni dell'istituto in parola, il sistema sopra descritto consente di rilevare il triplo degli attacchi malevoli in più di un sistema basato esclusivamente su computer.

Un'altra modalità di divisione dei compiti è quella di pensare in termini di quattro ruoli chiave che i computer possono ricoprire rispetto a delle persone: quello di strumento, di assistente, di collega e di coordinatore. Il ruolo di strumento è sostanzialmente quello nel quale il computer svolge il compito che gli viene dato sotto la supervisione passo passo della persona. Un esempio possono essere le auto con il *cruise control*, i fogli di testo con funzione di auto completamento oppure i fogli di calcolo.

Moltissime funzioni utilizzate al giorno d'oggi aiutano alcune persone a comunicare con altre persone, consentendo loro di collaborare in modi prima

inimmaginabili. Un ruolo del genere potrebbe essere svolto anche da computer dotati di intelligenza artificiale: pensiamo a programmi utilizzabili da bancari addetti agli uffici prestiti che, sulla base di algoritmi di *credit scoring*, potrebbero fornire un'utile informazione di partenza per decidere se concedere o meno un finanziamento.

Un altro esempio potrebbe essere quello, già menzionato, dell'algoritmo di ricerca sviluppato da Google, nella parte che restituisce una risposta in tempo reale rispetto a quando la persona immette l'oggetto della ricerca. In realtà, affinché ciò sia possibile è necessario che l'algoritmo di Google scansioni e cataloghi continuamente nel proprio database ciò che trova su internet, e questo è più simile al concetto definito dal secondo ruolo: quello dell'assistente. Diversamente dallo strumento, un assistente può svolgere parte del lavoro autonomamente, senza cioè una diretta supervisione della persona; prende maggiori iniziative e può rivestire una partecipazione più attiva nell'aiutare a formulare e risolvere un problema.

Un esempio di questo ruolo è dato dai sistemi di auto a guida semi-autonoma, dato che sono considerabili come assistenti del conducente. Un altro esempio è dato da Watson[67] della IBM: in alcuni casi questo è usato da personale medico come aiuto nella diagnosi di alcuni casi clinici. Preventivamente si è provveduto a svolgere una fase di *training* con una serie molto ampia di casi, così da rendere Watson capace di rilevare specifici elementi riguardanti un particolare caso e di calcolare diverse diagnosi possibili, tutte corredate dagli elementi sui quali queste si basano.

Grazie a questo modo di procedere e di argomentare la diagnosi o le diagnosi proposte, è possibile per lo staff medico avere la massima informazione disponibile circa il processo di elaborazione posto in essere e decidere autonomamente circa la diagnosi che si ritiene valida. Lo staff, inoltre, può formulare ulteriori domande, prima di adottare la decisione finale circa la diagnosi da utilizzare effettivamente. Un altro esempio può essere dato dal sistema *chatbot* utilizzato da KLM Airlines,

[67] Per un approfondimento sulle capacità di Watson, si veda IBM Cloud Education, *Conversational AI*, IBM Cloud Learn Hub, 2020, https://www.ibm.com/cloud/learn/conversational-ai.

il quale combina la capacità del sistema di erogare risposte automatiche nei contesti più semplici alla supervisione di personale in *backoffice* che ha il compito di valutare i casi proposti dal sistema e, se del caso, prendere direttamente il controllo della conversazione scrivendo risposte *ad hoc*.

Il terzo ruolo è quello del collega, ed è il ruolo che vede i computer svolgere compiti che normalmente sono svolti anche da persone. La collaborazione, in questo caso, si fonda sul fatto che, benché i computer siano perfettamente in grado di risolvere da soli alcuni problemi esattamente come potrebbero fare alcune persone, in alcuni casi la soluzione delle fattispecie può essere affidata unicamente ad esseri umani. Un esempio è dato da una compagnia di assicurazioni chiamata *"Lemonade"*: questa consente ai propri clienti di aprire un sinistro tramite app e caricare immediatamente i relativi documenti.

Il sinistro, quindi, viene immediatamente analizzato da un sistema di IA il quale, se non rileva alcuna criticità, chiude positivamente la valutazione del sinistro e mette l'indennizzo in pagamento. Nel caso in cui sia rilevata una criticità, il sinistro viene passato alla gestione di un essere umano. L'ultimo ruolo elencato poc'anzi è quello del coordinatore ed è probabilmente quello che più degli altri ingenera preoccupazione nelle persone; tuttavia, ciò accade molto più spesso di quanto si è portati a pensare. Un esempio banale potrebbe essere quello dei semafori: un computer, sostanzialmente, sta coordinando flussi di persone alla guida di autovetture presso un incrocio senza che nessuno ci trovi qualcosa di strano.

Ci potrebbero essere molti esempi come questo. In generale, come "coordinatore" in questo elaborato ci si riferisce a un diverso tipo di coordinamento, che abbia a che fare con un ambito economico aziendale, come è sicuramente quello di assegnare un compito a un essere umano, addestrarlo a un determinato compito e valutare le sue performance. Un esempio per capire meglio il ruolo in parola è dato da un sistema chiamato "*CrowdForge"*, sviluppato da alcuni ricercatori alla Carnegie Mellon University.

Tramite il sistema da loro ideato riuscivano a coordinare un gruppo di persone affinché potessero scrivere contenuti tecnici, come ad esempio una voce enciclopedica (uno degli esempi scritti con questo sistema è proprio una voce enciclopedica circa New York). In fase di sviluppo, i ricercatori reclutarono persone usando *Amazon Mechanical Turk*, un mercato del lavoro online dove chiunque può offrire il proprio tempo per svolgere *micro-tasks* (compiti estremamente semplici), richiedenti di norma pochi minuti, per un corrispettivo pari a pochi centesimi alla volta.

I ricercatori chiesero prima a tante persone, organizzate indipendentemente per essere un unico gruppo con un solo obiettivo, di strutturare ognuno una piccola parte di un primo schema della suddetta voce enciclopedica: come risultato ottennero lo schema della voce organizzato per paragrafi (cose da vedere, storia della città, *et cetera*). Successivamente, chiesero tramite lo stesso portale surrichiamato di segnalare fatti rilevanti inquadrabili ognuno nelle sezioni dello schema di cui sopra; per ogni sezione, allo stesso modo, considerarono tutto ciò che gli venne segnalato e lo sottoposero ad un terzo gruppo di persone affinché queste sistemassero il tutto in paragrafi.

A questo punto diedero in input tutto quello che avevano raccolto al software ideato, affinché lo sistemasse in un'unica voce enciclopedica. Ottenuto il risultato descritto, lo sottoposero a persone ignare di come questo fosse stato scritto chiedendogli un parere circa la qualità dello stesso; in media, la voce veniva valutata migliore di come avrebbe potuto essere se fosse stata scritta da una singola persona e, complessivamente, paragonabile a una qualsiasi voce di Wikipedia.

L'esempio appena descritto vede alcune persone svolgere parti piccole o piccolissime e molto semplici di un lavoro, mentre un software si occupa di assiemare quanto raccolto e fornirgli un senso di unità, ciò che è di certo più complesso di quello che in questo caso è richiesto alle persone. L'esempio fornito peraltro non costituisce un'applicazione tipica di intelligenza artificiale, ma è in corso lo sviluppo di un sistema che non si occupi solo di fare quanto descritto, ma coordini e strutturi, complessivamente, il lavoro fin dall'inizio, valutando a quali

persone affidare un determinato compito sulla base del risultato di quello svolto in precedenza.

Un diverso esempio è dato da "*Cogito"*, un software utilizzato da persone addette all'assistenza telefonica. *Cogito* è un sistema di intelligenza artificiale che, sulla base del tono di voce utilizzato durante la chiamata, è in grado di rilevare l'umore della persona con la quale si parla, fornendo all'operatore un supporto estremamente importante nel capire come può essere in un determinato momento più opportuno parlare con il proprio interlocutore. In più, questo sistema riesce a valutare l'operato del telefonista sulla base di quanto riesce a creare una connessione emotiva con il proprio interlocutore, fungendo anche da valutatore della prestazione lavorativa – e quindi rientrando nel ruolo in parola.

La seconda domanda che ci si è posti è come migliorare nel tempo i sistemi uomo-macchina. Mentre negli anni Novanta, coloro i quali decidevano di porre in essere un processo di *Business Process Reengineering* cercavano di prendere scelte che potessero rimanere invariate per il maggior tempo possibile, con l'intelligenza artificiale, a causa della velocità con la quale questi sistemi migliorano nel tempo, è inevitabile valutare costantemente l'organizzazione adottata. Il sistema uomo-macchina così concepito è perciò qualcosa in continuo divenire, che impara dall'esperienza ad essere migliore, e ciò può accadere almeno in tre modi. Il primo vede gli esseri umani analizzare come possono migliorare i compiti che svolgono, un po' come avviene in una riprogettazione organizzativa, quando ci si rende conto che alcune operazioni non portano valore e si decide di eliminarle.

Il secondo modo consiste dal miglioramento informatico apportato ai computer, come fanno gli ingegneri Google ogni volta che migliorano gli algoritmi di ricerca utilizzati dal motore. Il terzo modo è fare in modo che i computer possano imparare da loro stessi con l'esperienza, similmente a come accade con l'implementazione di tecniche di *Machine Learning*. Volendo tornare al sistema *chatbot* di KLM menzionato in un precedente esempio, quando l'operatore decide di rispondere diversamente da come avrebbe fatto il sistema questo analizza la risposta fornita,

per cercare di adattare il proprio comportamento e non compiere una seconda volta lo stesso errore[68].

In conclusione, l'organizzazione fra esseri umani e computer dotati di intelligenza artificiale può essere cruciale per consentire implementazioni di successo della tecnologia in parola nelle fasi di produzione di un'azienda, come nelle infrastrutture di una città o, in generale, in qualsiasi sistema socioeconomico suscettibile di miglioramento.

2. *Paradigmi del cambiamento: il Machine Learning*

La tecnica del *Machine Learning* comprende al suo interno un vastissimo numero di applicazioni[69]. Per i dettagli tecnici circa le funzionalità e i possibili obiettivi ottenibili grazie al suo impiego si rimanda a quanto già dettagliato nel corso del primo capitolo del presente elaborato. Le applicazioni industriali, come si può intuire, sono molteplici; peraltro il *Machine Learning* è alla base di tutta una serie di funzioni che, altrimenti, sarebbero eccessivamente onerose da implementare in codice secondo tecniche di programmazione "tradizionali", se non del tutto impossibili[70]. In ambito aziendale si conoscono essenzialmente due modi principali di avvantaggiarsi del *ML*: l'analisi di dati costituenti

[68] "*Augmented intelligence, not artificial intelligence, is the way forward. This philosophy is endorsed by the United Services Automobile Association's (USAA) virtual assistant. Employees at the USAA create answers to members' questions, which are logged in the libraries. When a customer asks a question, the chatbot searches the libraries. If the answer is there, the chatbot will deliver it. If not, the chatbot will refer the customer to a human assistant. Barclays Bank are of the same view. The debate is no longer about humans versus AI. The issue is about integrating both so that customers will receive a seamless service. Debates and discussions about AI have become more popular in the media in the past few months. They are essential to educate and inform the public, remove the fear factor of AI and improve transparency in AI. Training robots and chatbots is equally important to provide a personalised, seamless and efficient customer experience."*, A. Lui, G. W. Lamb, *Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector*, Information & Communications Technology Law, 2018, 27:3, pag. 267-283.

[69] In questo elaborato viene trascurata l'analisi di tecniche di *Deep Learning*; per alcune possibili applicazioni si veda B. Marr, *What Is Deep Learning AI? A Simple Guide With 8 Practical Examples*, Forbes, 2018, https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/#52f9a1f8d4ba.

[70] Il numero dei campi nei quali è possibile avvantaggiarsi della tecnologia in parola è in continuo aumento. Per una applicazione nel campo della psicologia si veda N. DuVergne Smith, *New AI tool improves cognitive testing,* MIT News, 2017, https://news.mit.edu/2017/new-ai-tool-improves-cognitive-testing-0310.

un'immagine[71], un suono, o comunque parte di un contesto, anche in senso dinamico (in tempo reale, si pensi ad un'automobile o ad un robot che devono muoversi in uno spazio popolato da oggetti/persone[72]) e l'analisi di dati finalizzata a predire un determinato elemento[73] o risultato, molto diffusa soprattutto nel campo della finanza[74].

Proprio in questo campo è possibile analizzare alcuni utilizzi del *ML* particolarmente interessanti. Si consideri, in particolare, il mercato del credito al consumo e, ancora più nello specifico, quello delle carte di credito c.d. "*revolving"*[75]. Sostanzialmente è molto semplice comprendere quanto la possibile insolvenza del titolare della carta di credito, in particolare se si considera il funzionamento di simili carte di credito, possa essere pericolosa per l'istituto emittente[76]. Normalmente, per valutare il merito creditizio del richiedente la carta *revolving*, gli istituti di credito utilizzano un indice di merito, il quale tiene conto di una serie di fattori (reddito, patrimonio, storia creditizia *et cetera*).

---

[71] Vi sono innumerevoli esempi in merito, ma uno certamente dei più innovativi è quello seguito da *Stitch Fix* in tema di abbigliamento; si veda K. Lake, *Stitch Fix's CEO on Selling Personal Style to the Mass Market*, Harvard Business Review, 2018, https://hbr.org/2018/05/stitch-fixs-ceo-on-selling-personal-style-to-the-mass-market. Si veda anche WBR Insights, *How Stitch Fix Uses Data Science and Machine Learning to Deliver Personalization at Scale*, eTail, 2019, https://etailwest.wbresearch.com/blog/how-stitch-fix-uses-data-science-and-machine-learning-to-deliver-personalization-at-scale.

[72] Si veda in merito R. Wile, *Wall Street Loves This Gadget That's Bringing The World Closer To Self-Driving Cars — Here's How It Works*, Business Insider, 2014, https://www.businessinsider.com/how-mobileye-technology-works-2014-8?r=US&IR=T.

[73] L'oggetto di analisi può essere estremamente vario; può trattarsi, ad esempio, delle preferenze di un utente. In merito, si veda C. A. Gomez-Uribe, N. Hunt, *The Netflix Recommender System: Algorithms, Business Value, and Innovation*, ACM Trans. Manage. Inf. Syst., 2016, 6, 4, Articolo n. 13, 19 pagine.

[74] E non solo; fra le molteplici applicazioni possibili si veda E. Woyke, *Crystal Ball for Corn Crop Yields Will Revolutionize Commodity Trading*, Technology Review, 2016, https://www.technologyreview.com/2016/08/09/70472/crystal-ball-for-corn-crop-yields-will-revolutionize-commodity-trading/.

[75] La carta di credito è ciò "*che permette al titolare di acquistare (tramite POS) beni e servizi presso qualsiasi esercizio commerciale aderente al circuito al quale la carta è abilitata o di prelevare contante (tramite ATM) con addebito posticipato. Le operazioni prevedono generalmente un massimale di utilizzo (il cosiddetto plafond) definito nel contratto. Il titolare della carta, a seconda del contratto e del tipo di carta di credito, pagherà in un'unica soluzione, di solito ogni mese con addebito sul conto corrente ("carta di credito classica" o "charge"), oppure a rate, con gli interessi ("carta di credito revolving")*", Glossario della Banca d'Italia, 2022, https://economiapertutti.bancaditalia.it/glossario/index.html?letter=C&word=credito.

[76] Si tratta di un'attività di estrema delicatezza per gli istituti di credito tradizionali e non; si veda, in merito, E. Knorr, *How PayPal beats the bad guys with machine learning*, Infoworld, 2015, https://www.infoworld.com/article/2907877/how-paypal-reduces-fraud-with-machine-learning.html.

Naturalmente si tratta di indici che, sebbene aggiornati periodicamente, servono ad effettuare una valutazione in un determinato momento, non riuscendo bene a valutare cambiamenti abbastanza velocemente per fungere da campanello di allarme al cambiamento della situazione di partenza. Si consideri il grafico che segue:

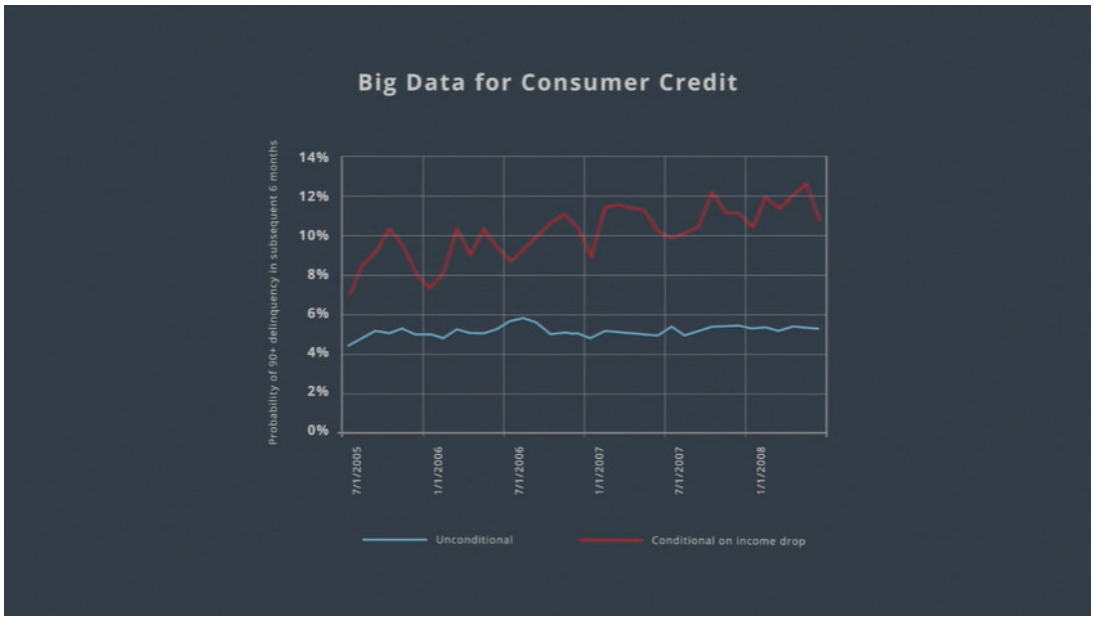
È possibile notare come, al passare degli anni (2005, 2006, 2007 e 2008) la valutazione del merito è sostanzialmente simile a quella dell'anno precedente. Ciò accade perché questo tipo di punteggi di merito è sostanzialmente poco variabile a fattori contingenti, che però possono modificare anche sostanzialmente la possibilità di insolvenza dovuta a crisi o frode del debitore. Per ovviare alle inefficienze appena descritte è stato sviluppato un software basato su *ML*[77] che ha preso in analisi un considerevole *dataset*[78] di informazioni riferite a transazioni finanziarie.

Questa analisi ha avuto la funzione di consentire l'addestramento del software, onde consentirgli di riconoscere potenziali situazioni di default basandosi su dati già verificati e conosciuti (sostanzialmente, i dati in parola hanno costituito un

[77] Si veda A. E. Khandani, A. J. Kim, A. Lo, *Consumer credit-risk models via machine-learning algorithms*, Journal of Banking and Finance, 2010, vol. 34, issue 11, pp. 2767-2787.

[78] Per dare un'idea della quantità di dati analizzati basti pensare che lo 1% corrisponde a circa 10 terabyte di dati.

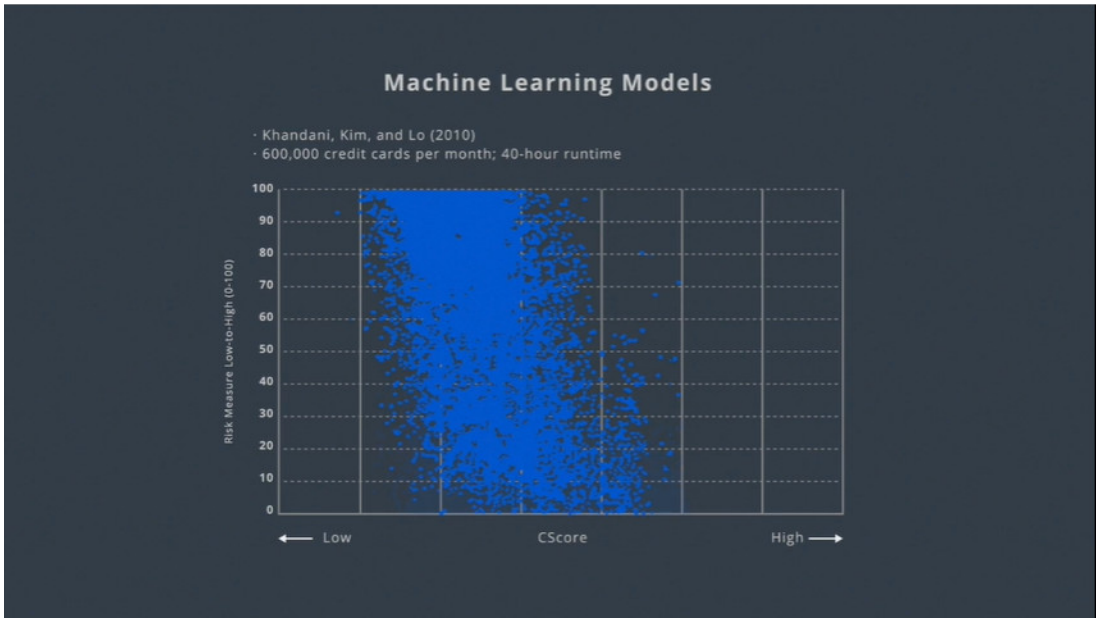
training set sulla base del quale costruire il sistema di analisi e riconoscimento del software di *ML*). Il risultato ottenuto è spiegato efficacemente dal seguente grafico:



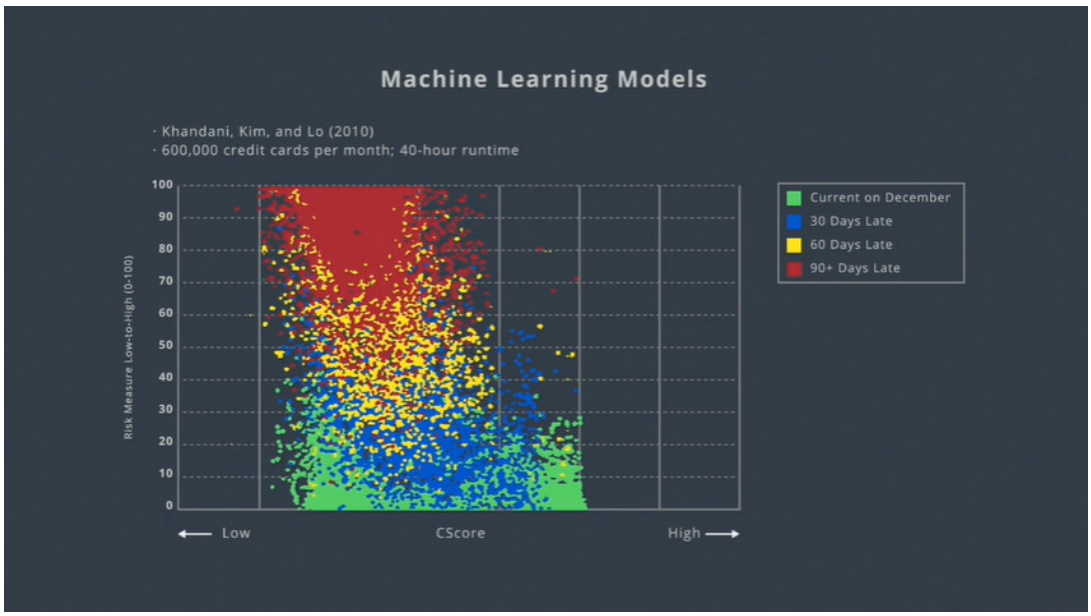
Nel grafico, il segmento di colore azzurro (*unconditional*) rappresenta il numero di intestatari di carte di credito con una probabilità di insolvenza nei successivi 6 mesi pari o maggiore del 90%, senza nessuna particolare selezione. Il segmento di colore rosso (*conditional on income drop*), invece, rappresenta la probabilità di insolvenza degli intestatari che hanno subito discontinuità nei propri incassi nell'arco dei 30 giorni precedenti al momento della valutazione.

È possibile osservare la concreta differenza fra i due segmenti, sia in termini di andamento che in termini di quantità di soggetti la cui insolvenza avverrà quasi certamente; un'analisi del genere, che tiene conto di dati precedenti di soli 30 giorni, sarebbe impossibile da condurre semplicemente con un indice o con un sistema di indici finanziari, data la natura sostanzialmente statica del procedimento di valutazione che queste tecniche comportano. La tecnologia in parola, per di più, consente di analizzare enormi quantità di dati: sono state oggetto di analisi le movimentazioni delle carte di credito di più di 600.000 titolari per ogni mese, ciò che dimostra quanto questa tecnologia possa cambiare il modo in cui le aziende possono assumere decisioni in situazioni critiche.

Ad ulteriore conferma dell'accuratezza della tecnica in parola si consideri il grafico seguente:



Nel grafico ogni punto ha, naturalmente, due coordinate: il *credit score* assegnato ad un particolare intestatario di una carta di credito, sull'asse delle ascisse, e la previsione del rischio di insolvenza secondo il software di *ML* su quello delle ordinate. Si confrontino i dati ottenuti *ex post*, basati sugli eventi di insolvenza effettivamente verificatisi:



Nel grafico sono rappresentati gli intestatari che, nel corso dei sei mesi successivi all'analisi, non sono mai stati insolventi; in blu quelli che hanno avuto

un ritardo di 30 giorni, in giallo di 60 e in rosso quelli che hanno avuto un ritardo nel pagamento superiore a 90 giorni o più. Da questa immagine risulta di tutta evidenza come, basandosi solo sul punteggio *CScore*, alcune persone avrebbero potuto avere scarso o nessun accesso al credito, pur essendo affidabili, mentre altre considerate affidabili sono invece state insolventi.

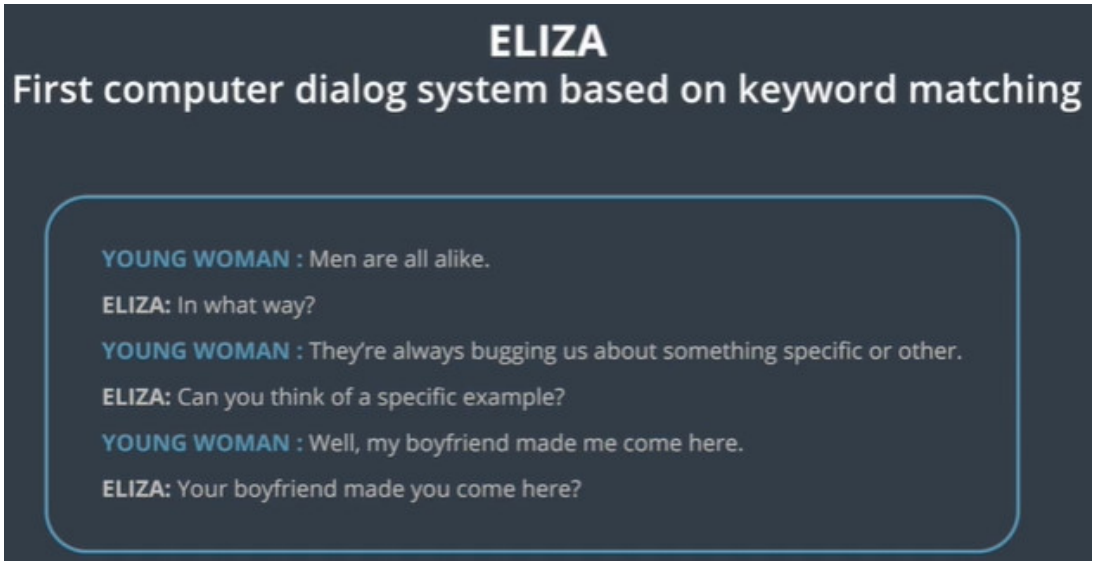
Quanto detto viene capovolto se guardiamo la misurazione del rischio di insolvenza basata sull'algoritmo di *ML*: è facile notare come questo abbia performato estremamente bene in un arco temporale di sei mesi, considerando rischiosi soggetti poi verificatisi effettivamente insolventi e, al contempo, sicuri intestatari che non hanno avuto fenomeni di insolvenza. Ci sono molte altre applicazioni di questo tipo che sfruttano il *ML* per verificare la probabilità che un fenomeno accada o meno[79], ma si ritiene che quella esposta rappresenti efficacemente i punti forti della tecnologia in analisi.

3. *Paradigmi del cambiamento: il Natural Language Processing*

Il *Natural Language Processing*, ovvero l'elaborazione del linguaggio naturale, è una branca di studio dell'intelligenza artificiale che si occupa di sviluppare sistemi che consentano ad un computer di comprendere correttamente il linguaggio utilizzato da un essere umano. La centralità dello sviluppo di tecniche adatte a rendere possibile ad una macchina la comprensione corretta del linguaggio umano è stata da subito evidente: lo stesso Turing, negli anni Cinquanta, cercò di definire un computer intelligente come qualcosa di capace di sostenere una conversazione con un essere umano senza che questo si rendesse conto di parlare con qualcuno di diverso da un essere umano. Tuttavia, bisognerebbe chiedersi preliminarmente cosa si intende per "comprensione".

[79] Si veda, ad esempio, K. Sato, *Using machine learning for insurance pricing optimization*, Google Cloud, 2017, https://cloud.google.com/blog/products/gcp/using-machine-learning-for-insurance-pricing-optimization.

Qualsiasi persona che abbia un cane sa perfettamente che esso non è in grado di comprendere parola per parola ciò che gli viene detto; benché esista una sorta di dialogo fra essere umano e animale, non è sempre possibile capire cosa questo abbia effettivamente compreso e cosa no. Nel 1966 Joseph Weizenbaum sviluppò un programma che chiamò "Eliza" in grado di dare l'impressione, in un qualsiasi dialogo, di comprendere cosa l'interlocutore stesse dicendo:



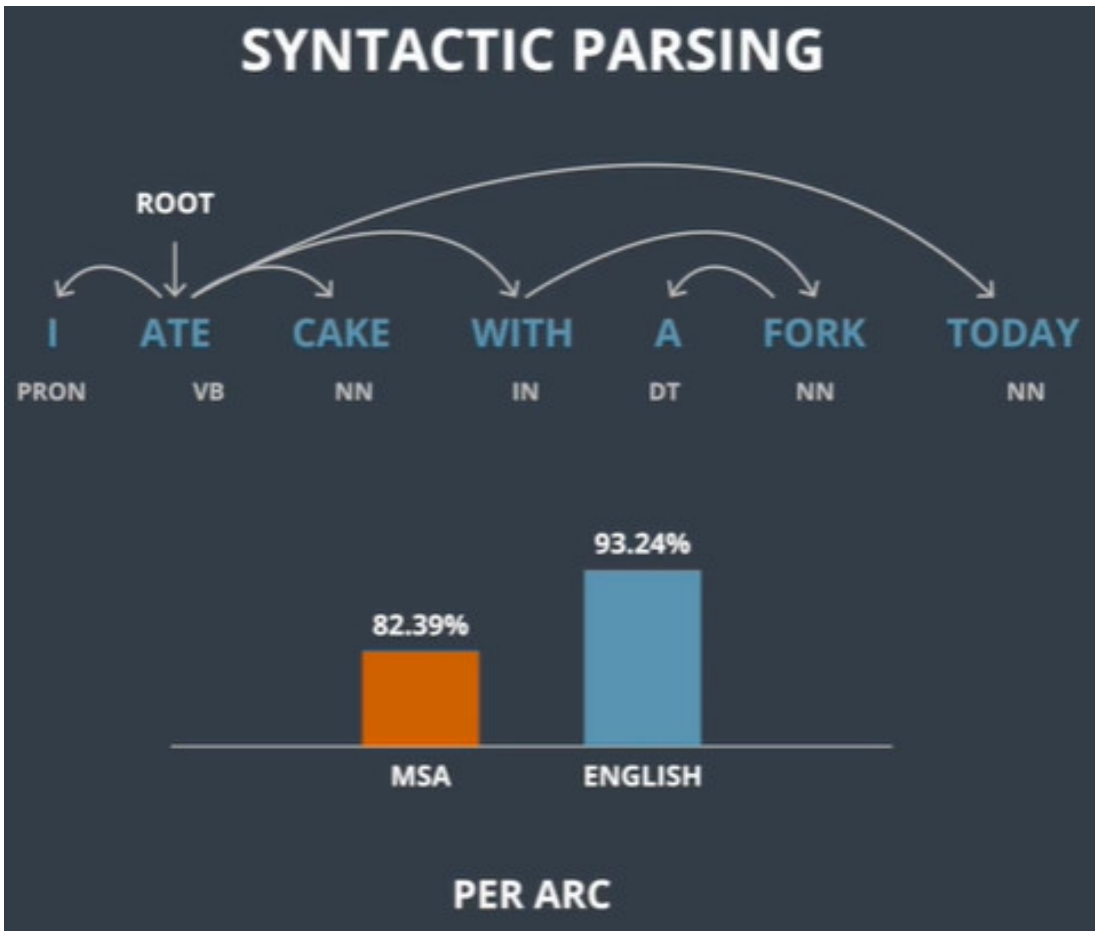
In sostanza, il programma non era assolutamente in grado di comprendere ciò che gli veniva detto ma, tramite l'utilizzo (e il riutilizzo) di parole usate dal suo interlocutore umano riusciva ugualmente a portare avanti una conversazione, almeno nelle fasi iniziali. Anche nell'era attuale vi sono alcune funzioni che le macchine riescono a svolgere con un grado di accuratezza estremamente elevato, mentre ve ne sono altre che risultano ancora appannaggio di esseri umani; non sempre, peraltro, la complessità del compito dice qualcosa circa ciò che una macchina è in grado o non è in grado di fare. Come già illustrato nel primo capitolo

in tema di *machine learning*, la macchina svolge una serie di analisi statistiche tali per le quali riesce, tramite l'utilizzo di una funzione matematica, a far corrispondere una determinata cosa ad un'altra. Il *NLP* non fa eccezione: non si tratta di comprendere qualcosa nel senso che un essere umano immaginerebbe, quanto piuttosto della possibilità di ricondurre o meno il compito da svolgere a una funzione statistica.

Al momento in cui si scrive, le tecnologie di *NLP* sono perfettamente in grado di svolgere compiti quali quello della *sentiment analysis*, ovvero rilevare quali sono le emozioni (positive o negative) espresse in un testo. Un altro compito che ha conosciuto un netto miglioramento rispetto al passato è quello della traduzione da una lingua ad un'altra, anche quando la struttura grammaticale e sintattica degli idiomi di partenza è estremamente diversa.

Il dialogo "naturale" fra uomo e macchina, invece, risulta ancora estremamente lontano, dal momento che anche la domanda più semplice può ingenerare forti difficoltà alla macchina. Guardando più nel dettaglio, ad esempio, la tecnologia *NLP* nel contesto della traduzione da una lingua a un'altra, uno degli elementi di base più importanti (ed utili anche nello svolgimento di altri compiti) risulta essere la comprensione della struttura grammaticale di una frase (l'identificazione di cosa è un verbo, cosa un soggetto e cosa un complemento oggetto).

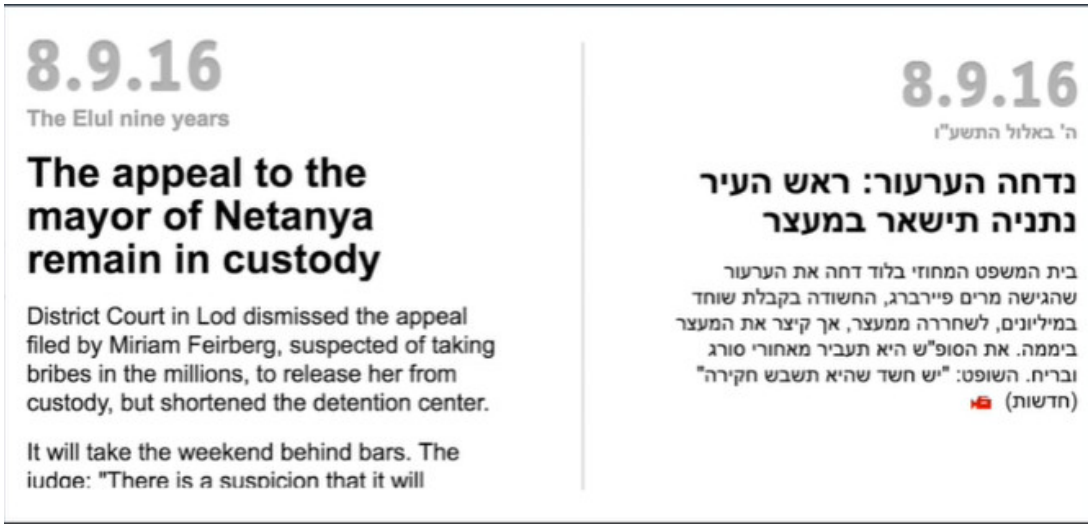
In questo compito la tecnologia oggi utilizzata è estremamente affidabile:



Come si vede, nel caso della lingua inglese l'affidabilità è superiore al 90% e anche nel caso dell'arabo standard (*modern standard arabic*), sebbene questa si attesti poco al di sopra del 80%, risulta comunque estremamente buona, data la complessità e la totale diversità dell'idioma considerato rispetto a quello della lingua inglese.

Ciò sta a significare che le metodologie utilizzate riescono a generalizzare piuttosto bene, quasi indipendentemente dalla complessità del compito assegnato. Ciò detto, se si analizza in concreto la traduzione di un testo ci si rende conto che la tecnologia ha ancora risultati altalenanti a seconda di ciò che le si chiede di tradurre.

Si guardi, ad esempio, la traduzione di una notizia dall'ebraico all'inglese:



8.9.16

The Elul nine years

The appeal to the mayor of Netanya remain in custody

District Court in Lod dismissed the appeal filed by Miriam Feirberg, suspected of taking bribes in the millions, to release her from custody, but shortened the detention center.

It will take the weekend behind bars. The judge: "There is a suspicion that it will

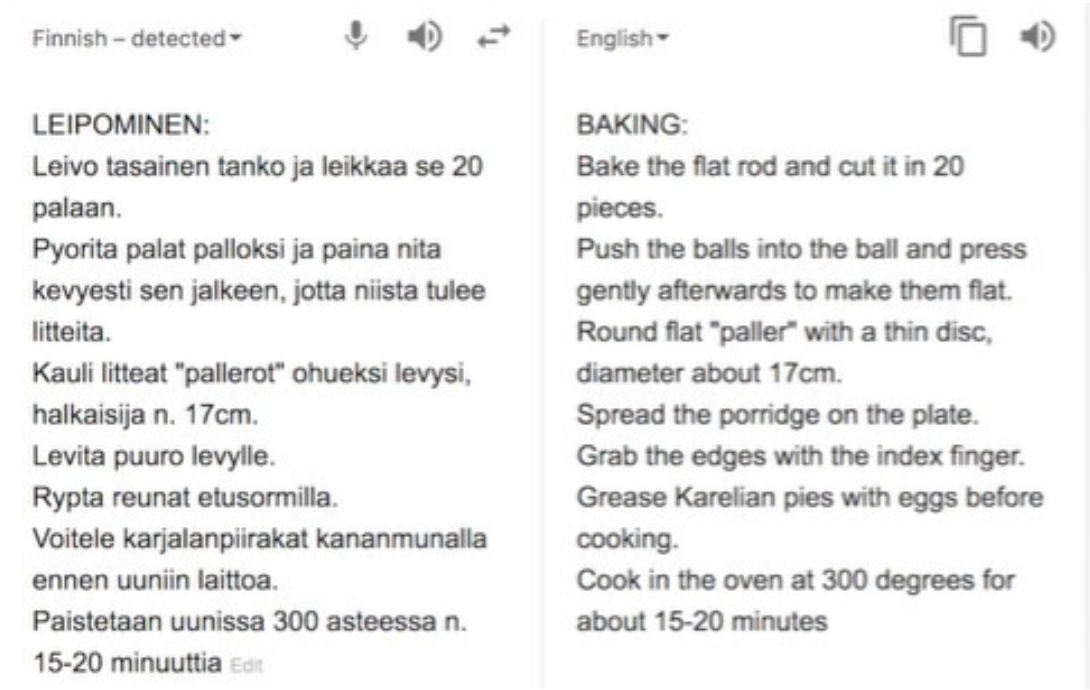
8.9.16

ה' באלול התשע"ו

נדחה הערעור: ראש העיר נתניה תישאר במעצר

בית המשפט המחוזי בלוד דחה את הערעור שהגישה מרים פיירברג, החשודה בקבלת שוחד במיליונים, לשחררה ממעצר, אך קיצר את המעצר ביממה. את הסופ"ש היא תעביר מאחורי סורג ובריח. השופט: "יש חשד שהיא תשבש חקירה" (חדשות)

La notizia, benché sia tradotta in un idioma assai differente da quello di partenza, risulta comunque comprensibile al lettore per la massima parte[80]. Si guardi invece l'esempio della traduzione di una ricetta di cucina dal finlandese all'inglese:



Finnish – detected

LEIPOMINEN:
Leivo tasainen tanko ja leikkaa se 20 palaan.
Pyorita palat palloksi ja paina nita kevyesti sen jalkeen, jotta niista tulee litteita.
Kauli litteat "pallerot" ohueksi levysi, halkaisija n. 17cm.
Levita puuro levylle.
Rypta reunat etusormilla.
Voitele karjalanpiirakat kananmunalla ennen uuniin laittoa.
Paistetaan uunissa 300 asteessa n. 15-20 minuuttia Edit

English

BAKING:
Bake the flat rod and cut it in 20 pieces.
Push the balls into the ball and press gently afterwards to make them flat.
Round flat "paller" with a thin disc, diameter about 17cm.
Spread the porridge on the plate.
Grab the edges with the index finger.
Grease Karelian pies with eggs before cooking.
Cook in the oven at 300 degrees for about 15-20 minutes

Il risultato è assai meno soddisfacente, eppure in termini di complessità non c'è alcun paragone possibile: la notizia vede l'utilizzo di termini complessi e specifici,

[80] Si veda *Narrative Science Employs Natural Language Generation*, nAnalyze, 2017, https://www.nanalyze.com/2017/01/narrative-science-natural-language-generation/.

di frasi complesse e di concetti diversi, mentre la ricetta è composta da termini semplici, da frasi molto brevi e da un elenco di istruzioni. La motivazione del perché ciò accade è da ricercarsi nel *training* sul quale la tecnologia utilizzata si basa: essa, infatti, è stata implementata tramite l'utilizzo massiccio di notizie espresse in molteplici linguaggi, non di ricette, per cui sa riconoscere molto meglio le prime rispetto alle seconde non perché le capisca, ma perché il modello è "fittato" in questo senso.

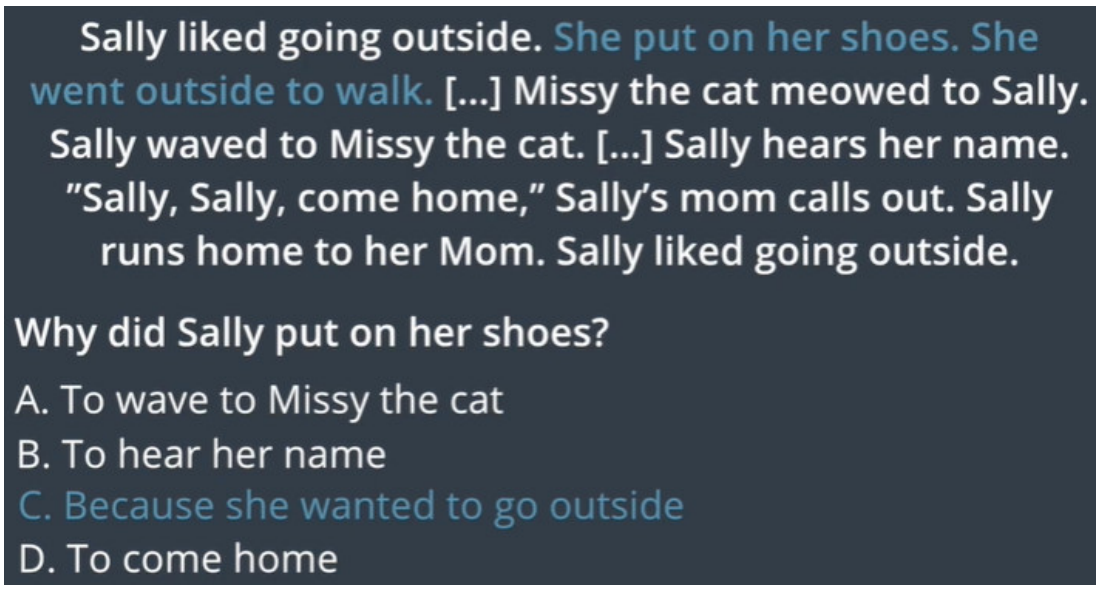
Un diverso esempio può essere dato dalla performance ottenuta da Watson[81] della IBM nel programma Jeopardy nel 2011: il computer sembrava riuscire a rispondere perfettamente alle domande del programma, peraltro piuttosto difficili per una persona di cultura media. Ciò generava negli spettatori l'impressione che la macchina potesse "capire" e rispondere in modo proprio, ovvero sostenere un dialogo.

La realtà è diversa: spesso, le domande che venivano poste alla macchina erano sufficientemente precise da poter essere utilizzate come base della risposta senza una particolare elaborazione. Alla domanda "L'opera di *William Wilkinson* chiamata *An Account of the Principalities of Wallachia and Moldavia* ha inspirato il racconto più famoso di quale autore?" la macchina rispose correttamente "Bram Stoker" non perché avesse compreso la domanda nel senso comune del termine "comprendere", ma perché si tratta di qualcosa alla quale è possibile dare una risposta sulla base di una ricerca in un database, per quanto ricco e sofisticato.

Ecco come quindi la comprensione di un testo nelle sue parti essenziali, combinata ad una ricerca in un database contenente un sufficiente set di informazioni, riescono a dare la sensazione di un processo cognitivo vero e proprio. Di per contro, questa sensazione viene completamente meno quando la domanda non è traducibile in un processo di ricerca, ma implica obbligatoriamente un processo razionale.

[81] Per un approfondimento si veda *Natural Language Understanding*, IBM Cloud, 2020, https://natural-language-understanding-demo.ng.bluemix.net/?cm_mc_uid=61913652150015064305656&cm_mc_sid_50200000=1508796017&cm_mc_sid_52640000=1508796017.

Un buon esempio è quello che segue:



La risposta "C", mentre è praticamente ovvia per qualsiasi bambino di circa sette anni, per un computer può essere estremamente difficile: questo tipo di domande ottiene risposta corretta solo il 71% delle volte[82]. In termini più tecnici, è possibile descrivere il funzionamento di un sistema *NLP* descrivendolo come un problema di classificazione supervisionata.

Si pensi ad un classificatore che debba rilevare se una determinata frase sia classificabile o meno come una frase nominale. L'esito della classificazione è di tipo binario (si oppure no), ciò che costituirà quanto è chiamato *prediction*. Per rispondere, il sistema *NLP* deve orientarsi sulla base delle caratteristiche (*feature*) che compongono la frase da analizzare.

Si può immaginare questo meccanismo come una serie di domande alle quali il sistema può rispondere in modo binario, come ad esempio "nella frase è presente un verbo?" oppure "la frase è del tutto nuova?"; le risposte fornite alle frasi suddette saranno traducibili in 0 o in 1 a seconda della risposta fornita e andranno a formare un vettore (*feature vector*) che sostanzialmente riepilogherà le caratteristiche della frase in esame in termini vettoriali. Si immagini la frase nominale "a casa": la risposta alla prima domanda è "no", quindi "0", mentre

[82] *Artificial Intelligence: Implications for business strategy*, modulo 3, R. Barzilay, MIT-CSAIL, 2017.

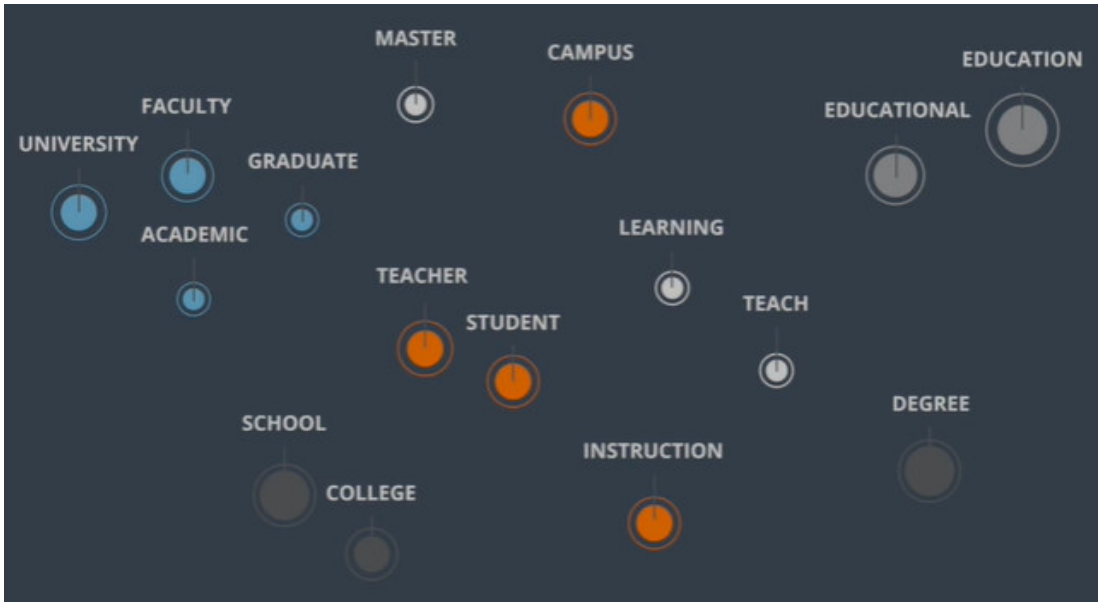
quella alla seconda potrebbe essere si o no a seconda delle frasi già analizzate dal sistema (poniamo sia "si", quindi "1"). Il vettore rappresentativo della frase nominale sarà (0,1).

Maggiore sarà la quantità di domande necessarie, maggiore sarà lo spazio dimensionale all'interno del quale sarà possibile rappresentare la posizione della frase in analisi e, di conseguenza, il risultato della classificazione. Un esempio di come, praticamente, ciò abbia aiutato a risolvere un problema di natura pratica è dato dal sistema implementato dalla prof.ssa Regina Barzilay presso il Massachussets General Hospital[83] finalizzato alla velocizzazione della rilevazione di possibili tumori. In particolare, il sistema è in grado di analizzare autonomamente un referto patologico partendo dal documento scritto dal personale medico, senza quindi bisogno che questo sia preventivamente oggetto di una schematizzazione da parte di personale qualificato.

Il sistema funziona grazie alla capacità di rilevare se una serie di termini sia effettivamente o meno presente nel referto, adottando il sistema riepilogato nell'esempio di cui sopra. La tecnologia in parola è stata in grado, analizzando oltre 50.000 referti, di ottenere una accuratezza del 96%, riducendo drasticamente i tempi di diagnosi di cancro al seno.

Il limite di questo approccio è dato dalla difficoltà con la quale la macchina riesce a tenere conto del contesto: con questo sistema, le parole "pera" e "mela" sono altrettanto diverse quanto le parole "cane" e "mela". Tale limite è superabile con la metodologia conosciuta come *deep learning*, la quale consente di ricondurre a dimensioni inferiori ciò che, per essere rappresentato con la tecnologia precedentemente descritta, avrebbe bisogno di un numero molto maggiore di dimensioni, ottenendo peraltro una rappresentazione delle possibili correlazioni riscontrabili fra termini prima considerati solo diversi.

[83] Sulla base di detto sistema, la prof.ssa Barzilay è stata insignita del premio "Squirrel AI Award" nel 2020, vincendo un premio di un milone di dollari.



In questo modo è possibile ottenere una comprensione del testo notevolmente maggiore rispetto alla metodologia applicata in precedenza, dato che ora è possibile tenere conto del contesto. Peraltro, lo stesso risultato è ottenibile sulla base di frasi, invece che di singole parole, ciò che rende di immediata comprensione perché questo sistema consenta di ottenere risultati più precisi del precedente. Il *NLP* ha diverse applicazioni a livello aziendale[84]: in un *call center*[85], ad esempio, può essere utilizzato per migliorare il livello del servizio offerto facendo da primo centro di smistamento[86].

L'attività svolta in un *call center*, quando è di natura complessa, ovvero funge da interfaccia con il cliente a trecentosessanta gradi, comprendendo tutte le possibili funzioni aziendali, da quella commerciale a quella di assistenza post-vendita, deve bilanciare adeguatamente il costo del servizio e il suo ritorno atteso:

[84] Per una introduzione in campo medico, si veda P. M. Nadkarni, L. Ohno-Machado, W. W. Chapman, *Natural language processing: an introduction*, Journal of the American Medical Informatics Association (JAMIA), 2011, Volume 18, edizione quinta, pag. 544–551.

[85] Si veda anche P. Olson, *This Startup's Artificial Voice Sounds Almost Indistinguishable From A Human's*, Forbes, 2017, https://www.forbes.com/sites/parmyolson/2017/11/03/this-startups-artificial-voice-sounds-almost-indistinguishable-from-a-humans/#69cfb3cc388c.

[86] Ci sono anche applicazioni di segreteria, simili a quella analizzata in seguito; si veda B. Popper, *The smart bots are coming and this one is brilliant*, The Verge, 2016, https://www.theverge.com/2016/4/7/11380470/amy-personal-digital-assistant-bot-ai-conversational.

una delle sfide alle quali l'impresa si trova è la ricerca del mix corretto di personale ed efficienza del servizio[87].

In questo, il *NLP* consente di fare una prima scrematura del chiamante, per individuare la persona corretta con la quale interfacciarlo, consentendo una più veloce risoluzione delle necessità che possono essere soddisfatte più semplicemente e un'attesa ragionevole agli utenti con necessità più complesse. In aggiunta, una volta stabilito che un determinato utente necessita di un'assistenza da parte di un addetto, il sistema può fornire all'operatore tutte le informazioni che ha raccolto (direttamente, tramite le domande poste, o indirettamente, tramite informazioni già presenti o comunque desumibili implicitamente dalle risposte ottenute) nella fase iniziale di scrematura, garantendo in questo modo un set di informazioni di partenza sicuramente più completo di quello che sarebbe possibile avere senza l'impiego della tecnologia in analisi.

Un sistema di questo tipo è in realtà composto da tre tecnologie fondamentali, di cui quella in analisi costituisce il cuore: la prima è il riconoscimento del linguaggio, necessario per trasformare l'informazione parlata in qualcosa di elaborabile dalla macchina; la seconda è proprio il *NLP*, necessario per trasformare il senso di quanto trasformato in contenuto elaborabile, ovvero il significato di ciò che un determinato utente ha detto[88]; la terza è costituita da un sistema di recupero dell'informazione, al quale è demandato il compito di cercare il contenuto necessario a soddisfare il bisogno del cliente al telefono.

Quest'ultima funzionalità è quella sulla quale è necessario compiere un'attività di configurazione più attenta, dato che non tutto è ricercabile semplicemente: un esempio che può aiutare a capire quanto affermato può essere ottenuto analizzando

[87] Si veda J. Goodman, *Get used to virtual assistants in business life*, Raconteur, 2016, https://www.raconteur.net/get-used-to-virtual-assistants-in-business-life/. In merito si veda anche C. Brown, *How To Use Digital Virtual Assistants In Your Startup*, Forbes, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/03/12/how-to-use-digital-virtual-assistants-in-your-startup/#7837899e1071.

[88] Sostanzialmente il software deve essere in grado, più che di compiere un'analisi sintattica (circa la correttezza formale di una frase), di apprezzare in qualche modo la semantica, ovvero il rapporto tra il significante e il significato di ciascun elemento e le relazioni reciproche tra i vari significati di una determinata fase cronologica.

ancora una volta il comportamento di Google Search. Se l'oggetto di ricerca è un fatto, qualcosa di preciso qualitativamente e/o quantitativamente (la data in cui è terminata la seconda guerra mondiale, oppure quanti negozi ci sono all'interno dello *Empire State Building*, ad esempio), il motore di ricerca risponde in modo eccellente; se invece l'oggetto della ricerca è di natura pratica (come tolgo la ruggine dal paraurti dell'auto?) il sistema risponde con meno precisione, restituendo peraltro migliaia di risultati, ciò che in una telefonata sarebbe assolutamente impraticabile.

Il limite appena descritto può essere risolto analizzando le domande più frequentemente chieste (*FAQ*) e, una volta individuate, trasformando ciò che può esserlo in elementi conosciuti dal sistema di intelligenza artificiale. In altre parole, per quanto complessa può essere una domanda, se questa non varia rispetto all'utente che la pone può essere comunque gestita dal sistema di intelligenza artificiale considerato. La decisione più importante davanti alla quale si trova il *management* che decide di implementare un sistema simile è quella di impostare il livello di confidenza al di sotto del quale l'intelligenza artificiale deve evitare di rispondere e inoltrare direttamente la domanda ad un operatore: il sistema, di volta in volta e sulla base del *training* e dell'esperienza accumulata, può calcolare la probabilità con la quale la risposta che fornirà sarà giusta o sbagliata (ovvero, il livello di confidenza).

Più è alta questa probabilità e maggiore è la sicurezza della macchina circa l'appropriatezza della risposta che sta per fornire. Se il livello di confidenza al di sopra del quale rispondere è impostato come troppo elevato il sistema erogherà un numero limitato di risposte, con il risultato che sarà necessario un maggior numero di personale per far fronte alle telefonate non gestibili automaticamente; al contrario, se sarà troppo basso il sistema finirà per erogare un servizio di livello insoddisfacente, generando frustrazione e disappunto nel cliente.

Una diversa possibile applicazione del *NLP* è nella classificazione intelligente dei documenti. Nel mondo legale americano, ad esempio, è frequente che, prima dell'inizio del processo, una parte possa chiedere all'altra di produrre tutti i

documenti che abbiano un determinato contenuto. Nel tempo, e soprattutto con l'avvento delle tecnologie di digitalizzazione, il volume dei documenti da analizzare ha conosciuto un incremento verticale, rendendo la fase di analisi dei documenti ricevuti un'attività estremamente onerosa da un punto di vista di tempo impiegato da personale qualificato il cui costo orario è notevolmente elevato.

Nel tentativo di ridurre questa inefficienza si è prima cercato di strutturare un sistema di ricerca basato su parole chiave, ma il risultato è stato deludente, poiché, soprattutto in un contesto tecnicamente complesso, le parole potevano variare molto frequentemente, di fatto rendendo questa soluzione non percorribile. Successivamente è stato implementato un sistema di intelligenza artificiale basato sul *machine learning* che consente di scartare tutti i documenti sicuramente di nessun interesse: in una prima fase è stato chiesto ad avvocati esperti di classificare alcuni documenti, così da costituire un *training set* sulla base del quale avviare un'attività di classificazione supervisionata; in una seconda fase, è stato applicato il *NLP* per elaborare il contenuto dei documenti e cercare di comprendere quali parole, associazioni di parole o frasi consentono nella maggior parte dei casi di identificare un determinato documento correttamente.

Similmente a quanto osservato nell'ambito dei *call center*, è stato deciso un determinato livello di affidabilità al di sotto del quale il documento doveva essere scartato, applicando però una logica che tenesse conto della criticità del compito svolto: sono state quindi individuate tre diverse fasce di probabilità, di modo che se un documento ha una probabilità del 90% di essere rilevante viene sicuramente preso in considerazione, se ne ha una pari o inferiore al 40% viene sicuramente scartato e se si colloca nel mezzo viene chiesta la valutazione di un avvocato esperto.

Il sistema così implementato ha consentito di ridurre significativamente i costi aziendali senza rinunciare alla collaborazione di una sola persona, poiché in ogni caso l'attività di selezione della documentazione pertinente è stata ridotta nella quantità, ma non nella qualità del lavoro, richiedendo che le persone lavorino diversamente, non di meno: quello appena fatto è quindi un esempio di

collaborazione fra persone e intelligenza artificiale. Un ulteriore esempio di applicazione di tecnologia *NLP* può essere fatto sempre all'interno del mondo legale, in particolare nelle attività di *due diligence* da svolgersi nell'ambito di decisioni legate al *M&A* (*Mergers and Acquisitions*).

In questi casi, risulta critico per l'acquirente analizzare se, ad esempio nei contratti in essere, vi possono essere conseguenze di una qualche natura discendenti dall'acquisto o dalla fusione in fase di considerazione. Talvolta queste attività possono prevedere l'analisi di centinaia di contratti, i quali possono contenere ognuno una serie di clausole che è necessario considerare. Le clausole in parola, peraltro, possono essere formulate in centinaia di modi diversi, quindi anche in questo caso un'attività di ricerca di parole chiave risulterebbe inutile.

Un software *NLP* in questo contesto può ridurre significativamente la quantità di lavoro svolto, ponendo all'attenzione di operatori qualificati solo le clausole che è bene che siano controllate ed escludendo le altre. In conclusione, si ritiene opportuno segnalare che la tecnologia in parola ha bisogno, con ogni probabilità, di un investimento economico significativamente inferiore a quello necessario per implementare altre tecnologie basate su intelligenza artificiale, dato che è possibile utilizzare software di terze parti e implementarlo all'interno dei propri prodotti[89].

4. *Paradigmi del cambiamento: la robotica*

Durante lo sviluppo delle tecniche di produzione industriale si è reso sempre più necessario, al fine di migliorare efficacia ed efficienza dei processi, il ripensamento degli strumenti utilizzati, anche e soprattutto sulla base delle nuove tecnologie disponibili in funzione del passare del tempo. La robotica, in quest'ottica, riveste un'importanza ormai capitale, poiché consente di ottenere processi di produzione di estrema precisione mantenendo volumi elevati, in questo modo ottenendo di mantenere se non abbassare il costo unitario di prodotto.

[89] Si veda, in merito, F. J. Ohlhorst, *Amazon Alexa Poised to Bring Natural Language Processing to Businesses*, Gigaom, 2017, https://gigaom.com/2017/01/10/rocketalexa1/.

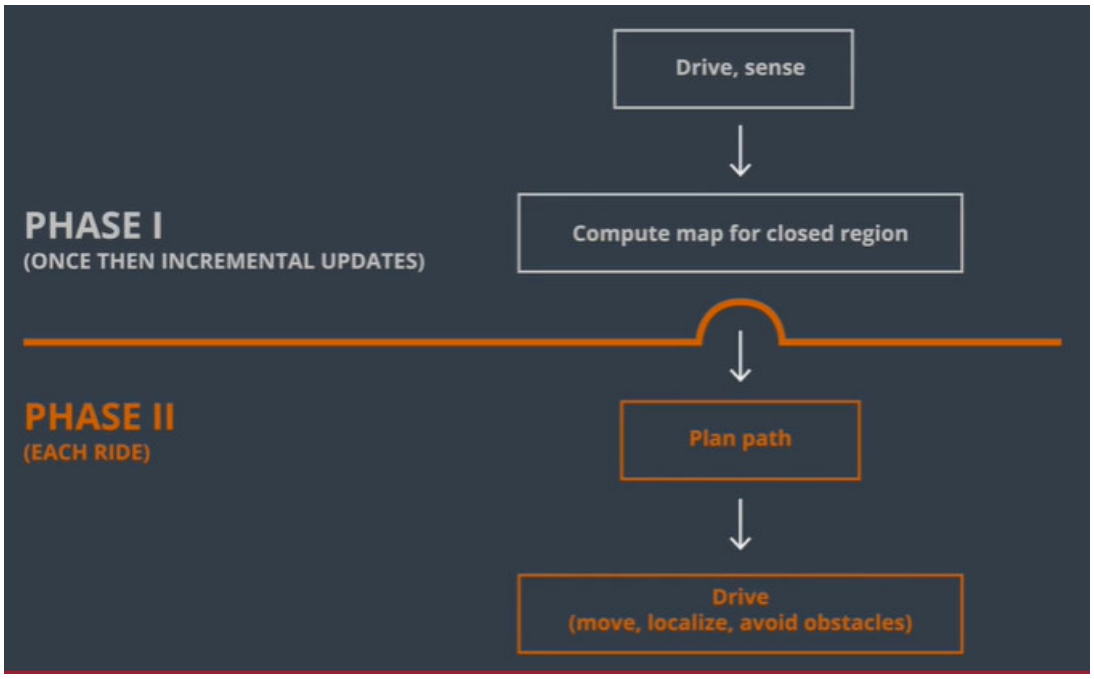
I robot sono, in sostanza, elementi *hardware* che, tramite attuatori, motori ed idrauliche sofisticate, coordinati attraverso componenti elettroniche e informatiche, riescono a interagire con il mondo che li circonda. Con il passare del tempo, la tecnologia alla base di questi sistemi si è evoluta, divenendo meno costosa e più compatta; lo sviluppo dei sistemi software, peraltro, ha reso possibile l'implementazione di sistemi completamente diversi da quelli industriali, pensati per un utilizzo destinato se non al mercato *consumer*, comunque a soggetti di dimensioni estremamente ridotte se comparate a imprese strutturate in modo complesso[90].

Il binomio intelligenza artificiale – robotica ha da subito suscitato estremo interesse, sia grazie alla particolare interazione prospettata da un sistema capace di comprendere ciò che gli viene detto in modo non strettamente dipendente dalla programmazione di base, sia grazie al possibile impatto che detta tecnologia potrebbe avere sulla quotidianità di un qualsiasi essere umano. Nel panorama attuale vi sono già molte applicazioni di robot più o meno intelligenti, basti pensare alle auto a guida autonoma, connesse a internet e capaci di analizzare l'ambiente che le circonda.

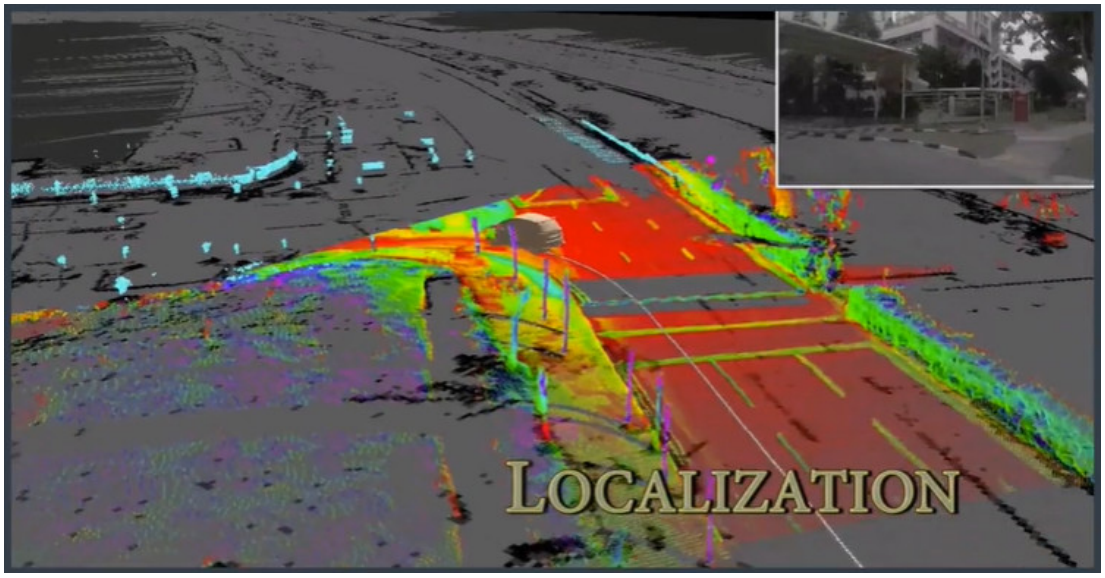
Nell'epoca dell'internet delle cose, dove anche gli elettrodomestici sono sempre più intelligenti e sempre più interconnessi, è evidente come ogni dispositivo sia capace di interagire con l'ambiente che lo circonda e con altri dispositivi, nella ricerca di una sorta di dialogo fra questi che consenta all'uno di avere le informazioni di cui necessita dall'altro. Un robot, in altre parole, è una macchina programmabile che è capace di processare come input ciò che ha attorno a sé, nell'ambiente che lo circonda, e condiziona quest'ultimo tramite attuatori servomeccanici. Dal discorso fatto finora è evidente che i robot in analisi possono avere le più disparate forme: assumono, sostanzialmente, l'aspetto che è maggiormente funzionale al compito che devono svolgere.

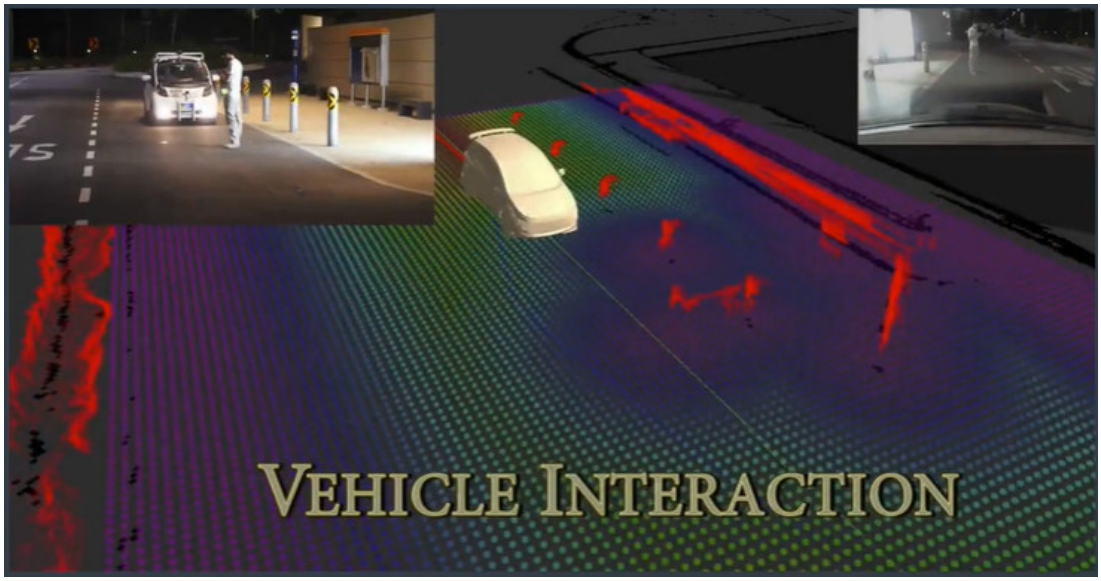
[90] Ci si riferisce qui non tanto alla dimensione del *robot* o dell'impianto di produzione al quale questo è destinato, quanto al capitale che chi vuole introdurre l'utilizzo dei *robot* all'interno della propria impresa deve investire.

Un'auto potrebbe essere un robot, come potrebbe esserlo anche un cestino dell'immondizia. Per approfondire la tecnologia da un punto di vista tecnico, può essere utile prendere ad esempio un'auto a guida autonoma, dato che la metodologia applicata è estremamente simile a quella da applicare in contesti differenti. È possibile, in prima battuta, distinguere due fasi: quella nella quale il sistema prende conoscenza dell'ambiente e una seconda nella quale è in grado di prendere decisioni all'interno dell'ambiente che conosce.



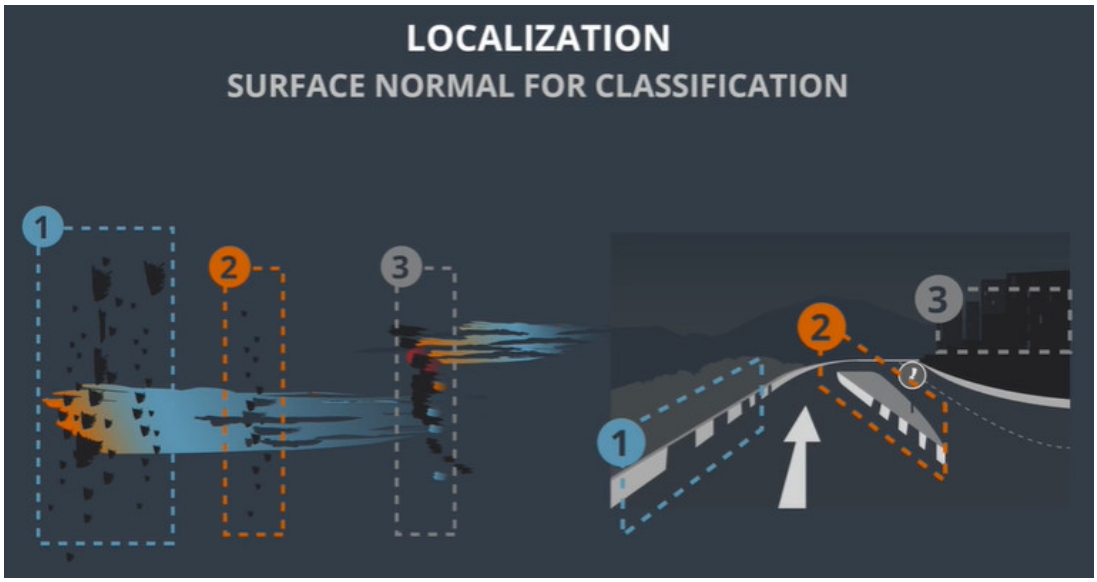
Nella prima fase, in sostanza, il sistema ricostruisce lo spazio traducendolo in vettori, come spiegato nel primo capitolo; si avrà pertanto uno spazio dei record che costituirà la mappa all'interno della quale il software dovrà prendere decisioni (nella fattispecie, direzionare l'auto sotto il suo controllo). Una volta ottenuto lo spazio dei record il sistema deve essere in grado di fare sostanzialmente due cose: pianificare un percorso e far fronte agli elementi che inizialmente non sono considerabili all'interno dello spazio iniziale (per esempio gli ostacoli che è possibile incontrare, come altre vetture in movimento, o pedoni che attraversano la strada).





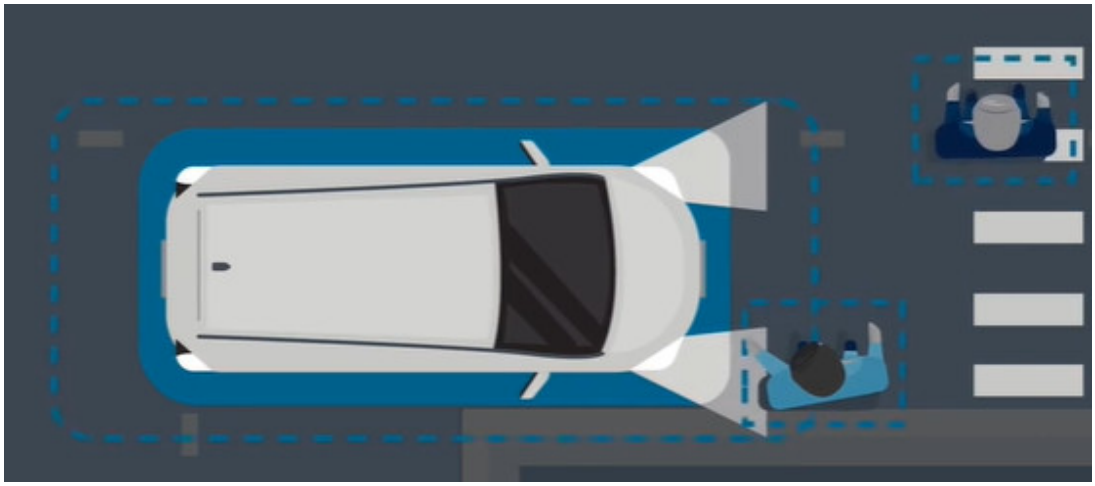
Per esempio, per rilevare gli ostacoli e ricostruire l'ambiente circostante possono essere utilizzati sensori a rilevazione laser, mentre per la rilevazione di oggetti o pedoni possono essere utilizzate videocamere poste tutto intorno al veicolo. Ciò che è estremamente importante è il numero di caratteristiche (*feature*) da osservare per ricostruire un ambiente e le loro relazioni: come si è già avuto modo di spiegare precedentemente, quante più caratteristiche vanno osservate, tante più dimensioni avrà lo spazio dei record che il sistema dovrà ricostruire. All'aumentare delle dimensioni, aumentano anche la complessità di calcolo e la capacità di memorizzazione necessarie a far funzionare il sistema. È stato tuttavia dimostrato che per identificare in modo univoco la maggior parte dei luoghi nel

mondo è sufficiente correlare due elementi: ciò che è presente ai bordi della strada da percorrere e l'aspetto dei palazzi circostanti.



Nell'immagine precedente è possibile vedere quali elementi sono presi in considerazione e come questi vengono sistemati nello spazio dei record all'interno del quale il sistema di guida si orienta. Normalizzando i dati desumibili da bordi e caratteristiche dei palazzi circostanti è possibile combinare e confrontare i dati ottenuti, al fine di ottenere una mappa tridimensionale di ciò che circonda l'auto. Tramite tecnologie di *deep learning* è possibile ricondurre il tutto ad una mappa bidimensionale, sufficientemente semplificata perché il sistema possa prendere decisioni in tempo reale.

L'ultimo componente di questo sistema è una sorta di navigatore, ovvero un sistema che consenta di pianificare un percorso dalla partenza all'arrivo; si tratta di qualcosa di molto simile a un qualsiasi navigatore, con l'unica differenza che questo deve essere obbligatoriamente dotato di un sistema che potremmo definire come un paraurti virtuale dinamico (*dynamic virtual bumper*). Anche se il sistema di percezione è in grado di prendere decisioni in tempo reale, bisogna che consideri il tempo necessario affinché una decisione sia trasformata in azione, tenuto conto di aspetti che attengono alla fisica della vettura (ad esempio l'inerzia, l'attrito, le condizioni della strada): ecco perché il paraurti deve essere dinamico, deve cioè tenere conto di vari fattori per poter assumere decisioni in sicurezza.



Nell'immagine, il paraurti virtuale è dato dalla linea tratteggiata blu. La persona è stata rilevata nel momento in cui le linee attorno al veicolo e alla persona stessa si sono incrociate, in modo tale che il sistema ha avuto il tempo di prendere una decisione, ovvero se fermare il veicolo o evitare il pedone cambiando direzione: qualora avesse preso la seconda decisione avrebbe impattato contro il pedone in attraversamento, perciò il veicolo è stato fermato. Tutto questo è possibile solo se viene mantenuta una velocità del veicolo che tiene conto delle capacità computazionali del sistema di bordo.

Nel considerare la circolazione su strada, peraltro, è necessario tenere conto anche delle norme di circolazione stabilite localmente. All'interno dell'algoritmo di I.A., pertanto, dovranno essere incorporate anche norme di comportamento coerenti con la normativa. Si pensi, però, ad un'auto che viaggia su una corsia delimitata dalla linea continua a sinistra e che, all'improvviso, incontra un ostacolo.

Come dovrebbe comportarsi il sistema? Ad esempio, nell'immagine che segue l'auto non potrebbe né proseguire né superare la linea continua, sulla base di un set di regole prefissato e non modificabile.

Sulla base del fatto che la convenzione di Vienna consente di non rispettare le norme di circolazione in uno spazio delimitato quando è necessario, la soluzione è piuttosto semplice: evitare l'ostacolo ignorando la linea continua. La possibilità di incorporare una tale azione, ovvero la capacità di derogare a una determinata regola in particolari situazioni è qualcosa di codificabile solo grazie alla tecnologia utilizzata, poiché questa è in grado di assumere decisioni volta per volta, che tengano conto del contesto.

La tecnologia appena illustrata oltre che un segno del progresso da un punto di vista tecnico è un cambiamento che avrà ripercussioni sociali, nel senso che cambierà completamente il modo in cui le persone approcciano alla guida, al trasporto pubblico e privato[91]. La progressiva introduzione della tecnologia sopra

[91] "*Driverless cars are nothing short of a revolution – not a technological revolution, but a social one, that will determine how fast we can accept, adapt and trust these new systems to change our lives. Driverless cars may be borne out of science fiction, but they are fast becoming realities on tomorrow's roadways. The transition from driver to robot is nothing short of a revolution. Not a technological*

brevemente descritta comporterà un processo di adattamento, inevitabilmente lento e disordinato, porterà ad una situazione nella quale i veicoli autonomi provocheranno interruzioni nella forza lavoro, influenzando al contempo la progettazione dei nostri spazi urbani e suburbani, l'idea stessa di "patente di guida", la nostra nozione di fiducia e in che cosa la riponiamo, nel nostro concetto di "proprietà", e in definitiva, la capacità di mobilità di cui godiamo. Una considerazione potrebbe chiarire meglio quest'ultima affermazione: un'auto a guida autonoma è mediamente più veloce e sicura di qualsiasi persona[92].

Ciò implica che, con la diffusione capillare di auto di questo tipo, si potrebbero rivedere i limiti di velocità imposti sulle strade pubbliche, pertanto una persona potrebbe decidere di vivere anche molto lontano da casa, dato che il tragitto casa-lavoro potrebbe essere coperto molto più velocemente. Ad oggi, comunque, sono tre i modi principali di utilizzare la robotica nelle aziende. I robot possono essere utilizzati presso gli impianti di produzione, negli uffici o in altri spazi aziendali.

Negli impianti di produzione possono essere usati per trasformare e assemblare i componenti di prodotti fisici, mentre nei magazzini possono occuparsi della logistica delle merci, ciò che, più in generale, può avvenire anche in altri luoghi con declinazioni differenti (in un ufficio un robot potrebbe spostare documentazione, in un hotel potrebbe spostare i bagagli e così via). Naturalmente in tutti i suddetti contesti vi è la compresenza di robot ed esseri umani, ciò che costituisce una delle sfide più impegnative risolte grazie all'impiego dell'intelligenza artificiale.

Un esempio dell'impiego di robot in contesti simili a quelli appena descritti può essere dato da *Relay* della *Savioke*, una società che si occupa di sviluppare robot

---

revolution, but a social one, that will determine how fast we can accept, adapt and trust these new systems to change how and where we live, work, play and interact with each other", J. F. Coughlin, *Driverless Cars Will be a Social Rather Than Technological Revolution*, Big Think, 2016, https://bigthink.com/the-present/driverless-cars-will-be-a-social-rather-than-technological-revolution/.

92 "*Nel 2014 un'auto autonoma, l'Audi RS 7, ha ottenuto una media di 240 chilometri orari e, nell'equivalente automobilistico della vittoria a scacchi di Deep Blue nel 1997 su Garry Kasparov, un'altra Audi autonoma ha sconfitto un pilota di auto da corsa umano su una pista chiusa viaggiando a velocità superiori a 190 km/h*", J. Coughlin e L. Yoquinto, *The Long Road Home*, slate.com, 2015, https://slate.com/technology/2015/05/autonomous-cars-and-the-future-of-the-commute.html.

in contesti aziendali[93]; in particolare, *Relay* può svolgere una serie di compiti nell'ambito dell'accoglienza (hotel, b&b *et cetera*): può occuparsi del servizio in camera, dalla *reception* alla camera destinataria, indipendentemente dagli ostacoli che deve affrontare nel percorso (un ascensore, ad esempio, anche se la struttura deve adeguarlo in modo che accetti input tramite *Wi-fi*). Ciò è stato ottenuto proprio implementando in esso una tecnologia di intelligenza artificiale simile a quello che è stato visto nella prima parte di questo paragrafo; in più, il robot è in grado anche di interloquire con l'occupante della camera: quando arriva davanti alla porta può chiamarlo al telefono per avvisarlo di ciò e, nel ritirare il servizio in camera, è in grado di rispondere ad alcune domande che gli vengono poste. Una volta eseguito il compito il robot è in grado di tornare al suo punto di caricamento e di ricaricare autonomamente le proprie batterie, così da essere pronto ad eseguire quanto gli verrà affidato in seguito.

I benefici per la struttura che impiega un simile robot potrebbero non essere immediatamente evidenti. Uno dei problemi ai quali l'industria della *hospitality* è più soggetta è il forte tasso di *turnover* del personale: dato che questo è in continuo mutamento, l'azienda deve occuparsi continuamente di individuare e addestrarne di nuovo, con tutte le inefficienze che ciò comporta. Uno dei vantaggi che *Relay* è in grado di apportare all'azienda, quindi, è la sicura disponibilità, come anche l'alto livello del servizio erogato, ad un prezzo sicuramente inferiore al costo di assunzione e formazione sostenuto a causa del *turnover*.

Se si considera, inoltre, che uno degli aspetti più importanti della comunicazione delle principali catene alberghiere è dato proprio dalla capacità di mantenere lo stesso livello di servizio indipendentemente dalla struttura alla quale ci si rivolge, diventa evidente che avere la possibilità di erogare un servizio tramite un prodotto standardizzato è un importantissimo *quid pluris* anche da un punto di vista del *marketing*. In media, la consegna in camera è effettuata da *Relay* in cinque minuti; dato che si tratta di una macchina che adotta comportamenti sempre uguali

[93] www.savioke.com

rispetto alla situazione in cui si trova, anche questo può essere un elemento da utilizzare nella comunicazione con i propri ospiti da parte delle strutture, cosa che difficilmente potrebbe avvenire qualora il personale fosse unicamente umano. Un altro possibile impiego di robot capaci di maneggiare oggetti è nel campo della logistica e dello spostamento del necessario fra uffici e/o laboratori differenti; un esempio può essere quello di FedEx.

Questa, fra le proprie strutture, ne gestisce una che ha il compito di riparare dispositivi di vario genere; ha quindi adattato sette dispositivi *Relay* perché, invece del servizio in camera, si occupassero di trasferire il necessario da un tecnico riparatore ad un altro, evitando che questo fosse fatto dai tecnici stessi. Ciò comporta evidenti benefici sia in termini di maggiore concentrazione e serenità dei tecnici, sia di efficienza e produttività della struttura. In entrambi gli esempi appena descritti il robot deve interagire con esseri umani in spazi nei quali trova altri esseri umani. Questo è un aspetto estremamente importante: se il robot non fosse in grado di comprendere l'ambiente intorno a sé, e quindi di evitare possibili collisioni, tutto quanto offerto dal prodotto sopra descritto non sarebbe semplicemente possibile.

Questo è anche il motivo a causa del quale, negli impianti di produzione tradizionali – anche quelli basati su robotica all'avanguardia, ma non dotata di IA – i robot sono tutti tenuti dentro apposite gabbie, o particolari sezioni di interi capannoni: nello svolgere il proprio compito non hanno alcuna consapevolezza dell'ambiente che li circonda, si muovono sulla base di una programmazione predeterminata, quindi se una persona si trovasse all'interno dell'area di movimento potrebbe farsi molto male, se non addirittura essere uccisa. La capacità di comprendere e analizzare in senso dinamico l'ambiente circostante, pertanto, è la chiave di volta della robotica. *Relay* è perfettamente consapevole di ciò che lo circonda, grazie ai sensori dei quali è dotato e alla tecnologia di intelligenza artificiale che gli consente di analizzarne i dati; peraltro, l'interazione uomo-macchina è un elemento molto importante non solo per consentire al robot di muoversi adeguatamente all'interno degli spazi, ma anche di risolvere situazioni

di possibile difficoltà (ad esempio, *Relay* è in grado di chiedere aiuto quando si rende conto di non riuscire a portare a termine un compito a causa di un imprevisto).

Volendo analizzare più da vicino *Relay* è possibile identificare diverse tecnologie di intelligenza artificiale implementate in esso; la principale di queste è il *path planning*, ovvero la capacità di pianificare un percorso. Spesso non vi è un solo modo di arrivare da un determinato punto A ad un punto B. La tecnologia in parola consente di prendere una decisione che consenta di tenere conto di tutte le informazioni disponibili al robot in un dato momento; tale processo decisionale deve essere ripetibile appena succede un imprevisto. Ad esempio, potrebbe capitare che all'interno dell'ascensore vi siano altre persone dirette ad un piano differente da quello del robot, ciò che potrebbe condurre *Relay* in luoghi diversi da quelli che aveva inizialmente previsto: la tecnologia in parola gli consente di far fronte a queste circostanze cambiando le assunzioni inizialmente prese.

Capitolo III

Il caso "Tuko Productions s.r.l."

SOMMARIO: 1. Progetto di sviluppo aziendale della Tuko s.r.l. e *quaestio juris*. - 2. Esposizione, trattazione delle problematiche più importanti e illustrazione delle risposte. - 2.1. Sull'approccio metodologico e sul trattamento dei dati. – 2.2. Sulla natura dei dati raccolti presso terzi. – 2.3. Sul funzionamento del *software* in progettazione. – 2.4. Sull'uso interno. – 2.5. Sull'uso esterno.

1. *Progetto di sviluppo aziendale della Tuko s.r.l. e quaestio juris*

Tuko productions s.r.l. è un'azienda attiva nel mercato del gioco online. Essa si rivolge ai concessionari che forniscono giochi ai consumatori finali sviluppando principalmente giochi da casinò. Il cliente della Tuko, pertanto, è un concessionario autorizzato, quindi siamo nell'ambito di un'azienda che lavora in un mercato B2B. I giochi sviluppati da Tuko sono messi a disposizione dei concessionari autorizzati al gioco d'azzardo nel proprio Paese. Il sistema consente al consumatore finale, regolarmente iscritto sul sito del concessionario e con un conto aperto, di giocare sui giochi sviluppati da Tuko grazie a un collegamento fra i sistemi informatici di Tuko stessa e quelli del concessionario.

Quando l'utente seleziona un gioco, viene collegato a una piattaforma gestita direttamente da Tuko e la sessione di gioco ha inizio. Ciò vuol dire che tutti i dati generati nella sessione stessa sono automaticamente noti a Tuko. Questi dati riguardano una discreta varietà di elementi, ad esempio il numero dei colpi eseguiti, gli importi delle puntate, le vincite, la durata della sessione di gioco, come anche il jackpot gold e silver, il numero cumulativo dei colpi, gli importi giocati in totale, i pagamenti avvenuti in un determinato arco di tempo. Alcuni di questi dati sono previsti dalla norma (l'ID di gioco rilasciato da ADM, per esempio), altri sono importanti per capire se tutto funziona correttamente (ad esempio se il gioco ha pagato nei tempi previsti, se ci sono state giocate che hanno vinto in modo notevolmente superiore alla media, se ci sono schemi di gioco ripetuti con

caratteristiche tali da considerarli fraudolenti, se c'è un bug nel software, eccetera), mentre altri sono sostanzialmente necessari al corretto funzionamento del sistema.

Tale funzionamento è replicato per ogni provider, sostanzialmente, quindi le considerazioni che si faranno possono essere considerate di carattere generale, al netto di alcune particolarità. I concessionari, inoltre, non si occupano solo di questo tipo di giochi: ospitano al loro interno una varietà molto ampia di possibilità di intrattenimento, anche in tema di scommesse sportive. Ogni sessione, pur nelle sue differenze tecniche, genera notevoli quantità di dati con frequenza oraria, rendendo molto laboriose le attività di analisi e controllo. Ad oggi, inoltre, non esiste un modo di automatizzare queste attività, data la natura notevolmente variabile delle stesse, né di analizzare tutto ciò che avviene in tempo reale (ai fini della c.d. *anomaly detection*, ad esempio) o in un secondo momento (ciò che sarebbe molto utile, ad esempio, per aiutare il management di un provider a scegliere quale direzione intraprendere nello sviluppo del futuro software, piuttosto che quello di un concessionario per direzionare correttamente le politiche di marketing).

Il software che la Tuko intende sviluppare mira a individuare e analizzare le correlazioni fra i dati generati nelle sessioni di cui sopra. Il fine ultimo è quello di vendere a concessionari o provider terzi (di seguito definiti clienti), sempre sul mercato B2B, la possibilità di utilizzo di questo software, anche se Tuko vorrebbe mantenere sempre la possibilità di utilizzarlo anche internamente. In base a quanto suesposto appare di tutta evidenza come tale software potrebbe avere molteplici applicazioni, sia per provider e concessionari terzi rispetto a Tuko, sia a Tuko stessa, ad esempio per valutare come indirizzare la produzione futura.

Ecco perché il software in parola, nell'idea attuale, accetta in input ogni tipo di dati ed è il cliente a decidere quale dato inserire: la genericità del dato stesso è una condizione essenziale perché tale software possa essere utilizzato con la massima flessibilità possibile, tenuto conto della profonda diversità degli ambiti gestionali e operativi ai quali ci si è riferiti in premessa. Appare altresì evidente che Tuko non ha alcun interesse a identificare il singolo giocatore, avendo in mente di offrire un tool utile al mercato B2B nelle operazioni sopra descritte, pertanto lo sviluppo

avverrà in modo tale da non consentire in alcun modo di ricondurre i dati raccolti ad un soggetto in particolare.

Quali obblighi legali devono essere rispettati da Tuko per essere conforme alla normativa vigente? In particolare, possono esserci problemi nel rispettare la normativa GDPR, tenuto conto che in ogni caso viene condotta un'attività di profilazione?

Il software realizzato potrà essere utilizzato dalla tipologia di clienti ai quali Tuko già si rivolge? In particolare, quali sono le attività che sicuramente detti clienti non potranno svolgere ai sensi della normativa vigente?

La genericità del dato di input è, nell'ottica di Tuko, un punto di forza estremamente importante, perché consente di ottenere un tool estremamente potente e versatile e, pertanto, utilizzabile nel contesto che il cliente riterrà più interessante per perseguire i propri fini. Ad esempio, uno degli utilizzi del software in parola potrebbe essere quello della *anomaly detection*: puntate particolarmente difformi dalla media, come anche vincite superiori alla media e ripetute nel lasso di breve tempo, già oggi sono oggetto di osservazione da parte dei clienti e di Tuko stessa, sia per rilevare possibili frodi che per scoprire possibili falle nelle matematiche dei software di gioco.

Tale funzione viene svolta nel tempo più breve possibile, data la sua delicatezza e i notevoli danni che potrebbe recare a un concessionario e, di riflesso, al provider che sviluppa un determinato software. Ciò che Tuko vuole sviluppare potrebbe aiutare a svolgere questa funzione in tempo reale, anche automatizzando buona parte del lavoro di analisi che oggi viene svolto da sviluppatori, costituendo in questo modo un tool estremamente utile per la generalità delle sessioni di gioco e non solo per quelle svolte sulla piattaforma fornita da Tuko. Tale elemento, però, prevede che Tuko memorizzi i dati in tempo reale e li conservi per tutto il tempo necessario alle analisi che si intenderà prevedere. Oltre a questo, potrebbe essere utile memorizzare i dati anche per elaborare specifiche query da parte dei clienti, prevedendo così che questi forniscano solo una parte dei dati necessari all'analisi (poiché un'altra parte sarebbe già memorizzata da Tuko). Non si prevede di

mettere a disposizione tutti i dati di input di una determinata query al cliente, ma solo quelli di output, escludendo in questo modo la possibilità di diffondere dati ad un cliente che potrebbero essere per lui non reperibili normalmente. Sulla base di quanto esposto, quali accorgimenti deve adottare Tuko per essere GDPR *compliant* in merito alla memorizzazione dei dati?

Inoltre, la potenza e la versatilità del software da realizzare potrebbe indurre un concessionario a voler tenere sotto controllo tutte le giocate svolte dai propri utenti, indipendentemente dalla piattaforma sulla quale questi vengono generati, mettendoli così a disposizione anche di Tuko. Tale circostanza metterebbe Tuko in condizione di dover stipulare specifici accordi con tutti i soggetti coinvolti nella raccolta dati, oppure basterebbe un accordo all'uopo stipulato fra concessionario e provider terzo per considerare del tutto legale l'utilizzo del concessionario nel modo suddetto?

Il cliente, poi, potrebbe anche voler fare un diverso utilizzo del software in parola, in un'ottica di marketing e di massimizzazione dei bonus da erogare. Per analizzare il comportamento dei consumatori finali iscritti sul proprio sito internet, in particolare, un concessionario potrebbe ritenere utile mettere in correlazione tramite il software di Tuko giochi di diversi produttori, per individuare key features che potrebbero aiutare la politica di erogazione bonus o di scontistica che normalmente viene praticata. Tale utilizzo del software dovrebbe portare Tuko ad adottare particolari accorgimenti al fine di non infrangere la normativa vigente, in particolare con riferimento alla protezione della proprietà industriale, sia in termini di contratti da stipulare che di funzionalità da non consentire?

2. *Esposizione, trattazione delle problematiche più importanti e illustrazione delle risposte*

2.1. *Sull'approccio metodologico e sul trattamento dei dati*

Il periodo di tirocinio presso la Tuko Productions s.r.l., finalizzato alla raccolta e alla sistemazione dei dati necessari ad effettuare l'analisi di seguito esposta, è stato organizzato tenendo in particolare considerazione la multidisciplinarietà del progetto di ricerca e, quindi, la necessità di adottare differenti approcci a seconda delle discipline coinvolte. Dall'analisi delle informazioni di carattere sia scientifico che industriale, illustrate nei precedenti capitoli, si è potuto desumere che era necessario, nel periodo di tirocinio aziendale, raccogliere quanti più dati possibile su due aspetti fondamentali: il trattamento del cliente da parte del concessionario di gioco e lo scambio delle informazioni fra i sistemi informatici coinvolti nel processo di gioco. Circa il secondo aspetto, le motivazioni della raccolta dati risultano evidenti al lettore: per svolgere un'analisi quanto più possibile compiuta delle ricadute della normativa privacy sull'elaborazione automatizzata da parte di un software di intelligenza artificiale dei dati raccolti nelle sessioni di gioco è fondamentale comprendere la natura dei dati raccolti, sia da un punto di vista squisitamente informatico che giuridico. Circa il primo aspetto, come si comprenderà più facilmente appresso, nonostante il cliente del concessionario non abbia formalmente un collegamento diretto con l'azienda ospitante, per comprendere la natura dei dati scambiati fra la Tuko e le aziende titolari di concessioni è necessario analizzare anche il rapporto sottostante queste e i propri utenti, dato che comunque sono proprio questi ultimi a collegarsi con i sistemi Tuko per le fasi più operative del gioco. La raccolta dati, pertanto, è partita dall'analisi del *framework* giuridico all'interno del quale devono muoversi i concessionari di gioco e la Tuko con questi ultimi. Nel primo caso, è stato necessario analizzare la documentazione circa i contratti di concessione e i relativi

allegati, disponibile integralmente sul sito dell'Agenzia Dogane e Monopoli[94]. Nel secondo caso, il tirocinio svolto presso la società ospitante è stato l'unico modo per comprendere esattamente il processo di comunicazione intra-server, dato che, benché nel settore vi siano aspetti che costituiscono sostanzialmente *standard* riconosciuti e applicati diffusamente, la natura dell'attività svolta e della disciplina trattata avrebbero reso estremamente difficile allo scrivente ottenere una comprensione tecnica sufficiente a svolgere il lavoro di ricerca oggetto della presente dissertazione con un sufficiente grado di sicurezza. Le informazioni così ottenute sono state, quindi, analizzate da un punto di vista legale, sia con riferimento ad aspetti più prettamente civilistici inerenti il rapporto fra i soggetti coinvolti, sia ad aspetti più strettamente inerenti alla normativa sulla *privacy*. Una volta compreso e analizzato il settore di riferimento e le metodologie di lavoro della società ospitante, si è provveduto a raccogliere le necessarie informazioni inerenti alla struttura di base del *software* basato su intelligenza artificiale ipotizzato dalla Tuko, per capire come i dati trattati, in considerazione della loro natura, avrebbero dovuto essere considerati tenuto conto della normativa di riferimento. Detto approccio metodologico ha consentito di procedere per gradi, calando nella realtà aziendale le conoscenze raccolte lungo la fase preparatoria di ricerca scientifica.

Prima di approfondire l'analisi della fattispecie proposta si ritiene indispensabile analizzare le modalità con le quali i dati vengono trasmessi, la tipologia di questi e i soggetti coinvolti. I soggetti coinvolti, in un'attività di fornitura di servizi di *gaming online*, sono essenzialmente tre: il giocatore, il concessionario di gioco e il provider di gioco. Il giocatore è una persona fisica, necessariamente maggiorenne e dotata di codice fiscale italiano, la quale ha stipulato un contratto di conto di gioco personale infruttifero con il concessionario

[94]https://www.adm.gov.it/portale/documents/20182/542484/SCHEMA_CONVENZIONE_COMUNITARIA.pdf/0a9a82db-a63e-45e0-b78b-bfd15d45090a?t=1456159682751

secondo lo schema predisposto dall'Agenzia delle Dogane e dei Monopoli (ADM)[95].

Il concessionario di gioco è un soggetto d'impresa autorizzato da ADM ad erogare servizi di gioco a distanza sulla base di una convenzione stipulata secondo quanto previsto dalla normativa vigente. Nella convenzione, il concessionario assume una serie di impegni, dei quali in questa sede si ritiene opportuno citare alcuni: l'impegno formale ad adottare lo schema surrichiamato in fase di stipula del contratto di conto di gioco con il giocatore, la raccolta e la trasmissione di un documento di identità in corso di validità ad ADM per gli opportuni controlli, la verifica costante del regolare utilizzo del conto di gioco sulla base di quanto previsto dalla L. 88/2009[96], la segnalazione ad ADM di qualsiasi fatto che possa comportare la risoluzione di diritto del contratto in parola (come, ad esempio, l'utilizzo del conto di gioco da parte di un soggetto diverso dal titolare) e il trattamento dei dati raccolti secondo il disposto del D.Lgs. 196/2003[97] in qualità di titolare dello stesso.

La convenzione fra concessionario e ADM regola, peraltro, anche il trattamento dei dati del giocatore da parte di ADM stessa, che nomina come titolare del trattamento So.Ge.I., la società che gestisce gran parte degli aspetti informatici delle agenzie di Stato. Nel contratto di conto di gioco è altresì esplicitamente previsto che il concessionario e ADM possano trasmettere, "eventualmente e se necessario", i dati personali del giocatore a "società sub-fornitrici di servizi

[95] Allegato 4) dello schema di convenzione reperibile presso il seguente sito internet: https://www.agenziadoganemonopoli.gov.it/portale/documents/20182/542484/SCHEMA_CONVENZIONE_COMUNITARIA_AGENZIA_DOGANE_E_MONOPOLI.pdf/ca259a81-8218-4fb0-ab76-7395d213c9c6.

[96] La norma richiamata prevede una serie di disposizioni di varia natura, fra le quali in questa sede si intende richiamare il comma 17 dell'articolo 24, che testualmente dispone che "la sottoscrizione della domanda di concessione […] implica altresì l'assunzione da parte del soggetto richiedente dei seguenti obblighi valevoli per l'intera durata della concessione: […] e) adozione ovvero messa a disposizione di strumenti ed accorgimenti per l'autolimitazione ovvero per l'autoesclusione dal gioco, l'esclusione dall'accesso al gioco da parte di minori, nonché l'esposizione del relativo divieto in modo visibile negli ambienti virtuali di gioco gestiti dal concessionario".

[97] Il richiamo non è aggiornato alle novità normative introdotte sia a livello comunitario, con l'entrata in vigore del GDPR, sia a livello nazionale, con il D.Lgs. 101/2018, ma si ritiene che ciò sia irrilevante atteso che gli obblighi disposti in capo al concessionario in qualità di titolare del trattamento sono del tutto uguali a quelli che avrebbero dovuto essere previsti sulla base della norma vigente *ratione temporis*.

necessari per la realizzazione delle attività di gioco oggetto del contratto"[98]. Il terzo soggetto surrichiamato è il provider di gioco; si tratta di un soggetto che svolge attività d'impresa consistente nell'erogazione di servizi di gioco online, progettati *in house* oppure da terzi che li concedono in licenza d'uso, tramite una piattaforma dedicata che gestisce tutte le fasi di gioco.

Detta piattaforma è sostanzialmente un software a parte, che funge da "contenitore" nel quale avvengono le diverse sessioni di gioco. Il giocatore, una volta registratosi presso il sito di un concessionario e ottenuta la disponibilità del proprio conto di gioco, può scegliere fra una varietà di giochi online. La società che pone le suesposte *quaestio juris*, la Tuko s.r.l., si occupa principalmente di *slot machines*, ma in realtà lo schema di funzionamento qui descritto è sostanzialmente lo stesso per la maggior parte dei giochi di sorte a quota fissa[99] online. Una volta scelto il gioco al quale desidera giocare, il giocatore clicca su un link che lo collega direttamente alla piattaforma del provider di gioco; questa, una volta ricevuto il collegamento in entrata, contatta il sistema del concessionario di gioco per aprire la sessione di gioco vera e propria.

La prima informazione in assoluto ricevuta e memorizzata dal provider di gioco è l'indirizzo IP del giocatore, che viene comunicato al concessionario affinché questo lo comunichi a sua volta ad ADM. Nelle fasi iniziali della sessione di gioco vengono scambiate alcune informazioni di base: un codice utente (tecnicamente

[98] Vd. Comma 4, articolo 18, schema di contratto di conto di gioco.

[99] Nel caso dei giochi di abilità vi è la necessità di garantire la presenza di un solo giocatore allo stesso tavolo. Ciò potrebbe essere particolarmente complicato qualora ad uno stesso tavolo siedano giocatori provenienti da diversi concessionari, cosa che accade frequentemente nei network di gioco, ovvero nel caso in cui più concessionari decidono di offrire ai propri utenti la possibilità di sedersi a tavoli da gioco gestiti in comune. Se la natura dei dati fosse la stessa di quella descritta nel presente elaborato, poiché il codice utente è univoco fra concessionario e provider ma ben potrebbe accadere che lo stesso provider abbia un utente con identico codice ospitato su un diverso concessionario, il controllo dell'effettiva identità di un giocatore diventerebbe impossibile. Ciò consentirebbe ad un singolo soggetto di iscriversi con utenze differenti presso diversi concessionari e di sedersi allo stesso tavolo, al fine di giocare con più carte contemporaneamente. Per evitare questo comportamento, in questo caso lo schema dell'integrazione prevede che il concessionario, oltre al codice utente, comunichi anche il codice fiscale dell'intestatario del conto di gioco. Ciò rende edotto il provider dell'identità personale del giocatore, consentendogli di evitare lo scenario sopra descritto. Per la precisione, il campo nel quale si inserisce il codice fiscale è presente anche nello schema dell'integrazione utilizzato nei giochi di sorte a quota fissa, ma si tratta di un campo non obbligatorio. Nell'esperienza svolta in azienda si è rilevato che è possibile, talvolta, che un concessionario riempia il campo in parola, ma Tuko non memorizza né analizza in alcun modo questa informazione, pertanto la si esclude completamente dall'analisi effettuata.

detto *login*), l'importo disponibile al giocatore per il gioco (*getbalance*) e l'identificativo della sessione di gioco (*startsession*) e del *ticket* di gioco[100]. Il codice utente è un codice univoco nell'ambito di un concessionario: viene stabilito la primissima volta che il giocatore si collega ad una determinata piattaforma e rimane sempre lo stesso da quel momento in poi.

Non è necessario che il codice rispetti un determinato formato: provider e concessionario concordano in fase di integrazione[101] il formato che il codice utente rispetterà, per ragioni tecniche, senza che questo codice porti con sé alcuna informazione utile alla ricostruzione dell'identità del giocatore. In altre parole, il codice serve alla piattaforma a ricondurre i dati di gioco ad un determinato soggetto per ragioni tecniche e organizzative (ad esempio la comunicazione di vincite/perdite per l'accredito o l'addebito sul conto di gioco da parte del concessionario), senza che abbia alcuna rilevanza l'identificazione personale del giocatore. In apertura della sessione di gioco, pertanto, il concessionario potrà tranquillamente generare un codice da trasmettere al provider, basta che crei contemporaneamente una corrispondenza biunivoca fra questo e l'utenza del giocatore, così da poter comunicare sempre lo stesso codice ogni volta che quest'ultimo apre una nuova sessione di gioco presso lo stesso provider.

Tutte le sopra descritte comunicazioni avvengono sulla rete internet, quindi transitano su una rete pubblica, anche se opportunamente criptate (per esempio tramite *TLS*[102]) per evitare problemi di sicurezza informatica. Una volta che il

---

[100] La differenza fra identificativo sessione e identificativo del *ticket* ha rilevanza solo nel momento in cui il concessionario prevede il *rebuy*, ovvero la possibilità per il giocatore di ricaricare il proprio conto di gioco senza dover chiudere la sessione. Qualora il concessionario dia questa possibilità – non tutti lo fanno – quando il giocatore chiederà di ricaricare il conto di gioco, il concessionario invocherà una funzione in ADM (*acquistodiritto*) con la quale comunicherà questa circostanza e ADM risponderà trasmettendo un nuovo *ticket* di gioco, da sostituire al precedente. Il codice sessione pertanto non cambierà, mentre cambierà quello del *ticket*. Anche quando il concessionario non supporta il *rebuy*, un codice *ticket* viene comunque comunicato, con la sola differenza che non sarà soggetto a cambiamento durante l'intera sessione di gioco.

[101] Ovvero quando il provider struttura parte dei propri servizi affinché comunichino correttamente con il concessionario; è una fase necessaria solo all'inizio del rapporto, successivamente concessionario e provider possono far partire nuovi giochi senza doverla ripetere.

[102] *"Transport Layer Security (TLS) è un protocollo che permette di stabilire un canale con le proprietà di integrità e riservatezza in senso crittografico tra un client e un server. Dopo aver stabilito una connessione sicura tramite il protocollo TLS, le applicazioni possono utilizzarla per scambiare dati. TLS viene utilizzato in molteplici contesti applicativi (HTTPS, SMTPS, etc.)"*, Agenzia per l'Italia Digitale, www.agid.gov.it

giocatore termina la sessione di gioco viene comunicata la chiusura della stessa al concessionario (*finesessione*) affinché questo contabilizzi correttamente i relativi importi sul conto di gioco[103]. Lo schema di comunicazione appena descritto non è, in verità, l'unico possibile fra provider e concessionario[104], ma è quello adottato da Tuko, pertanto è valido ai fini delle considerazioni che si faranno appresso; è comunque vero che, anche cambiando schema, la natura dei dati trasferiti da un sistema all'altro non cambia, poiché al provider servono solo e soltanto i dati sopradescritti affinché sia possibile l'erogazione dei servizi di gioco.

2.2. *Sulla natura dei dati raccolti presso terzi*

Prima di svolgere qualsiasi tipo di valutazione circa la liceità del trattamento e gli eventuali accorgimenti da adottare al fine di rendere il sistema GDPR *compliant by design* è opportuno interrogarsi sulla natura dei dati trattati dal provider. Riepilogando, con riferimento al singolo giocatore sostanzialmente sono trasmessi e memorizzati i seguenti dati: indirizzo IP, codice univoco del giocatore e importo disponibile per il gioco; si preferisce non considerare, ai fini del presente elaborato, il codice della sessione o del *ticket* di gioco perché non sono dati che ineriscono al giocatore in senso stretto, quanto alla sessione vera e propria, e sono forniti in ogni caso da ADM su istanza del concessionario.

Il primo dato, ovvero l'indirizzo IP, consiste in una serie di numeri[105] che consentono di identificare in maniera univoca un determinato dispositivo elettronico connesso a internet in un dato momento. Sostanzialmente è possibile avere due tipologie di indirizzi: statico e dinamico[106]. Nel primo caso l'indirizzo

[103] Si omette, in questa breve descrizione semplificata, la comunicazione che avviene fra concessionario e ADM su rete dedicata, dato che non è rilevante ai fini della trattazione dell'oggetto del presente elaborato.

[104] Gli schemi possibili sono sostanzialmente due: *wallet* e *seamless*.

[105] Ci possono essere due protocolli, il TCPv4 e il TCPv6, che cambiano il formato dell'indirizzo, ma ciò non cambia lo scopo del dato trattato: identificare in modo univoco un determinato computer in una rete informatica.

[106] La differenza, in un primo momento, aveva portato la dottrina e la giurisprudenza a discutere circa la possibilità di considerare un indirizzo statico come dato personale, mentre uno dinamico non avrebbe avuto la stessa qualificazione. Nel tempo, prima con la sentenza *Scarlet Extended* (C-70/10, ECLI:EU:C:2011:771) e successivamente con la sentenza *Breyer* (C-582/14, *Patrick Breyer*

non cambia mai: l'utente che si disconnette avrà lo stesso indirizzo nel momento in cui si connetterà nuovamente; nel secondo caso, invece, l'indirizzo sarà attribuito ad ogni connessione dal provider internet. In entrambi i casi, comunque, è possibile considerare l'indirizzo IP come una sorta di indirizzo fisico, con tanto di strada, Cap, Comune e località: avendo i numeri che lo compongono è possibile recapitare un'informazione ad un determinato computer.

Fatta questa breve ma doverosa premessa, è ovvio che un indirizzo IP non consenta di identificare direttamente una persona, esattamente come il civico della villetta unifamiliare di una qualsiasi strada non può identificare univocamente un individuo; detto ciò, è pur vero che il provider di servizi internet, ovvero il soggetto che fornisce la connessione ad un determinato utente è perfettamente a conoscenza dell'identità dell'intestatario di una determinata linea avente uno specifico indirizzo IP, quindi è in grado di collegare le due informazioni. Si è quindi discusso di una tesi "oggettiva" e di una tesi "soggettiva", circa la natura del dato in parola[107]: secondo la prima, un indirizzo IP è da considerarsi "dato personale" ogniqualvolta questo consenta in concreto l'identificazione di un determinato utente, indipendentemente dal fatto che ciò richieda determinate autorizzazioni e/o capacità tecniche, mentre la seconda sostiene che tale dato diventi personale solo nel momento in cui il soggetto che ne dispone può anche risalire autonomamente all'identità del titolare dello stesso, senza bisogno di ulteriori autorizzazioni.

Una svolta a questo proposito si è avuta con la sentenza *Breyer* del 19/10/2016 ad opera della seconda sezione della Corte di Giustizia dell'Unione Europea[108], dove la Corte ha stabilito che è sufficiente che esista un qualsiasi mezzo legale per

c/Bundesrepublik Deutschland, ECLI:EU:C:2016:779) la natura del dato "indirizzo IP" è stata non solo chiarita da un punto di vista oggettivo, ma anche rispetto alla possibilità di considerarlo dato personale a seconda del caso concreto.

[107] Si veda A. El Khoury, "*Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat*", European Journal of Risk Regulation, 2017, volume 8, pp. 191–197.

[108] Op. cit.; si noti che la sentenza in oggetto si riferisce ad una direttiva previgente al GDPR, ovvero alla 95/46, ma è comunque conferente al caso di specie poiché il principio secondo il quale è necessario che vi sia un collegamento fra l'identità di una persona e un qualsiasi dato affinché questo sia considerabile come "personale" – e quindi soggetto alla normativa *privacy* – è rimasto inalterato nella normativa vigente (si veda il considerando 26 del GDPR e quanto già espresso nella prima sezione del primo capitolo del presente elaborato).

un determinato soggetto di chiedere l'identificazione dell'intestatario di una connessione avente un determinato indirizzo IP perché questo sia qualificato come dato personale[109]. Tornando al caso di specie, è sicuramente possibile, per il provider di gioco, chiedere che un provider internet comunichi l'identità del titolare di una connessione qualora vi siano motivi fondati per effettuare questa richiesta, per esempio nel caso in cui un utente cerchi di forzare in qualche modo la piattaforma di gioco, provocando danni e/o disservizi, ciò che costituisce un comportamento punibile ai sensi del Codice penale[110].

Sulla base di quanto espresso finora risulta comprensibile per quale motivo gli indirizzi IP degli utenti che si collegano alla piattaforma di gioco, benché siano sconosciute allo stesso le identità degli intestatari delle relative connessioni, siano comunque da considerarsi dati personali e, in quanto tali, soggetti alle disposizioni del GDPR. Il secondo dato conosciuto dal provider, ovvero il codice univoco del giocatore, si ritiene possa essere assimilato in tutto e per tutto ad una sorta di indirizzo IP, da un punto di vista giuridico.

Vero è che il provider non conosce l'identità del titolare del conto di gioco e che, come detto poco sopra, il codice in parola non porta in sé nessun tipo di elemento che consenta, nemmeno tramite approfondite ricerche, di risalire all'identità del giocatore, ma vale la stessa considerazione fatta riguardo la conoscibilità del reale intestatario della connessione a internet a partire da uno specifico indirizzo IP dato il verificarsi di determinate condizioni (ad esempio, il subire un attacco informatico da parte della piattaforma di proprietà del provider).

In altre parole, il provider potrebbe, querelando l'attaccante, conoscere l'identità dello stesso sulla base dell'ordinanza di un giudice adito allo scopo dal pubblico ministero incaricato, pertanto esiste un mezzo legale per conoscere

[109] "[…] u*n indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*".

[110] Si pensi al disposto dell'art. 615 ter c.p., in tema di accesso indesiderato, o dell'art. 617 quater in tema di attacchi finalizzati a intercettare o impedire l'erogazione di un servizio informatico o telematico.

l'identità dell'utente a partire dal codice in analisi. Ciò detto, è pur vero che, presumibilmente, qualsiasi pubblico ministero si muoverebbe a partire dall'indirizzo IP, rivolgendosi al provider di servizi internet, piuttosto che al concessionario di gioco, unico soggetto in grado di ricondurre un determinato codice utente al titolare di un conto di gioco, dato che la prima soluzione è sicuramente molto più frequentemente battuta della seconda, essendo applicabile a una qualsiasi fattispecie di reato telematico; questa affermazione, però, non muta la circostanza che, sebbene con eventualità remota, è possibile identificare una determinata persona fisica a partire dal dato in parola, ciò che è sufficiente a considerarlo un dato personale.

L'ultimo dato da prendere in considerazione, fra quelli conosciuti dal provider, è l'importo disponibile per il gioco. Detto importo non corrisponde necessariamente all'intero importo disponibile sul conto di gioco del giocatore: potrebbe essere impostato dallo stesso utilizzando le funzioni di autolimitazione della sua area riservata, oppure potrebbe essere limitato solo dalla legge. Non c'è alcuna connessione fra l'importo monetario e una qualità del giocatore inteso come persona: un importo del genere, che sia basso o elevato, non può dare nessuna indicazione circa la capacità reddituale o patrimoniale di un individuo, misurando al massimo solo la sua disponibilità a perdere al gioco quella determinata somma di denaro.

Purtuttavia si deve considerare che si tratta comunque di un dato riferito ad una persona identificabile e che costituisce in ogni caso un elemento caratteristico della sua "identità economica"[111], pertanto si tratta di un dato personale. L'affermazione risulta ancora più significativa se si considera il contesto in analisi in senso dinamico, invece che statico: è frequente che un giocatore utilizzi più di una volta la stessa piattaforma (anche utilizzando giochi diversi), per cui, posto che l'identificativo del giocatore rimane sempre lo stesso, avere a disposizione dati riguardanti una serie di sessioni di gioco, ognuna con un importo disponibile e

[111] Art. 4, paragrafo 1, GDPR.

caratterizzata da una serie di colpi vincenti e perdenti, consente abbastanza facilmente al provider di profilare la predisposizione al gioco di un determinato individuo la quale, anche se non indica elementi idonei a ricostruire dati di carattere più generale (come ad esempio il reddito di una persona), comunque è idonea a definire con una certa precisione una caratteristica economica riferibile a una persona identificabile, ovvero la somma di denaro vinta/persa in un determinato periodo temporale.

2.3. *Sul funzionamento del software in progettazione*

Il provider di gioco Tuko s.r.l. intende progettare un software, *GDPR compliant by design*, che sia capace di analizzare il comportamento dei giocatori di giochi di sorte a quota fissa *online* (sostanzialmente, il tipo di *audience* al quale Tuko si rivolge) basato sull'algoritmo di intelligenza artificiale *k-means*, del quale già si è avuto modo di illustrare il funzionamento e le principali caratteristiche nel corso della seconda sezione del primo capitolo. Il software in analisi deve, in particolare, essere in grado di accettare dati in *input* non solo da Tuko ma da qualsiasi cliente a cui Tuko voglia concederne l'utilizzo, tramite apposita licenza.

In termini generali, il software accetta in *input* tutti i dati relativi ad una moltitudine di sessioni di gioco, quali sono i dati raccolti presso il concessionario esposti sopra e tutti quelli generati durante la sessione stessa (come ad esempio gli *spin*, ovvero il numero di volte che il giocatore fa girare i rulli della *slot machine*, le puntate e le relative linee di gioco, i *free spin*, l'erogazione come l'accumulo dei *jackpot* dove previsti, *et cetera*), al fine di raggruppare gli utenti in *cluster* omogenei secondo gli elementi presi in considerazione volta per volta. A titolo meramente esemplificativo, si potrebbe analizzare l'utilizzo dei giochi per fascia di età degli utenti, magari tenendo contemporaneamente conto, nella formazione dei *cluster*, anche del modo in cui questi effettuano le puntate (molte di piccolo importo, poche di importi consistenti e così via).

Ciò consentirebbe di analizzare una serie di elementi, come ad esempio il gradimento di un gioco rispetto ad una determinata fascia di utenza o la predisposizione di una determinata fascia a giocare più frequentemente in un certo modo piuttosto che in un altro – cosa che potrebbe essere di estrema rilevanza anche per identificare comportamenti che potrebbero far emergere una dipendenza dal gioco. Il software in parola potrebbe avere principalmente due utilizzi: uno interno, da parte di Tuko stessa, e un altro esterno, da parte dei clienti concessionari. I suddetti utilizzi saranno oggetto di trattazioni separate, per meglio identificare gli eventuali problemi emersi e le relative soluzioni.

2.4. *Sull'uso interno*

Ci possono essere diversi vantaggi nell'utilizzo del software in parola da parte di Tuko: a titolo esemplificativo, possiamo citare la *fraud detection*, oppure l'indirizzo delle scelte di marketing inerenti ai giochi già sviluppati o quelle di produzione relative ai giochi da sviluppare e a come farlo. Riguardo alla *fraud detection* il software in parola potrebbe dare un contributo significativo sia per la notevole capacità di analisi di una grande mole di dati in tempi estremamente ridotti, sia per la possibilità di considerare molteplici aspetti della sessione di gioco alla ricerca di correlazioni che potrebbero non essere immediatamente identificabili. Circa le scelte di marketing o quelle di produzione interne all'azienda risulta evidente che il software in parola consentirebbe di avere una qualità e una quantità di informazioni da fornire al *management* tale per cui sarebbe possibile ripensare per intero entrambi i processi, consentendo di focalizzare l'attenzione su aspetti realmente generatori di valore, massimizzando in questo modo gli sforzi e il ritorno economico del tempo impiegato.

Affinché questo software possa essere *compliant by design* è necessario e opportuno, sulla base di quanto detto precedentemente, adottare alcune tecniche che consentono di interrompere il collegamento fra i dati e il soggetto al quale si riferiscono, così da pervenire all'elaborazione di dati non riferiti a persone

individuabili e, pertanto, non rientranti nel concetto di dato personale. Circa le tecniche di anonimizzazione/pseudonimizzazione già si è detto nel corso del primo capitolo; le tecniche di anonimizzazione, nel caso di specie, renderebbero i dati improcessabili, dato che uno dei concetti di base del software in analisi è proprio la riconducibilità del dato raccolto a uno specifico soggetto.

Se si interrompe del tutto questa riconducibilità diventa impossibile effettuare una *clusterizzazione* che tenga conto dell'individuo che ha compiuto una serie di azioni, rendendo parimenti impossibile effettuare tutte le valutazioni espresse in premessa, al netto di quelle che non prevedono raggruppamenti per individui. Si ritiene, pertanto, che nel caso di specie l'adozione di tecniche di pseudonimizzazione sia decisamente più appropriata, poiché questa potrebbe essere sufficiente a rendere il software rispettoso della normativa senza perdere alcuna informazione circa la riconducibilità dei dati a un determinato individuo.

Tecnicamente, tale obiettivo potrebbe essere raggiunto tramite l'applicazione di un algoritmo (cd. *hashing*) che trasformi il codice utente trasmesso dal concessionario e memorizzato dal provider in un diverso codice. Ciò, in particolare, avviene in modo da non poter essere effettuato il calcolo inverso, così da rendere impossibile l'operazione di ricostruire il codice utente di partenza sulla base del codice calcolato in fase di *hashing*. L'esito di questa prima operazione consentirebbe di mantenere il collegamento fra i dati relativi alle varie sessioni di gioco e i singoli utenti, senza però consentire l'identificazione di questi ultimi.

Con riferimento, poi, alle elaborazioni possibili tramite la *clusterizzazione*, si ritiene che l'unico rischio concreto di mancato rispetto della normativa sarebbe dato dalla potenziale identificazione di dati personali o dell'identità di un utente tramite *query* appositamente formulate; in sostanza, potrebbero verificarsi situazioni nelle quali restringendo sufficientemente le chiavi di ricerca si potrebbe ottenere un *single-out*, ovvero una risposta contenente una singola voce.

Ciò, sebbene sarebbe impossibile da ottenere solo usando il software in parola, potrebbe però essere ottenuto incrociando i dati elaborati dal software con dati reperibili altrove, ad esempio tramite piattaforme di *open data*. Tale rischio può

essere ridotto adottando tecniche di *Differential Privacy*[112], così da impedire *in nuce* l'ottenimento di risposte aventi ad oggetto un singolo individuo. Ciò detto, deve essere osservato che il software considerato presenta pochissimi elementi che è possibile circostanziare con dati esterni alla piattaforma di gioco: al di là dei dati più squisitamente attinenti al gioco, uno di quelli che potrebbero essere confrontabili è la durata della singola sessione di gioco, intesa come orario di inizio e di fine sessione, che potrebbe essere confrontata con altri elementi pubblicamente disponibili (un post, un tweet, un messaggio di qualche tipo rilasciato in chiaro sul sito del concessionario, per esempio) al fine di identificare un determinato soggetto.

Allo scopo di rendere del tutto impossibile l'identificazione di un soggetto nelle modalità suddette una diversa soluzione, più semplice da implementare rispetto a quella precedentemente esposta, potrebbe essere quella di fare in modo che il software in analisi non consideri come *input* valutabile la durata della sessione in un formato che consenta di identificare un dato momento (data e ora, per esempio), bensì in termini di tempo assoluto (ore, minuti e secondi).

Questa stessa operazione dovrebbe essere fatta per qualsiasi dato che, in via potenziale, potrebbe essere confrontato con elementi esterni alla piattaforma di gioco, così da rendere impossibile la ricostruzione dell'identità dell'interessato. Circa il rispetto del principio di minimizzazione, infine, Tuko, avendo eliminato la possibilità di risalire all'identità dell'interessato potrebbe conservare i dati risultanti dalle analisi effettuate per un tempo indefinito, non trattandosi più di dati definibili come personali ai sensi della norma; ciononostante, dato che potrebbe ad un certo punto diventare possibile ricalcolare all'inverso gli *hash* ottenuti in fase

[112] Si tratta di una metodologia che integra "*i benefici delle tecniche di generalizzazione e randomizzazione, in quanto prevede un meccanismo di accesso ai dati basato su interrogazioni (query based mechanism) e non sulla pubblicazione di dati aggregati o randomizzati (sanitized data), ed è molto robusta rispetto alla possibilità di impiegare informazioni ausiliarie (anche pubblicamente disponibili) per la re-identificazione*", Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2020. Per un'applicazione della tecnica in parola a dispositivi iOs si veda https://appleinsider.com/articles/16/06/20/apples-differential-privacy-analyzes-the-group-protects-the-individual.

di pseudonimizzazione, è comunque opportuno che i dati siano memorizzati solo per il tempo necessario alla loro analisi.

Se, ad esempio, l'obiettivo dell'analisi è la *fraud detection*, una volta escluso il verificarsi di comportamenti illeciti è possibile cancellare i dati alla base dell'analisi; nel caso di analisi di marketing, si potrebbero conservare solo le osservazioni finali dei dati, eliminando tutto ciò che sarebbe alla base di detta analisi.

2.5. *Sull'uso esterno*

I concessionari di gioco, clienti di Tuko, potrebbero voler utilizzare la piattaforma per una serie di differenti utilizzi: analisi di marketing volte allo sviluppo di politiche di promozione di determinati giochi, analisi di utilizzo di tipologie di giochi differenti finalizzate allo sviluppo di politiche decisionali del *management*, controllo di possibili indicatori di dipendenza dal gioco d'azzardo e analisi di *fraud detection* sono solo alcuni esempi delle possibilità, sostanzialmente dipendenti dalle concrete possibilità di interconnessione dei sistemi del concessionario con il software in analisi. Per il concessionario quanto più il software sviluppato da Tuko è in grado di accettare dati provenienti da qualsiasi sessione di gioco – includendo, eventualmente, quelle tenute presso piattaforme di proprietà di altri provider – tanto più risulta uno strumento utile, perché può essere adattato alla propria fenomenologia aziendale.

Il mercato dei provider di gioco è assai variegato: i player del settore non sono molti, in realtà. Oltre a Tuko vi sono molteplici provider attivi nel mercato di riferimento, come ad esempio NetEnt, Microgaming, Playtech, Merkur, Novoline, IGT, Amaya e IsoftBet. Ogni provider, naturalmente, ha la sua piattaforma e offre una serie di giochi online di vario tipo; la dimensione di ognuno, peraltro, è molto variabile; nella breve elencazione sopra proposta, ad esempio, sono contemporaneamente presenti multinazionali e piccole società familiari. I concessionari, d'altra parte, cercano di offrire ai propri clienti la maggior quantità

possibile di giochi per mantenere l'offerta quanto più varia possibile e consentire a tutti di trovare un gioco che rispetti il gusto personale.

La quantità di dati raccolta dal concessionario, sulla base di quanto detto, è notevole, dato che il meccanismo di comunicazione è sostanzialmente lo stesso esplicitato sopra per ognuno dei provider elencati. Il software sviluppato da Tuko vuole proporsi come strumento utile al management, sia con finalità di marketing che con finalità più strettamente inerenti le integrazioni con questo o quel provider e/o lo sviluppo di un determinato gioco. Qualsiasi concessionario, pertanto, potrebbe considerare utile il software, a maggior ragione se potesse utilizzarlo in generale per tutta l'attività dei propri utenti e non solo per quella svolta sulla piattaforma di Tuko.

Le problematiche affrontate in questo caso, rispetto a quello relativo all'uso interno del software, sono evidentemente differenti e molteplici. Intanto, il concessionario non ha la stessa utilità se deve utilizzare il software di Tuko con dati pseudonimizzati: in questo modo potrebbe indirizzare determinate politiche circa l'offerta di gioco, ma gli sarebbe impossibile applicare qualsiasi discorso di marketing diretto ad incentivare determinati utenti sulla base delle proprie sessioni di gioco, come anche effettuare l'analisi dei comportamenti degli utenti alla ricerca di possibili fenomeni di dipendenza da gioco d'azzardo. L'identificazione, pertanto, è un elemento che, sebbene non sia essenziale all'offerta del software in parola, diviene comunque estremamente importante per l'appetibilità del software agli occhi dei clienti di Tuko.

La mancata pseudonimizzazione del dato comporta, sostanzialmente, che l'attività che viene svolta è a tutti gli effetti considerabile come profilazione ai sensi del primo paragrafo dell'art. 22 del GDPR. Il concessionario, titolare del trattamento, deve pertanto preventivamente informare l'interessato, ovvero il suo cliente, che ha intenzione di elaborare i dati raccolti in sede di sessione di gioco per effettuare attività di profilazione[113]. Dato che ciò è già previsto dallo schema

[113] Preliminarmente, è bene rilevare che per profilazione, a norma del numero 4) del paragrafo 1 dell'art. 4 del GDPR, si intende *"qualsiasi forma di trattamento automatizzato di dati personali consistente*

di contratto di gioco utilizzato, si ritiene che gli accorgimenti da adottare per adempiere al suddetto obbligo siano facilmente organizzabili da un punto di vista tecnico, magari inviando una e-mail ai clienti già iscritti dove li si informa della possibilità di concedere questo tipo di autorizzazione accedendo alla propria area personale.

Si ritiene che informarli della circostanza che l'autorizzare il trattamento potrebbe dargli diritto, sulla base delle attività di profilazione svolte, a specifici bonus non significherebbe in alcun modo rendere il consenso non liberamente concesso, poiché non si reca nessun *vulnus* al cliente che non desidera concederlo, limitandosi a prevedere particolari *benefit* a chi invece desidera farlo. Per consentire al concessionario di utilizzare il software potrebbe essere aperto un *web service* che fungesse da *frontend* per tutte le operazioni di inserimento dati e di configurazione dei principali aspetti di clusterizzazione. L'interfaccia non necessariamente prevederebbe funzioni avanzate (come per esempio l'impostazione personalizzata di *k*) ma servirebbe principalmente a dare al concessionario la possibilità di personalizzare le funzioni del software in considerazione dell'oggetto del quale si vuole approfondire la conoscenza: ad esempio se si vuole conoscere l'utilizzo di un determinato gioco piuttosto che di un altro sulla base dell'età anagrafica o degli spin o dell'importo medio giocato o se si vuole confrontare la durata della sessione di gioco in relazione alla puntata media si deve poter configurare il software di conseguenza.

Un altro modo di utilizzare il software da parte del concessionario sarebbe quello di trasmettergli in modo trasparente – cioè man mano che i dati vengono nella disponibilità del concessionario stesso, ad esempio durante una sessione di

---

nell'utilizzo di tali dati personali 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 di detta persona fisica". Questa eventualità è peraltro prevista dal comma 2 dell'articolo 20 della convenzione stipulata fra ADM e il Concessionario stesso, dove si prevede che *"qualora il concessionario, […], intenda trattare i dati personali del cliente per ulteriori e diverse finalità, quali, a titolo esemplificativo, ma non esaustivo, profilazione e cessione dei dati del cliente a terzi, dovrà informare preventivamente il cliente, raccogliendone, ove necessario, il relativo esplicito consenso"*; si richiama, per completezza, quanto già detto sopra con riferimento al comma 4 dell'art. 18 del contratto di gioco.

gioco – tutti i dati di cui il concessionario vuole tenere conto in una fase successiva di elaborazione, tramite un servizio contattabile direttamente dai sistemi automatici del concessionario che sovrintendono alle sessioni di gioco. Questa funzionalità sarebbe necessaria, ad esempio, qualora il concessionario volesse analizzare le modalità di utilizzo di giochi non presenti sulla piattaforma di Tuko in tempo reale (per esempio per le sopracitate finalità di *fraud detection* o per la rilevazione di schemi riconducibili alla dipendenza da gioco).

In entrambi i casi i dati verrebbero trasmessi dal concessionario, titolare del trattamento, a Tuko, la quale non ha alcuna autorizzazione da parte degli interessati. In altre parole, Tuko si troverebbe a trattare dati personali per conto del titolare del trattamento, ovvero del concessionario; ciò, conseguentemente, la configurerebbe come responsabile del trattamento[114]. Tale circostanza renderebbe necessario integrare il contratto fra provider e concessionario prevedendo che il primo si vincoli al secondo nella qualità di responsabile del trattamento, definendo con precisione la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, ai sensi dell'art. 28 del GDPR.

Il contratto, inoltre, dovrebbe prevedere che il provider tratti i dati personali secondo le indicazioni fornite dal concessionario di gioco, assicuri che tutte le persone autorizzate al trattamento dei dati siano vincolate da un accordo di riservatezza, garantisca la sicurezza del trattamento in termini di misure tecniche e organizzative adeguate, tali da garantire la cifratura dei dati, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, il tempestivo ripristino dei sistemi in caso di guasto fisico o tecnico dell'accessibilità e della disponibilità dei dati personali e l'implementazione e l'adozione di una procedura atta a verificare il corretto funzionamento dei sistemi di sicurezza di protezione dei dati personali.

[114] Cfr. numero 8), paragrafo 1, art. 4 del GDPR.

Il provider, inoltre, dovrebbe collaborare con il titolare del trattamento per consentirgli di adempiere ai propri obblighi in caso un interessato intenda esercitare i diritti di cui al Capo III del GDPR; dovrebbe, inoltre, assisterlo nell'adempimento degli obblighi di comunicazione previsti in caso di sottrazione o accesso non autorizzato ai dati personali, sia nei confronti degli interessati che delle autorità di garanzia. Tenuto conto delle finalità del software, ovvero quello di costituire uno strumento quanto più flessibile possibile per le esigenze del concessionario, è evidente che Tuko non ha alcun interesse a ritenere dati per più tempo di quanto strettamente necessario alla loro elaborazione da parte del concessionario. Tale circostanza, anche in accordo a quanto stabilito alla lettera g) del paragrafo 3 dell'art. 28, deve essere esplicitata differentemente a seconda che la raccolta e l'elaborazione dei dati sia contestuale, avvenendo tramite interfaccia web, oppure sia successiva alla raccolta effettuata in tempo reale, tramite servizio contattabile dal concessionario.

Nel primo caso è evidente che la soluzione è più semplice da adottare, da un punto di vista tecnico, poiché basta prevedere che quando il concessionario prelevi i dati che ha ottenuto dalla piattaforma scelga se cancellarli dalla stessa o lasciarli memorizzati, onde poterli riutilizzare. Nel secondo caso la scelta dovrà essere posticipata alla elaborazione dei dati, poiché questa non è contestuale alla raccolta. L'elaborazione, peraltro, potrebbe anche avvenire in un momento di molto successivo a quello della raccolta, o non avvenire affatto: il concessionario, per ottenere la possibilità di avere comunque i dati a disposizione, potrebbe configurare i propri sistemi affinché passino automaticamente i dati al software di I.A., indipendentemente dalla effettiva volontà di elaborarli.

Ciò potrebbe comportare, ai fini della normativa privacy, un'indebita memorizzazione di dati personali per un tempo ingiustificatamente lungo. In ossequio del principio di minimizzazione già richiamato più volte, sarebbe necessario per il provider prevedere, nel contratto con il concessionario, un periodo massimo di memorizzazione oltre il quale i dati vengono cancellati indipendentemente dal fatto che siano stati utilizzati, insieme a tutte le copie a

qualsiasi titolo detenute dal provider; prima della cancellazione i dati dovrebbero essere inviati al concessionario, così da restituirglieli e renderlo edotto dell'avvenuto processo. Tutta l'attività svolta sulla piattaforma dovrebbe poi essere rendicontata e organizzata in forma di registro, anche con riferimento a quanto previsto dall'art. 30 del GDPR[115], in modo del tutto automatico e trasparente al concessionario.

Tale adempimento può essere organizzato tecnicamente mediante l'utilizzo di file di *log* strutturati per rispondere esattamente al contenuto stabilito dalla normativa surrichiamata. In fase di contratto, peraltro, il provider dovrebbe raccogliere tutte le informazioni utili alla compilazione del registro delle categorie di attività relative al trattamento svolte per conto del concessionario[116]. Detti registri non sono necessari qualora il trattamento sia effettuato ad opera di imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10, secondo quanto previsto dall'ultimo paragrafo dell'art. 30 del GDPR.

---

115 *"Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1".*

116 *"a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.", paragrafo 2, art. 30, GDPR.

Si ritiene, nel caso di specie, che il trattamento operato dal provider non possa in alcun modo definirsi come occasionale; esso, infatti, è effettuato sulla base di un contratto di servizio con il concessionario di gioco ed è sostanzialmente indispensabile al corretto funzionamento del software di I.A. il cui utilizzo si concede in licenza. Sulla base di quanto detto, si ritiene che sussista l'obbligatorietà della tenuta dei registri summenzionati e che possa essere adempiuta in fase di programmazione del software strutturando adeguatamente i file di *log*. In ultimo, con riferimento all'uso esterno del software si ritiene opportuno effettuare una riflessione circa l'utilizzo che il concessionario potrebbe fare al fine di profilare un singolo utente.

Il contesto giuridico entro il quale si muove il concessionario di gioco è sostanzialmente diverso da quello analizzato per il provider ai fini dell'uso interno: il primo è direttamente e specificamente autorizzato dall'interessato ad effettuare attività di profilazione, mentre il secondo no. Anche in qualità di responsabile del trattamento egli tratta i dati personali nella misura e con le modalità specificate dal titolare; qualora, infatti, utilizzasse i dati raccolti in altro modo si configurerebbe l'ipotesi di cui al paragrafo 10 dell'art. 2, con la conseguenza che il provider rivestirebbe il ruolo di titolare del trattamento (o di contitolare, ai sensi dell'art. 26).

Non si pone, pertanto, il problema di limitare il risultato dell'analisi dei dati ad un singolo utente (il fenomeno del cd. s*ingleouting* richiamato sopra); ciò, anzi, potrebbe consentire al concessionario di porre in essere azioni di contrasto alla dipendenza da gioco di azzardo o di *fraud detection*. Va considerato che qualsiasi decisione presa dal concessionario sulla base della profilazione effettuata tramite il software di I.A., benché dietro consenso esplicito dell'interessato, potrebbe dover essere spiegata all'interessato che lo chiedesse eventualmente; nel fornire adeguate spiegazioni, il provider gestore del software di I.A., nella qualità di responsabile del trattamento, dovrebbe fornire al titolare tutta l'assistenza tecnica necessaria a giustificare le modalità di analisi dei dati alla base della decisione

assunta, conformemente a quanto stabilito in sede di contratto tra provider e concessionario.

Conclusioni

Dalla disamina della fattispecie concreta e dalle analisi condotte finora sono possibili alcune riflessioni. Il regolamento UE 2016/679, conosciuto come *General Data Protection Regulation*, procedendo sul solco già tracciato dalla normativa precedente, nel fissare nuovi *standard* ai quali attenersi per la tutela dei dati personali dei cittadini europei impone un cambiamento del modo di pensare e, quindi, di strutturare e organizzare il lavoro precedente le fasi di realizzazione di qualsiasi *software*, specialmente se questo è basato su algoritmi di intelligenza artificiale.

Le tematiche affrontate, infatti, sono costituite da almeno due aspetti principali: le competenze necessarie in fase di progettazione *software*, tenuto conto della complessità della normativa vigente, e gli strumenti di protezione *privacy* disponibili ai progettisti e ai programmatori in fase di realizzazione. Circa le prime, il GDPR impone un cambio di passo: è necessario un approccio multidisciplinare, ottenibile solo tramite la compresenza di più figure professionali che diano ognuna il proprio apporto tecnico ed esperienziale ad un processo sempre più complesso come quello di realizzazione di una intelligenza artificiale. Ciò è necessario per garantire il rispetto, prima che di ogni altra cosa, della *ratio legis* della quale è informata la norma europea in esame.

Non ci si può dimenticare, infatti, che il legislatore europeo, anche aiutandosi con i 173 considerando, ha inteso delineare un'area di movimento (un *framework*, volendo usare un inglesismo) all'interno della quale sono fissate regole precise per tutti i soggetti coinvolti. È ormai evidente come la spinta delle aziende all'ottenimento e all'utilizzo, quanto più libero possibile, dei dati personali degli utenti sia fortissima, esercitata a tutti i livelli, talvolta da aziende con fatturati di molto superiori al PIL della maggior parte delle Nazioni del mondo[117]. Questo ha reso estremamente urgente ridefinire il rapporto fra azienda e consumatore, in

[117] Amazon ha conseguito, nel 2021, ricavi per un totale di 469,82 miliardi di dollari, inferiore solo al PIL di 26 Stati su 197.

primis, e fra progettazione e programmazione delle applicazioni e legislazione vigente, in *secundis*. Circa gli strumenti di protezione *privacy* si sta cercando di intervenire su due diversi fronti: uno è costituito dalle sedi di normazione, nelle quali si stanno affrontando argomenti di carattere etico, alla ricerca di un approccio che possa essere condiviso e abbastanza delineato da poter essere imposto secondo una norma di diritto[118], mentre l'altro è costituito dalla dottrina, la quale cerca sempre nuove strade e nuove tecniche per introdurre, all'interno dei *software*, tecnologie che consentano in modo nativo e oggettivo (quindi sicuro) il rispetto di alcuni principi alla base della normativa *privacy*[119]. Ciò è ancor più vero se si considera il ritmo di crescita del settore correlato all'Intelligenza Artificiale: Gartner, in proposito, stima che entro la fine del 2022 il settore varrà complessivamente 3.9 milioni di miliardi di dollari, ovvero cinque volte il valore del 2017[120].

Nello specifico, le attività di ricerca svolte presso l'azienda ospitante hanno consentito di definire un *framework* giuridico all'interno del quale la stessa può muoversi, se lo desidera, per implementare il sistema di analisi basato su algoritmi di intelligenza artificiale compiutamente descritto nel terzo capitolo. Si ritiene, ad ogni modo, che un ulteriore approfondimento sarebbe di sicuro giovamento sia alle attività di sviluppo, atteso il mutare quasi frenetico della normativa di riferimento, sia alla possibile attenuazione di parte degli obblighi normativi vigenti, ad esempio valutando l'adozione di figure professionali a garanzia dell'interessato (come potrebbe essere, ad esempio, il *Data Protection Officer*).

Queste stesse riflessioni, tuttavia, spingono a considerare di quanto sia stata ormai superata la fase di uno sviluppo iniziale della tecnologia, che spingeva molti a considerarla come un qualcosa più attinente alla fantascienza che ad applicazioni

---

[118] Ci si riferisce, ad esempio, al *libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia,* il quale delinea alcuni importanti aspetti su come dovrebbe funzionare un *software* di intelligenza artificiale, cosa dovrebbe essere in grado di spiegare e quali distorsioni cognitive dovrebbe evitare di incorporare in sé.

[119] A questo mira il concetto della cd. *Trustworthiness-by-Design* menzionato alla fine del primo capitolo.

[120] https://www.gartner.com/en/newsroom/press-releases/2018-04-25-gartner-says-global-artificial-intelligence-business-value-to-reach-1-point-2-trillion-in-2018.

concrete e presenti nelle realtà quotidiane di chiunque[121]. L'intelligenza artificiale è una realtà ed uno strumento, e come tutti gli strumenti è buono o cattivo a seconda di come viene usato: il diritto, ancora una volta, è chiamato a sorvegliare su utilizzatori e sviluppatori, nel pedissequo e instancabile bilanciamento dei valori che, da sempre, lo mette a garanzia del sistema democratico.

[121] Si pensi alla presenza degli assistenti vocali di Apple, Microsoft, Amazon e Google nelle case di miliardi di persone.

Bibliografia

1) Adel A., Bahattab A., *A comparison between three SDLC models waterfall model, spiral model, and Incremental/Iterative model,* International Journal of Computer Science Issues (IJCSI), 2015, 12.1.
2) Angwin J., Larson J., Mattu S., Kirchner L., *Machine bias: there's software used across the country to predict future criminals. And it's biased against blacks,* ProPublica, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
3) Barzilay R., *Artificial intelligence: implications for business strategy*, MIT-CSAIL, 2017, https://www.csail.mit.edu/.
4) Brown C., *How To Use Digital Virtual Assistants In Your Startup*, Forbes, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/03/12/how-to-use-digital-virtual-assistants-in-your-startup/#7837899e1071.
5) Coughlin J. e Yoquinto L., *The Long Road Home*, slate.com, 2015, https://slate.com/technology/2015/05/autonomous-cars-and-the-future-of-the-commute.html.
6) Coughlin J. F., *Driverless Cars Will be a Social Rather Than Technological Revolution*, Big Think, 2016, https://bigthink.com/the-present/driverless-cars-will-be-a-social-rather-than-technological-revolution/.
7) Chui, M., Malhotra, S.: AI adoption advances, but foundational barriers remain, McKinsey. https://www.mckinsey.com/featured-insights/artificial-intelligence/ai-adoption-advances-but-foundational-barriers-remain (2018)
8) DuVergne Smith N., *New AI tool improves cognitive testing,* MIT News, 2017, https://news.mit.edu/2017/new-ai-tool-improves-cognitive-testing-0310.
9) El Khoury A., "*Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat*", European Journal of Risk Regulation, 2017, volume 8.

10) European Commission, *Ethics guielines for trustworthy AI,* 2018, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
11) European Union Agency for Network and Information Security (ENISA), *Privacy and Data Protection by Design – from policy to engineering*, 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
12) Gamma E., Helm R., Johnson R., Vlissides J., *Design Patterns - Elements of Reusable Object-Oriented Software*, 1995, Boston.
13) Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2020.
14) Gomez-Uribe C. A., Hunt N., *The Netflix Recommender System: Algorithms, Business Value, and Innovation*, ACM Trans. Manage. Inf. Syst., 2016, 6, 4, Articolo n. 13.
15) Goodfellow I., Bengio Y., Courville A., *Deep Learning*, 2016, Boston.
16) Goodman J., *Get used to virtual assistants in business life*, Raconteur, 2016, https://www.raconteur.net/get-used-to-virtual-assistants-in-business-life/.
17) Gruppo di lavoro articolo 29 per la protezione dei dati, parere 8/2001 sul trattamento dei dati personali nell'ambito dei rapporti di lavoro, WP 48, Bruxelles, 13 settembre 2001.
18) Gruppo di lavoro articolo 29 per la protezione dei dati, documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995, WP 114, Bruxelles, 25 novembre 2005.
19) Gruppo di lavoro articolo 29 per la protezione dei dati, Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), WP 131, Bruxelles, 15 febbraio 2007.
20) Gruppo di lavoro articolo 29 per la protezione dei dati, parere 4/2007 sul concetto di dati personali, WP 136, 20 giugno 2007.
21) Gruppo di lavoro articolo 29 per la protezione dei dati, parere 15/2011 sulla definizione di consenso, WP 187, Bruxelles, 13 luglio 2011.

22) Gruppo di lavoro articolo 29 per la protezione dei dati, parere 5/2014 sulle tecniche di anonimizzazione, WP216, 10 aprile 2014.
23) Gruppo di lavoro articolo 29 per la protezione dei dati, parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, Bruxelles, 8 giugno 2017.
24) Gruppo di lavoro articolo 29 per la protezione dei dati*, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 2017.
25) Hafiz. M., *A collection of privacy design patterns,* Proceedings of the 2006 conference on Pattern languages of programs, 2006, New York.
26) Hamon R., Junklewitz H., Sanchez I., Malgieri G., De Hert P., *Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making*, Ieee Computational Intelligence Magazine, 2022, Volume 17 – numero 1.
27) IBM Cloud Education, *Conversational AI*, IBM Cloud Learn Hub, 2020, https://www.ibm.com/cloud/learn/conversational-ai.
28) IBM Cloud*, Natural Language Understanding*, 2020, https://natural-language-understanding-demo.ng.bluemix.net/?cm_mc_uid=61913652150015064305656&cm_mc_sid_50200000=1508796017&cm_mc_sid_52640000=1508796017.
29) Khandani A. E., Kim A. J., Lo A., *Consumer credit-risk models via machine-learning algorithms*, Journal of Banking and Finance, 2010, vol. 34, issue 11.
30) Knorr E., *How PayPal beats the bad guys with machine learning*, Infoworld, 2015, https://www.infoworld.com/article/2907877/how-paypal-reduces-fraud-with-machine-learning.html
31) Lake K., *Stitch Fix's CEO on Selling Personal Style to the Mass Market*, Harvard Business Review, 2018, https://hbr.org/2018/05/stitch-fixs-ceo-on-selling-personal-style-to-the-mass-market.

32) Lui A., Lamb G. W., *Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector*, Information & Communications Technology Law, 2018, 27:3

33) Malone T., *Artificial intelligence: implications for business strategy*, MIT-CSAIL, 2017, https://www.csail.mit.edu/.

34) Marr B., *What Is Deep Learning AI? A Simple Guide With 8 Practical Examples*, Forbes, 2018, https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/#52f9a1f8d4ba.

35) Minsky M., *Steps towards artificial intelligence,* Proceedings of the IRE, 1961, Volume 49, Numero 1.

36) Minsky M., *The Emotion Machine: Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind*, 2007, New York.

37) Mitchell T., *Machine Learning*, 1997, New York.

38) Nadkarni P. M., Ohno-Machado L., Chapman W. W., *Natural language processing: an introduction*, Journal of the American Medical Informatics Association (JAMIA), 2011, Volume 18, edizione quinta.

39) nAnalyze*, Narrative Science Employs Natural Language Generation*, 2017, https://www.nanalyze.com/2017/01/narrative-science-natural-language-generation/.

40) Ohlhorst F. J., *Amazon Alexa Poised to Bring Natural Language Processing to Businesses*, Gigaom, 2017, https://gigaom.com/2017/01/10/rocketalexa1/.

41) Olson P., *This Startup's Artificial Voice Sounds Almost Indistinguishable From A Human's*, Forbes, 2017, https://www.forbes.com/sites/parmyolson/2017/11/03/this-startups-artificial-voice-sounds-almost-indistinguishable-from-a-humans/#69cfb3cc388c.

42) Pearson S., Benameur A., *Decision support for design for privacy: A system focused on privacy by policy*, *Privacy and Identity Management for Life*,

IFIP International Federation for Information Processing, 2011, volume 352 of IFIP AICT.

43) Pietropaoli S., *Scienza giuridica e tecnologie informatiche*, 2017, Torino.

44) Popper B., *The smart bots are coming and this one is brilliant*, The Verge, 2016, https://www.theverge.com/2016/4/7/11380470/amy-personal-digital-assistant-bot-ai-conversational.

45) Ransbotham S., Khodabandeh S., Fehling R., LaFountain B., Kiron D., *Winning with AI,* MIT Sloan Management Review and Boston Consulting Group, 2019.

46) Russel S. e Norvig P., *Artificial Intelligence: A Modern Approach (seconda ed.)*, 2003, Upper Saddle River, New Jersey.

47) Russel S. e Norvig P., *Artificial Intelligence: A Modern Approach (terza ed.)*, 2009, Upper Saddle River, New Jersey.

48) Sato K., *Using machine learning for insurance pricing optimization*, Google Cloud, 2017, https://cloud.google.com/blog/products/gcp/using-machine-learning-for-insurance-pricing-optimization.

49) Van Blarkom G. W., Borking J. J., Verhaar P.., *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents*, College bescherming persoonsgegevens, 2003, capitolo 3, L'Aia, Paesi Bassi.

50) WBR Insights, *How Stitch Fix Uses Data Science and Machine Learning to Deliver Personalization at Scale*, eTail, 2019, https://etailwest.wbresearch.com/blog/how-stitch-fix-uses-data-science-and-machine-learning-to-deliver-personalization-at-scale.

51) Wile R., *Wall Street Loves This Gadget That's Bringing The World Closer To Self-Driving Cars — Here's How It Works*, Business Insider, 2014, https://www.businessinsider.com/how-mobileye-technology-works-2014-8?r=US&IR=T.

52) Winston P., *Artificial intelligence: implications for business strategy*, MIT-CSAIL, 2017, https://www.csail.mit.edu/.

53) Woyke E., *Crystal Ball for Corn Crop Yields Will Revolutionize Commodity Trading*, Technology Review, 2016, https://www.technologyreview.com/2016/08/09/70472/crystal-ball-for-corn-crop-yields-will-revolutionize-commodity-trading/.