INDICE

Capitolo 2° - Le tecnologie della società digitale.

Capitolo 3° - I rapporti tra il GDPR e le IA: tra sicurezza e flessibilità.

Introduzione

«Qualunque tecnologia sufficientemente avanzata è indistinguibile dalla magia.»

Secondo il celebre scrittore britannico, Arthur C. Clarke, autore del ciclo “Odissea nello spazio”, questa frase, costituisce una delle tre leggi che ha guidato ogni suo romanzo. Questo dogma, seppur privo di un estrinseco carattere scientifico, ha un significato molto profondo perché l'uomo nello spingersi oltre i suoi limiti, alla ricerca della magia, ha trovato la tecnologia.

É l'immaginazione che prima di tutto guida il progresso, è quella capacità di spingersi, con la mente, oltre alla conoscenza per cercare dei nuovi obiettivi e poi trasformarli in realtà.

Dalla metà dello scorso secolo, grazie a scrittori, registi e filosofi, abbiamo visitato molti scenari futuristici dove la tecnologia avanzata, in grado di dare una soluzione permanente a numerosi problemi della vita, ha trasportato l'essere umano verso scenari che lo hanno costretto a mutare il suo modo di vivere, a volte con effetti totalmente distopici. Tutto questo ha creato terreno fertile per scienziati e ricercatori che, spinti dal desiderio di trasformare in realtà quelle macchine “perfette”, stanno oggi portando a casa i primi risultati di quegli studi, mostrando gli embrioni di Intelligenze Artificiali capaci altresì di ingannare l'essere umano sulla loro natura artificiale.

Tutti i dispositivi di questa era tecnologica, tuttavia, necessitano di grandi quantità di dati per poter esprimere le loro capacità elaborative. Attraverso i dati in archivio, le macchine possono confrontare, elaborare e riconoscere le informazioni in ingresso e fornire in uscita dei risultati coerenti.

Tutte queste informazioni vengono estrapolate dagli ambienti informatici più disparati e molto spesso sono personali, cioè si riferiscono a persone individuate o individuabili. Allo stesso tempo, va tenuta in debita considerazione il fatto che già dal 2010, con l'entrata in vigore del Trattato di Lisbona, la tutela dei dati personali è stata chiaramente definita un diritto fondamentale dell'Unione.

La necessaria tutela dei medesimi, unitamente alla circostanza che lo sviluppo tecnologico si nutre delle informazioni degli utenti, porta ad affrontare il tema della conciliabilità degli strumenti legislativi a disciplinare le mutate esigenze della realtà digitale.

Assumendo che il progresso informatico non sembra volersi arrestare, risulta di fondamentale importanza una normativa che offra tutele dinamiche dei diritti e libertà degli interessati e che sappia adattarsi alle nuove circostanze sociali. Senza opportuna regolazione, difatti, non si riuscirebbero a contenere gli scenari dispotici possibilmente derivabili dall'impiego di tali tecnologie.

Non è più la sola *privacy,* intesa quale diritto di non ingerenza sulla propria vita privata e familiare, ad essere tutelata ma l'intera gamma dei dati personali, ivi compresi quelli la cui indebita manipolazione non sia produttiva di pregiudizio sulla dignità personale.

Un'impostazione di tal genere risulta di particolare importanza poiché testimonia la maturata consapevolezza che non è più solo la nostra libertà ad essere potenzialmente in pericolo dalle nuove tecnologie ma perfino il diritto alla vita stesso (per assurdo, si immagini una macchina con guida autonoma manomessa da un pirata informatico).

L'obiettivo che posto in questo elaborato è lo studio, a livello giuridico e legale, dello sviluppo in questione e l'adeguatezza degli strumenti legislativi a nostra disposizione ad arginare questa rivoluzione informatica.

Il progresso non può arrestarsi e la perdita di alcuni diritti risulta logicamente conseguenziale, tuttavia, deve essere obiettivo degli ordinamenti moderni quello di ridurla ai minimi termini. In questa prospettiva si pone il nuovo Regolamento Europeo 679/2016 che , come si esaminerà in seguito, presenta questa duplice finalità: la liberalizzazione del mercato dei dati personali e la tutela dei diritti e libertà fondamentali delle persone fisiche.

Sarà oggetto di osservazione le modalià con cui viene affrontata questa sfida legislativa sopratutto in riferimento alle macchine Intelligenti che si stanno inserendo nel mercato. Verrà analizzato, in modo separato, prima la disciplina Europea, come definita dal Regolamento 679/2016, sottolineandone gli aspetti essenziali. Si vedranno i soggetti definiti dalla disciplina ed il ruolo che essi svolgono, partendo dall'Interessato e dai suoi diritti fondamentali, trattando poi le responsabilità del Titolare, comprese le condizioni che rendono lecito un trattamento di dati personali e, infine, verrà puntualizzato il ruolo di sorveglianza ed adeguamento svolto dalle Autorità di Controllo sulle singole attività.

Perimetrato lo scenario normativo generale entro cui deve svolgersi un'attività di tale calibro l'attenzione sarà focalizzata sugli strumenti di Intelligenza Artificiale immessi nel mercato e di quelli che, con elevate probabilità, si integreranno nella società. Verranno descritte, in particolare, le tecniche e gli algoritmi sfruttati da codeste macchine per la raccolta e l'elaborazione dei dati ossia i sistemi di *data analysis* che consentono di ricavare informazioni nuove da quelle che già possiede ed i dispositivi dell'*Internet of things*, i quali, in quanto connessi alla rete, riescono a comunicare e ricevere in modo autonomo i dati dagli altri dispositivi connessi.

Una volta definiti gli aspetti essenziali dell'argomento si potrà valutare l'impatto ed i risultati ottenuti dalla disciplina Europea nella gestione di queste nuove metodologie ed apparecchiature. Si osserverà come il panorama normativo si complichi al complicarsi delle attività poste in essere e delle tecnologie impiegate, consentendo da un lato una grande libertà di azione per il Titolare ma dall'altro un obbligo a garantire costantmente un adeguato livello di sicurezza.

L'unico modo per impedire gli epiloghi distopici che si sono prospettati, primo tra tutti il mondo Orwelliano governato dal “Grande Fratello” nel celebre libro “1984”, è quello di creare un contesto sociale e sopratutto normativo che, oltre a favorire il progresso, lo confini entro argini ben definiti, in modo da avere

contezza delle libertà a cui abbiamo rinunciato e dei diritti che ancora sono in nostro possesso per prevenire gli abusi e permettere che lo sviluppo avvenga nella legalità del sistema ma sopratutto nel rispetto della dignità umana.

CAPITOLO I

La disciplina Europea per la Protezione dei Dati Personali

1. Dalla *Privacy* alla Protezione dei dati personali.

Secondo quanto dichiarato da Stefano Rodotà, primo garante della privacy dal 1997 al 2005, nel libro "Intervista su privacy e libertà[1]" , la privacy viene definita per la prima volta nel 1890 da due celebri giuristi statunitensi Brandeis e Warren in una pubblicazione della Harvard School Review chiamata proprio "The Right Of Privacy[2]". La configurazione prospettata di questo diritto ricalcava la logica proprietaria dello ius excludendi alios e cioè del diritto di escludere terze persone dal godimento di un determinato bene della vita, in questo caso la vita stessa, intesa come quel groviglio di informazioni e di esperienze che ci compongono e ci definiscono.

Probabilmente i due giuristi non avrebbero mai immaginato di creare un diritto che sarebbe diventato così forte e diffuso col passare del tempo, essendo nato per proteggere la moglie di Warren dalla cronaca mondana che ritagliava numerosi articoli sulla vita salottiera della signora ma bisogna riconoscere che a distanza di oltre cent'anni, la loro definizione rimane più che attuale.

La Corte di Cassazione occupandosi di definire il concetto di *privacy* in un caso del 2010, infatti, ne ha dato la seguente definizione; "Privacy" è il diritto di scegliere cosa, del nostro spazio personale, vogliamo rendere conoscibile agli altri. La portata di questo diritto è ben esemplificata dall'immagine di un cancello chiuso. Tutto quello che sta dietro il cancello è privato, su tutto ciò che è al di fuori del cancello – nello spazio pubblico - viene meno la *reasonable privacy expectation* [3].

Da questo istituto, con il tempo e sopratutto grazie all' avanzare della tecnologia, ne è derivato un altro: "la protezione dei dati personali" che ha assunto in pochissimo tempo una configurazione fondamentale e autonoma. Tra privacy e protezione dei dati personali infatti non esiste un rapporto di identità di significato ma sono diritti contigui in quanto il secondo tutela solo le situazioni che non rientrano nel primo.

Nel dare un significato più preciso alla formula "protezione dei dati personali", soccorre il Considerando n. 15 del R. 679/2016 (noto anche come GDPR[4]) il quale afferma che "[...] La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. [...]".

Dunque nello spiegare questo rapporto di contiguità tra Privacy e Protezione dei dati vediamo che attraverso il primo, "selezioniamo" quale tipo di informazioni vogliamo rendere pubblico o tenere privato, il

1 RODOTÀ, Stefano; CONTI, Paolo. Intervista su privacy e libertà. GLF Editori Laterza, 2005.
2 HOFSTADTER, Samuel Harold, et al. The Right of Privacy. Central Book Company, 1964.
3 Cass. n. 40577/2008 e n. 47165/2010.
4 GDPR, acronimo per *Guidelines on Data Protection Regulation* (R. 679/2016).

secondo invece opera su quelle informazioni, ormai pubbliche, determinando come possono essere utilizzate ed eventualmente alienate a terze persone. Pertanto, rendere pubbliche delle informazione che ci riguardano non significa disinteresse verso le stesse e quindi consentire a trattamenti spietati o esagerati ma l'interessato mantiene anche su questi dati un elevato livello di controllo.

Il GDPR, come vedremo nei prossimi paragrafi, riesce ad integrare perfettamente questi due istituti mostrando con consapevolezza come entrambi i diritti si pongono sullo stesso piano ed entrambi vanno adeguatamente tutelati per permettere uno sviluppo solido di questo progresso.

1.2. La "nascita" dei Big Data.

L'ingresso degli elaboratori moderni nel contesto sociale oltre a mutare l'originario concetto di privacy ha mutato anche il concetto stesso di dato, inteso quale bene giuridico protetto dalle norme.

Originariamente la tutela dei dati si focalizzava quasi esclusivamente sui P.I.I.[5] e cioè su quei dati che permettevano l'identificazione di una persona specifica nel mondo. Proprio per questa capacità identificativa venivano ritenuti come potenzialmente lesivi della privacy in quanto vi si possono ricollegare dati anche piuttosto delicati riguardanti lo stato di salute, il casellario giudiziario o ancora, più in generale, notizie che il soggetto può ritenere lesive della propria dignità.

L'attuale Regolamento tiene debitamente, e in realtà esclusivamente, in conto la tutela di questa categoria di dati e ne da puntuale definizione all'art. 4, par. 1, del GDPR: "[...] qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale [...]".

Nel tutelare la dimensione individuale del dato, il GDPR però ne tiene conto anche nella sua veste aggregata e cioè volgendo lo sguardo al trattamento automatizzato di grandi quantità di dati che, nel mondo dell'informatica, viene denominato come "*Big Data"*.

Non esiste ad oggi una definizione universale di Big Data[6][7] ma esistono caratteristiche comuni a tali procedimenti. Secondo un'accurata tesi, descrive "l'insieme delle tecnologie e delle metodologie di analisi di grandi quantità di dati, ovvero la capacità di estrapolare, analizzare e mettere in relazione un'enorme mole di

5 Acronimo di *Personally Identifiable Information.*

6 Consiglio per una visione ampia e completa sui *Big Data* l'articolo pubblicato da Jennifer Dutcher sul sito dell'Università di Berkeley (https://datascience.berkeley.edu/what-is-big-data/) dove vengono raccolte definizioni di oltre 40 esperti del settore.

7 Uno studio molto interessante di Bob Hayes pubblicato sul "Business Broadway" (http://businessoverbroadway.com/2014/09/09/six-ways-to-define-big-data/), suddivide tutte le definizioni, contenute nell'articolo citato nella nota n. 8, di Big Data in sei possibili categorie in base a finalità.

dati eterogenei, strutturati e non strutturati, per scoprire i legami tra fenomeni diversi e prevedere quelli futuri".[8]

Dunque si può dire che un processo di Big Data si componga di due parti che interagiscono costantemente tra loro. La prima è costituita da una massiccia banca dati, ottenuta dalla somma di numerosissime informazioni[9] eterogenee che può essere strutturata secondo modelli logici, i cd. dataset, o non strutturata.

La seconda, è la capacità del sistema di catturare, gestire e analizzare le informazioni che contiene, o che ricerca da altre fonti[10], così da elaborarle ottenendo altre informazioni di contenuto che varia in base alle finalità del sistema stesso, i cd. "Dati dai Dati".

Questo tipo di processo sta assumendo una portata sempre più ampia nel mondo dell'informatica, creando sistemi in grado di prevedere, ad esempio, gli andamenti economici-politici[11], i gusti dei consumatori[12] o ancora l'avvento di catastrofi ambientali.

Il tipo di tutela accordata ai dati personali dal Regolamento Europeo tiene conto di questo fattore in modo decisivo e riconosce che la correttezza dei singoli dati offerti dagli utenti assumano un ruolo centrale nei sistemi Big Data poiché un informazione erronea provoca a sua volta previsioni distorte e ne riducono la funzionalità in modo decisivo. Per fare una metafora, l'informazione errata prolifera nel sistema come un tumore, danneggiandolo lentamente e progressivamente fino ad azzerarne ogni capacità predittiva.

Nel tutelare i singoli diritti e libertà degli interessati, riguardanti le loro informazioni personali, si tutela in realtà il sistema nel suo complesso. Ritengo che questa chiave di lettura sia fondamentale nel comprendere appieno alcune sfumature del sistema normativo, come ad esempio quelle dell'art. 5, lett. d) del GDPR "I dati sono, […] d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); [...]".

L'esattezza dei dati è sicuramente un elemento che tutela la posizione individuale dell'utente ma al tempo stesso permette di parametrarli in modo adeguato dalle macchine cosicché il suo utilizzo nei sistemi Big Data permetterà la fuoriuscita di dati più "giusti".

Nell'ottica di questa trattazione, il concetto ha un'importanza fondamentale e lo si capisce solo con una preliminare definizione funzionale di Intelligenza Artificiale (I.A.) intesa come quella capacità di calcolare, in poche frazioni di secondo, grandi quantità di dati così da ottenere soluzioni a problemi concreti

8 Andrea De Mauro, Marco Greco e Michele Grimaldi, A Formal definition of Big Data based on its essential features, in Library Review, vol. 65, nº 3, 2016.

9 Con i Big Data la mole dei dati è dell'ordine degli zettabyte (1'000'000'000'000'000'000'000 byte, cioè 1 triliardo di byte.).

10 Si veda, più avanti, la parte relativa all'*Internet of Things,* Capitolo 2, paragrafo 4.2.

11 Un esempio emblematico può essere lo scandalo *"Cambridge Analytics"* ma per approfondimenti (https://www.bbs.unibo.it/hp/elezioni-il-ruolo-dei-big-data-nelle-campagne-politiche-2/)

12 Sempre per richiamare un esempio: Netflix, con appositi algoritmi in grado di catturare i gusti dei suoi utenti, riesce a elaborare percentuali di compatibilità che un soggetto può avere con determinate serie TV o film, sulla base di quelle precedentemente viste/valutate.

per cui la macchina è stata ideata.

In conclusione la visione del GDPR deve sempre essere abbastanza ampia da comprendere anche la natura aggregata del dato, perchè, se incorretti e/o soggetti a trattamenti abusivi, ci possono danneggiare due volte, la prima rimane quella relativa alla sfera dei nostri diritti e libertà più intimi e la seconda riguarda il contesto informatico in cui viviamo, rendendo incorretti e poco funzionali le macchine che li elaborano.

2. Cambio di prospettiva del R. 679/2016 rispetto alla D 46/1995.

La tutela dei dati riguardanti una persona fisica viene considerata nel contesto Europeo come un diritto fondamentale e questo è dichiarato *expressis verbis* nell'Articolo 8 della Carta Europea dei diritti fondamentali dell'uomo (CEDU) che recita: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."

La normativa Europea precedente al Regolamento 679/2016, cosi come definita dalla Direttiva 96/45/CE, aveva proprio come cardine assoluto tale impostazione ed infatti, nel definire il suo oggetto, nell'Articolo 1 dichiara: "Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali."

Tuttavia la Direttiva, già riconosceva il ruolo ricoperto dai dati personali all'interno del mercato dell'Unione, specificando nel secondo comma dell'Art. 1 che: "Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1."

Si vede come già nel 1996, l'obiettivo del legislatore sovranazionale fosse quello di aprire il mercato interno al traffico dei dati personali seppure non in modo incisivo. Il Considerando n. 3 della Direttiva infatti sembra dare rilevanza al traffico dei dati personali solo in relazione al corretto funzionamento del mercato interno, configurandolo solo parzialmente come attività commerciale autonoma[13].

Il Regolamento eredita entrambe le finalità, ricercando però un equilibrio più stabile tra libertà di circolazione dei dati e tutela dei diritti e libertà fondamentali così come risulta chiaramente dall'Articolo 1, GDPR: "Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. [...]"

Se prima assumeva un ruolo primario la tutela delle persone fisiche, considerate dotate di diritti

13 "[...] considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona;"

proprietari rispetto ai dati che la riguardavano, oggi il libero traffico dei dati assume una rilevanza almeno parificata, come risulta dal Considerando n.7, secondo cui: "La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."

Tale parificazione ha comportato però la caduta della visione proprietaria del singolo sui suoi dati, portandola verso una tutela che si concretizza nella garanzia che il singolo mantenga sui dati un controllo effettivo. Questa è stata la posizione dell'*European Data-Protection Supervisor* nel noto parere 4/2015 che analizzando la struttura della società digitale ha sottolineato come sia inevitabile che i dati forniti per avere un servizio vengano trattati da una pluralità di soggetti collegati tra loro[14].

Allo scopo di permettere lo "sviluppo dell'economia digitale in tutto il mercato interno[15]", il regolamento ha alla sua base una concezione normativa dinamica e flessibile; mentre la direttiva ha posto al centro della sua normativa il dato personale e i diritti dell'interessato, il regolamento è strutturalmente incentrato sul titolare e la sua responsabilità. Una responsabilità che è incentrata sui rischi che i trattamenti posti in essere possono determinare, e la cui valutazione, dalla quale dipende anche l'individuazione delle misure di sicurezza da adottare, è sempre rimessa al titolare [16].

Quindi il focus normativo non è più l'interessato ed il suo diritto all'autodeterminazione informatica ma lo diventa il titolare del trattamento, in quanto è proprio nelle sue mani la ricerca del delicato equilibrio tra libera circolazione e rispetto dei diritti fondamentali.

Il cambio di prospettive del legislatore Europeo però si vede con molta più chiarezza nella scelta dello strumento normativo utilizzato per disciplinare la materia. Nel 1996 non si riuscì a percepire la rivoluzione che avrebbe comportato l'avvento del mondo digitale ed informativo e si approcciò la materia con una Direttiva[17], il cui scopo non è quello di creare un contesto normativo puntuale ma quello di armonizzare la materia con principi generali che vanno applicati negli Stati Membri dell'UE i quali, tuttavia, mantengono ogni libertà, nel rispetto di quei principi, di regolare specificamente, con legge interna, il settore.

Nonostante l'ambizioso proposito, tuttavia, il versante applicativo la direttiva *de qua* aveva permesso la frammentazione della protezione dei dati personali nel territorio dell'Unione, ed aveva favorito l'incertezza giuridica e la percezione che le operazioni online, in particolare, comportassero rischi per la

14 EDPS *Opinion 4/2015 towards a new digital ethics, Data, dignity and technology,* Settembre 2015.
15 Citando il Considerando (8) del GDPR.
16 *La protezione dei dati personali dalla direttiva al nuovo Regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni"* di Franco Pizzetti, rivista di diritto dei media, MediaLAWS.
17 Seguendo L'articolo 288 del TFUE " […] una direttiva è vincolante per i paesi destinatari (uno, alcuni o tutti) per quanto riguarda il risultato da raggiungere, lasciando alle autorità nazionali la scelta della forma e dei metodi [...]". Per approfondimenti https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3Al14527.

protezione delle persone fisiche[1819]. Questo vuoto normativo è stato colmato, sin dall'inizio degli anni settanta, dalla giurisprudenza della Corte europea di Giustizia[20], la quale, facendo leva sulle tradizioni costituzionali comuni degli Stati membri e sui principi affermati nella Convenzione europea per dei diritti dell'uomo (CEDU), ha riconosciuto la tutela dei diritti umani come parte integrante dell'ordinamento comunitario.

Tutto ciò, però, non risultava il contesto più adatto per il buon funzionamento del mercato interno ed appariva sempre più indispensabile l'adeguamento degli strumenti legislativi a tutela della privacy alla incessante sequenza di innovazioni tecnologiche, economiche e sociali[21]

Per infondere nei cittadini di tutti gli Stati Membri una nuova consapevolezza ed un contesto sicuro, come è avvenuto nelle altre libertà fondamentali del mercato comune UE[22], le istituzioni Europee hanno deciso di disciplinare la materia con uno strumento molto più decisivo, qual è il Regolamento[23]. Tale approccio, crea un contesto normativo comune e dettagliato, capace di applicarsi in ogni legislazione interna senza necessità di nessun atto legislativo di adattamento ma sopratutto, come vedremo, disciplina la materia in modo completo.

Tale scelta mostra una posizione molto più chiara ma si è resa possibile solo in tempi recenti dove si sono potuti analizzare gli sviluppi tecnologici e le carenze normative dell'ultimo ventennio così da adottare uno strumento funzionale ed efficiente, in grado di adattarsi ai mutamenti tecnologici che ci troveremo ad affrontare.

3. Ambito di applicazione del Regolamento.

Nei paragrafi precedenti[24] abbiamo analizzare l'oggetto e le finalità del nuovo GDPR che vengono puntualmente definite nell'articolo 1[25], adesso ne va specificato l'ambito di applicazione, sia materiale che

18 Per una lettura completa dell'argomento rimando alla lettura del sito http://www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.

19 Secondo delle stime del 2015 compiute dall' Eurobarometer, "L'81% degli europei ritiene di non avere il controllo completo dei propri dati personali online" e "solo il 24% degli europei ha fiducia nelle società attive online, quali i motori di ricerca, i siti delle reti sociali e i servizi di posta elettronica."

20 Il cui ruolo principale è proprio quello di garantire che il diritto dell'UE venga interpretato e applicato allo stesso modo in ogni paese europeo e di garantire che i paesi e le istituzioni dell'Unione rispettino la normativa dell'UE. (https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_it)

21 Tale necessità è sottolineata nella analisi di S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali,* Padova, 2006.

22 Mi riferisco ai 4 pilastri del mercato comune che si esprimono nella libera circolazione di beni, persone, servizi e capitali. A tal proposito, l'Articolo 26 del TFUE recita: "L'Unione adotta le misure destinate all'instaurazione o al funzionamento del mercato interno" ed ancora che "Il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni dei trattati."

23 Sempre l'Articolo 288 afferma che " […] Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. [...]" Vedi anche http://www.treccani.it/enciclopedia/regolamenti-diritto-dell-unione-europea/.

24 In particolare si vedano i paragrafi 2 e 3 di questo Capitolo.

25 "Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati

territoriale, e le modalità pratiche di attuazione.

L'approccio seguito dal legislatore Europeo è stato quello di estendere al massimo la portata applicativa del Regolamento così da ricomprendere ogni trattamento suscettibile di minacciare la tutela dei diritti e delle libertà degli interessati. Tale obiettivo è stato perseguito attraverso tre diverse strategie.

La prima di queste consiste nel definire nel modo più ampio alcuni concetti fondamentali quali quelli di dato personale e trattamento, così da ricomprendervi il maggior numero di situazioni. Secondo l'Articolo 4 del GDPR, dedicato proprio alle definizione di alcuni concetti fondamentali, per trattamento si intende: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come 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;".

Il trattamento si concretizza quindi con un'insieme di attività e viene concepito non tanto in riferimento al sistema informatico utilizzato, potendone anche prescindere, ma va ricercato guardando al suo oggetto che è sempre costituito da un "dato personale" o "insiemi di dati". Per evitare lacune, sempre l'Articolo 4 si occupa di dare una definizione ampissima anche di Dato Personale[26], qualificandolo come: "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;"

Il dato che viene tutelato non è solo quello suscettibile di ledere direttamente la nostra dignità o, più in generale, i nostri diritti ma è un qualsiasi dato che sia idoneo ad identificare un soggetto, sia in modo diretto che in modo indiretto. La sola capacità identificativa è idonea affinché si applichino le norme sul trattamento e questo lo si comprende bene analizzando il suo ambito di applicazione materiale indicato nell'Articolo 2: "Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a

personali, nonché norme relative alla libera circolazione di tali dati."

26 Bisogna però sottolineare che il Regolamento dedica poi un articolo a specificare che tra i dati personali esiste una categoria "particolare" il cui trattamento è, di regola, escluso. L'articolo 9 infatti nel prima paragrafo esplicita che "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.". Il secondo paragrafo inoltre elenca una lunga lista di casi in cui il divieto è escluso per i quali rimando alla lettura dell'articolo (https://www.privacyitalia.eu/wp-content/uploads/2017/10/GDPR_Italiano_PDF.pdf). Tra questi dati, dotati di particolare potenziale pregiudizievole per l'interessato, l'articolo 10 annovera anche quelli relativi a condanne penali e reati, stabilendo ulteriori condizioni per il loro trattamento come lo si evince dal testo che afferma "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica. "

figurarvi. “

Il secondo accorgimento per aumentare la tutela offerta dal Regolamento consiste nell'estenderne proprio la portata geografica anche oltre i confini dell'UE. Tuttavia, affinché tale ampliamento normativo possa operare sono necessarie delle condizioni, tra loro alternative, che vengono definite dettagliatamente nell'Articolo 3: “1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. 2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.”

Il terzo punto cruciale per consentire un'applicazione estesa del Regolamento è quello di individuare da quale momento le norme vincolano e regolano le attività del titolare ed i diritti dell'interessato. Mentre l'interessato può far valere i suoi diritti solo a seguito di un trattamento gia in corso, il GDPR prevede un *iter* preventivo che il titolare deve seguire, sotto la sua sua responsabilità, prima di far circolare i dati che si basa su informativa, consenso e valutazione d'impatto.

Per poter comprendere appieno quest'ultimo punto, tuttavia, va analizzata la disciplina nel dettaglio andando prima di tutto ad individuare i soggetti attivi ed il ruolo che la disciplina gli riserva.

4. Il GDPR ed i suoi protagonisti.

Come nella Direttiva 96/45/CE anche nel Regolamento 679/2016, tutto l'assetto normativo si articola attorno a tre figure principali: l'interessato, il titolare e l'Autorità di controllo. Ciò che muta nell'odierna disciplina sono però i ruoli ed i poteri a loro riconosciuti. Già nel terzo paragrafo abbiamo visto come nel Regolamento avviene un rovesciamento di caratterizzazione passando da un apparato normativo tutto incentrato sui diritti dell’interessato ad uno complementare basato sui doveri del titolare e del responsabile, dove il ruolo dell'Autorità di Controllo viene notevolmente rafforzato.

L'interessato è la persona fisica che vede i suoi dati trattati, così come è definito il trattamento nel GDPR[27]. Lo spartiacque quindi che porta la persona fisica a divenire interessato è proprio l'inizio di

27 «Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e

un'attività di trattamento di dati che lo riguardano, configurando così due diverse posizioni per il soggetto. Quando diviene interessato, questo ha molti poteri di controllo sui suoi dati potendo arrivare addirittura ad impedirne il trasferimento o richiedendone la cancellazione. Prima di tale momento, l'unico individuo in grado di accordare una tutela *ex ante*, verso la persona fisica, ma anche *ex post*, verso l'interessato, è proprio il titolare del trattamento[28].

Vediamo appunto come l'interessato si sia parzialmente svuotato del suo ruolo di protagonista assoluto. É il dato che viene tutelato *in primis* ed il soggetto cui si riferiscono tali informazioni viene protetto solo nel momento in cui un trattamento ha effettivamente inizio. Il baricentro dell'attività tutelata è proprio quella compiuta dal titolare sul dato e quindi l'interessato può fare valere i suoi diritti solo a seguito di tali operazioni e solo se queste siano state compiute *contra ius*.

La responsabilità nell'accordare tale tutela è definita proprio dall'articolo 24 che stabilisce: "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario."

Tale norma ha un'incidenza fondamentale perché chiarisce che il titolare deve sempre, dopo aver stabilità natura e finalità del trattamento e anche prima che questo inizi, adottare "misure tecniche" che, dovendosi conformare al regolamento, rispettino i diritti e libertà fondamentali delle persone fisiche. Quindi spetta proprio al titolare la protezione della posizione dei potenziali interessati in quella fase dove loro non hanno diritti da esercitare, vedremo più avanti che il frutto di tale adeguatezza si concretizza nella "valutazione dei rischi".

Al titolare, quale garante della posizione degli interessati, si pongono anche dei doveri di cooperazione e informazione così da rendere sempre trasparente la sua attività. Questi si palesano nell'articolo 12 : "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento, [...] con un linguaggio semplice e chiaro, [...] il titolare del trattamento agevola l'esercizio dei diritti dell'interessato. [...] Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo.[...]."

Da ultimo va poi analizzato il ruolo delle Autorità di controllo che è stato rivitalizzato e rafforzato.

---

applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu razione, 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;

28 L'articolo 4 del GDPR lo definisce come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; [...]".

Tali organismi vengono definiti, nell'articolo 4, come: “autorità pubbliche indipendenti[29] istituite da uno Stato membro ai sensi dell'articolo 51[30];” e hanno una serie molto eterogenea di funzioni che vengono dettagliatamente definite dall'Articolo 57[31]

Principalmente svolge funzioni di controllo, sorveglianza e consultive ma è chiamata anche a svolgere indagini, con ampi poteri, autonomamente o sulla base di reclami provenienti da terzi. Le Autorità di controllo, sono poi tenute a coordinarsi tra loro per definire una politica unica in materia di trattamento dati personali, in particolar modo per quelli transfrontalieri, dove si attiva obbligatoriamente il meccanismo

29 L'indipendenza e, di riflesso, la funzionalità di tale Autorità ricopre per il sistema nel suo complesso un elemento cardine e in tal senso si esprime l'articolo 52, il quale nei primi due commi, afferma: “1. Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.
2. Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno. “

30 Riportando il testo dell'articolo 51: “Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»). 2) Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII. 3) Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63. 4) Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

31 Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:
-sorveglia e assicura l'applicazione del presente regolamento;
-promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;
-fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
-promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
-su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;
-tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'ar ticolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;
-collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;
-svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;
-sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;
-adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
-redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'ar ticolo 35, paragrafo 4;
-offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;
-incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;
-incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;
-ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
-definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
-effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
-autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 46, paragrafo 3;
-approva le norme vincolanti d'impresa ai sensi dell'articolo 47;

di coerenza ex articolo 63[32].

Come appare chiaro dunque nell'obiettivo di perseguire la tutela del dato personale ognuno di questi soggetti svolge un ruolo essenziale tale che la loro cooperazione garantisce la perfetta funzionalità del sistema.

5. L' interessato ed i suoi diritti.

Abbiamo osservato che la posizione dell'interessato si concretizza solo a seguito di un trattamento di dati riguardanti il soggetto, prima di tale momento questi individui sono solo interessati potenziali. Il concetto ha una notevole rilevanza perché solo all'interessato in quanto tale il GDPR riconosce una lunga serie di diritti.

Prima di analizzarli tutti in dettaglio va osservato che questi si articolano in due diverse famiglie: la prima è legata ad una visione proprietaria del dato che ricalca il diritto all'autodeterminazione informatica ed il secondo che attribuisce una tutela fondata su un controllo delle informazioni che li riguardano. La discriminante va ricercata proprio nella base normativa su cui si fonda il trattamento stesso. L'articolo 6[33] del GDPR delinea le sei condizioni affinché si possa dire che un trattamento sia lecito, la prima di queste è il consenso.

In sintesi se il trattamento si basa sul consenso, oppure per eseguire un contratto, si delinea una visione proprietaria del dato, negli altri casi, non essendo necessario un consenso informato provato per iscritto, rimane all'interessato solo un potere di controllo.

La visione proprietaria del dato si concretizza proprio nella prestazione del consenso da parte dell'interessato; in armonia con il considerando 32[34] del Regolamento che, nel delineare le condizioni e le

-contribuisce alle attività del comitato;
-tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, par. 2; e
-svolge qualsiasi altro compito legato alla protezione dei dati personali.

32 Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione.

33 Secondo l'Articolo 6: "Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a)l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b)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;
c)il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d)il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è 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;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

34 Il testo del Considerando così recita: "Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale

modalità attraverso cui tale consenso debba essere prestato, prescrive che il titolare debba fornire la necessaria informativa[35] su cui lo stesso si basa così da rendere la scelta dell'interessato consapevole rispetto alle finalità del trattamento dati. L'espressione di questa dimensione proprietaria è completata da due ulteriori aspetti, uno relativo alle modalità di revoca dello stesso che può essere effettuata liberamente e in qualsiasi momento da parte dell'interessato, nella forma in cui lo ha prestato inizialmente come sottolinea l'Articolo 7.3 GDPR[36], e la seconda, dalla circostanza che il titolare deve sempre essere in grado di dimostrare che il consenso sia stato prestato, entrambe, anche disgiuntamente, incidono direttamente sulla liceità del trattamento[37].

Negli altri casi, la tutela affidata dal Capo II del GDPR si estrinseca in un potere di controllo affidato agli interessati: in questi casi infatti il trattamento è lecito anche al di fuori della volonta del soggetto potendo prescindere da una previa richiesta di consenso informato. L'interessato, in sostanza, non può opporsi all'*an* del trattamento ma può controllare il *quomodo* esso avviene e se risulta illecito può arrivare ad impedirlo o limitarlo.

Tale possibilità seppur sembra intragrarsi poco con la finalità di tutela di diritti fondamentali, permette di raggiungere in modo concreto quella libertà di circolazione dei dati personali e quel progresso dell' "economia digitale." Ciò però non significa essere senza tutele.

La protezione si esplica sostanzialmente in doveri di trasparenza[38] in capo al titolare, il quale, in accordo con l'articolo 12, deve: "adotta(re) misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13[39] e 14[40] e le comunicazioni di cui agli articoli da 15 a 22[41] e all'articolo 34[42] relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e

---

contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso."

35 Rispetto alle modalità con cui tale informativa deve essere prestata, l'articolo 7.2 GDPR così si esprime: "Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma compren sibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante. "

36 Articolo 7.3 GDPR :"L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato."

37 In accordo con l'articolo 7.1 GDPR: "1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali."

38 Ed in questa prospettiva si muove anche il Considerando 60 che afferma: "I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. "

39 Riguardante le informazioni da fornire qualore i dati siano raccolti presso l'interessato.

40 Riguardante le informazioni da fornire qualore i dati non siano raccolti presso l'interessato,

41 Si riferisce in questi articoli ai diritti degli interessato: diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto di notifica in caso di rettifica o cancellazione diritto di opposizione ed il diritto connesso ai processi decisionalizzati automatizzati compresa la profilazione.

42 Riguarda i casi in cui il titolare è tenuto ad informare l'interessato di eventuali violazioni dei dati personali, conseguenti al verificarsi di massicce perdite di dati (*data breaches*). Sul tema rimando alla lettura del paragrafi 3.3. e 3.4. del terzo Capitolo.

chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici" ed inoltre "agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22."

Tali doveri informativi specifici si pongono ad assicurare un controllo sui dati sia quando gli stessi vengano raccolti dall'interessato sia quando vengono raccolti presso altri.

In armonia con l'articolo 12.7 GDPR, le informazioni da dare a norma degli artt 13 e 14 non solo possono essere rilasciate con mezzi informatici ma possono anche essere "fornite in combinazione con icone strandardizzate[43] per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico."

Secondo alcuni autori, primo tra tutti Franco Pizzetti[44], tali icone strandardizzate, per quanto risultino apparentemente marginali, potranno ricoprire un ruolo piuttosto massiccio nello sviluppo delle intelligenze artificiali. Queste macchine saranno, e già lo sono per la verità, implementate con programmi in grado di raccogliere valutazioni dal mondo esterno per sintetizzarle in altre e nuove informazioni, complicando incredibilmente il trattamento dei dati e ampliando la tutela degli interessati con informative sempre più esaustive. Il baricentro tra questi trattamenti e le necessarie informative viene visto proprio in queste icone.

Rispetto al contenuto delle informazioni di cui si è discusso, va segnalato come gli articoli 13 e 14 stabiliscano tre norme fondamentali. La prima prevede che il titolare debba comunicare se ha "intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione"[45].

La seconda norma obbliga il titolare a dare comunicazione dell' "esistenza di un processo decisionale automatizzato, compresa la profilazione [...], e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato."[46]

La terza, legata fortemente all'evoluzione della ricerca e dello sviluppo tecnologico, infine, impone che "qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2."[47]

Solo per i casi in cui i dati non siano raccolti presso l'interessato soccorre una quarta regola, fondamentale nella logica della trasparenza dei trattamenti, che obbliga il titolare ad indicare "la fonte da cui

43 Mettere a disposizioni alcune immagini standardizzate che stanno a rappresentare l'attività che si svolge in quel luogo per darne un ampia informazione. Un esempio noto è il cartello che segnala la presenza di videosorveglianza.

44 D'Acquisto, G., Naldi, M., Bifulco, R., Pollicino, O., & Marco, B. (2018). Intelligenza artificiale, protezione dei dati personali e regolazione (Vol. 6). G Giappichelli Editore.

45 Come prevede il comma 1, lettera *f*) dell'articolo 13 e 14, rispettivamente se i dati vengono raccolti o meno presso l'interessato.

46 Confrontare il comma 2, lettera *f*) dell'articolo 13 e il comma 2, letterga *g*) dell'articolo 14, rispettivamente se i dati vengono raccolti o meno presso l'interessato.

47 Tale disposizione è stabilita dal paragrafo 3 dell'articolo 13 e dal paragrafo 4 dell'articolo 14 a seconda che i dati siano racconti o meno presso l'interessato.

hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico."[48]

5.1. I diritti classici.

Oltre alla distinzione tra proprietà e controllo dei diritti sui dati dell'interessato, si è delineata un'ulteriore distinzione tra questi, basata non più sul loro contenuto ma da ragioni storiche.

Nel GDPR, vengono ereditati alcuni diritti già presenti nella Direttiva 95/46/CE e riadeguati sia al nuovo contesto tecnologico sia alle nuove garanzie e finalità ricercati dalla nuova disciplina. Questi vengono denominati, i "diritti classici" dell'interessato, cui si contrappongono quelli di nuova matrice, e cioè nati con il regolamento stesso, che vengono denominati i "diritti dinamici."

Rientrano nei diritti classici: Il diritto d'accesso, di rettifica, e di cancellazione dei dati.

Sub – Il diritto d'accesso.

Il diritto di accesso, rappresenta un'estensione di quel dovere del titolare di predisporre un'adeguata informativa. Secondo l'articolo 15 del GDPR: "L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:" finalità del trattamento, natura e origine dei dati, destinatari a cui i dati saranno trasferiti, periodo di conservazione dei dati, informativa sui diritti spettanti all'interessato, il diritto di proporre reclamo a un'autorità di controllo e l'esistenza di un processo decisionale automatizzato.

Il titolare, secondo quanto stabilito dal terzo comma, deve fornire copia di queste informazioni all'interessato ma per evitare di appesantire la tutela di questo diritto e nell'ottica dello sviluppo di una società digitale, la norma si preoccupa di sottolineare che: "Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune."[49]

Sub – Il diritto alla rettifica

48 Si osservi il paragrafo 2, lettera *f*) dell'articolo 14, GDPR.
49 Per completezza rimando alla lettura integrale dell'articolo 15 GDPR

La consapevolezza che esistono di trattamenti sui nostri dati da parte di un titolare apre poi all'interessato un'ampia gamma di diritti che per un'*iter* logico appaiono attivabili solo successivamente.

Primo tra tutti è il diritto alla rettifica definito dall'articolo 16[50] GDPR che permette di richiedere, ed ottenere, l'integrazione di dati incompleti e/o la correzione di quelli inesatti. A prima vista sembrerebbe ricoprire un'importanza marginale, quasi una pignoleria della norma ma vedremo, nell'analizzare a fondo gli algoritmi di *machine learning* e *big data*, quanto sia fondamentale per lo sviluppo tecnologico e per la sicurezza del sistema, la correttezza e la qualità dei dati negli stessi contenuti.

Visto nell'ottica di una funzionalità del sistema stesso, tale diritto viene ritenuto quasi complementare al dovere generale posto in capo al titolare di valutare i rischi del trattamento e in questi rischi rientra sicuramente anche l'impiego dei cosidetti *Bad Data*.

Sub – Il diritto alla cancellazione (diritto all'oblio)

Uno dei diritti più importanti presenti nella Direttiva ed ereditati nel Regolamento è sicuramente il diritto alla cancellazione dei dati che nella sua veste tradizionale rappresenta per l'interessato il diritto all'oblio. Questa sua impostazione tradizionali riene ricalcata in modo poco innovativo nel paragrafo 1 dell'articolo 17 che precisa: "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali." Tuttavia tale diritto non è assoluto in quanto deve sussistere uno dei motivi[51] specificati nella norma al fine di ottenere la cancellazione ed inoltre in certi casi tale diritto è addirittura escluso[52].

---

50 Il testo dell'articolo 16 così recita: "L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa."

51 Il secondo capoverso del paragrafo 1, articolo 17 così precisa: "se sussiste uno dei motivi seguenti:
-i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
-l'interessato revoca il consenso su cui si basa il trattamento,[...] e se non sussiste altro fondamento giuridico per il trattamento;
-l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
-i dati personali sono stati trattati illecitamente;
-i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
-i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. "

52 Il terzo paragrafo dell'articolo 17 fissa che: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
-per l'esercizio del diritto alla libertà di espressione e di informazione;
-per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
-per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
-a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

Fin qui va riconosciuto che non c'è granchè di nuovo rispetto alla precedente disciplina; ciò che segna una grande innovazione è il paragrafo 2, il quale sancisce: “Il titolare del trattamento, se ha reso pubblici i dati ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.”

Questa norma appare emblematica di quel bilanciamento che è il fulcro del Regolamento: da un lato c'è la tutela delle libertà dell'interessato e per rendere effettivo il suo diritto alla cancellazione, si prescrive che la richiesta venga trasmessa a cura del primo titolare, a tutta la catena di sub-titolari che lo stesso ha generato rendendo pubblici i dati. D'altro canto, per evitare di paralizzare l'attività del titolare, nell'ottica dello sviluppo della società digitale, la norma viene interpretata[53] nel senso che la comunicazione della richiesta non deve essere inoltrata ad ogni sub-titolare esistente ma solo a quelli di cui abbia effettiva conoscenza, nei limiti della “tcnologia disponibile” e dei “costi di attuazione”, ed inoltre il titolare non è appesantito dall'obbligo di verificare che i dati siano stati effettivamente cancellati a seguito dell'inoltro.

5.2. I diritti dinamici nel contesto decisionale automatizzato.

Analizzando la famiglia dei diritti “dinamici” anticipati all'inizio del paragrafo, si nota che vi rientrano tre diritti, già presenti nella Direttiva ma totalmente rivisti e rafforzati nell'attuale contesto normativo fino a stravolgerli dalla loro veste originaria per consentire un adeguamento ai progressi tecnologici. Questi sono il diritto di opposizione, alla limitazione dei dati e di conoscere la logica dei processi decisionali automatizati.

Sub – Il diritto di opposizione

L’art. 21 del Regolamento n. 679 disciplina il diritto di opposizione al trattamento dei dati personali, configurabndone però due vesti diversi a seconda della base giuridica su cui si fonda il trattamento stesso. Secondo il primo paragrafo della disposizione, l’interessato del trattamento, ovvero il soggetto cui i dati si riferiscono, ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare,

-per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. “

53 Una visione proposta dall'ex Autorità garante per la privacy Italiana, F. Pizzetti nel manuale: D'Acquisto, G., Naldi, M., Bifulco, R., Pollicino, O., & Marco, B. (2018). Intelligenza artificiale, protezione dei dati personali e regolazione (Vol. 6). G Giappichelli Editore.

al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e)[54] o f)[55], compresa la profilazione sulla base di tali disposizioni.

In queste ipotesi viene garantito all'interessato, esercente tale diritto, che il titolare si astenga dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Risulta tuttavia chiaro, nella lettera d) del primo comma dell'articolo 18[56], che la sospensione del trattamento debba avvenire anche nell'arco di tempo necessario al titolare per fornire la prova di quell'interesse prevalente all'interessato e solo successivamente alla stessa il trattamento puà proseguire normalmente. Se, al contrario, tale prova non viene fornita, la sospensione temporanea si trasforma in interruzione definitiva.[57]

Inoltre nei paragrafi 2 e 3, il legislatore europeo disciplina una ulteriore tipologia di diritto di opposizione, quella riferita a trattamento di dati svolto nell'ambito di operazioni di marketing diretto. In tale veste si prevede che, "qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa al marketing diretto."

In questa accezione i diritti dell'interessato sembrano assoluti in quanto non è ammessa una ragione che il titolare possa addurre a contrastare l'opposizione, se questa interviene il trattamento deve essere immediatamente e definitivamente cessato.

Qualunque sia la veste che assume, si prevede che il titolare debba dare informativa specifica all'interessato del suo diritto e, nell'ottica del prosresso di un'Unione digitale, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati.

L'informativa risulta perfettamente coerente alla natura del diritto quale massima espressione del potere di controllo spettante all'interessato sui suoi dati in quanto, non può esternarnarsi nei casi in cui il trattamento si basa sul consenso, perchè allora sarebbe sufficiente, per interromperlo, la revoca dello stesso.

---

54 Tratta il caso in cui: "il trattamento è 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."

55 Il paragrafo dichiare lecito: "il trattamento necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

56 Il quale prevede i casi in cui il trattamento deve essere limitato da parte del titolare. L'ipotesi che nella specie rileva prevede che: "d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. "

57 Tale *iter* che porta da una sospensione temporanea ad un bivio dove il trattamento, o può riprendere in modo lecito o va interrotto in modo definitivo si applica anche in riferimento al trattamento dei dati ai fini di ricerca scientifica e statistica. Il quinto paragrafo dell'articolo 21 infatti recita: "Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico. "

Sub – Il diritto a richiedere la limitazione del trattamento.

Il diritto dell'interessato a richiedere che il tratamento dei suoi dati venga limitato[58] è definito dall'articolo 18. Il primo paragrafo segnala i casi in cui tale diritto è esercitabile, configurando quattro fattispecie: "a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato."

L'ipotesi più "particolare" e innovativa, considerata dalla norma è proprio la lettera *a* che sembra ricalcare e completare il diritto alla rettifica dei dati personali.[59] Questo fornisce l'occasione di sottolineare, ancora una volta, quanto nel contesto di una società digitale sia fondamentale la qualità e sopratutto l'esattezza dei dati che vengono immessi nel sistema. Il legislatore Europeo a tal proposito ha optato per conferire all'interessato un diritto abbastanza "forte" in quanto, sin dal momento della richiesta, il trattamento deve essere sospeso a prescindere dalla sua fondatezza. Spetterà poi al titolare verificarla nel merito e decidere, eseguiti i necessari accertamenti, se ottemperare alla richiesta dell'interessato o, al contrario, di revocare la sospensione alla limitazione ritenendo i dati corretti. In ogni caso l'interessato deve essere informato della scelta intrapresa dal titolare in quanto potrebbe ricorrerla dinnanzi all'Autorità. Va anche rilevato che l'istanza dell'interessato ha un'incidenza rilevante anche sull'efficienza dei trattamenti posti in essere dal titolare in quanto un *bias*[60] dei dati compromette la funzionalità del sistema.

La fattispecie contenuta nella lettera *b*, concerne un trattamento eseguito illecitamente e cioè in assenza delle condizioni definite nell'articolo 6[61]. In queste circostanze, l'istante ha a disposizione due scelte libere e alternative, o si oppone al trattamento e richiede che venga cessato, in quanto avvenuto *contra ius* oppure ne può domandare la limitazione.

Il caso successivo, concerne quello contenuto nella lettera *c* dove l'interessato ha facoltà di interrompere l'ultima fase del trattamento: la cancellazione dei dati. Qui il titolare ha perso interesse alla continuazione del trattamento e sarebbe tenuto alla cancellazione delle informazioni riguardati l'interessato ma questo ha l'interesse contrapposto a conservare gli stessi per l'esercizio di un diritto in sede giudiziaria.

Infine, la lettera *d* è stata già analizzata nel paragrafo precedente, parlando del diritto di opposizione

58 In tal caso va precisato fin da subito che la limitazione può essere compressa fino a quanto strattamente necessario ai fini della conservazione.
59 Si veda sopra, il paragrafo 5.1.
60 Definita, nel contesto specifico, dall'encicolpedia Treccani come: "tendenza a deviare dal valore medio."
61 *Infra,* paragrafo 6.

ex articolo 21 paragrafo 1, GDPR. Sinteticamente, qualora l'interessato si opponga al trattamento dei suoi dati, basato su un legittimo interesse del titolare, questo deve subito sospendere il trattamento e non può farlo ripartire fintantochè non sia in grado di dimostrare che il suo interesse è prevalente rispetto a quello dell'interessato.[62]

Sub – Diritto a non essere sottoposto a processi decisionali automatizzati

L'ultimo diritto appartenente alla famiglia dei diritti "dinamici" consente all'interessato di porsi al riparo da trattamenti che vengano effettuati esclusivamente sulla base di procedimenti decisionali automatizzati, compresa la profilazione. Prima di analizzarne il contenuto è opportuno precisare il significato di queste tecniche di trattamento.

Per processo decisionale automatizzato si intende quell'attitudine del sistema a prendere decisioni solo attraverso mezzi tecnologici, ossia senza il coinvolgimento umano. La profilazione poi è dettagliatamente definita all'articolo 4[63], come quella tecnica attraverso cui si raccolgono informazioni di un individuo o gruppo di individui per poi valutarne le attitudini o i modelli di comportamento così da tracciare un profilo individuale per dar luogo ad ulteriori valutazioni o previsioni riguardanti il soggetto[64].

La decisione automatizzata e la profilazione non sono quindi tecniche necessariamente sovrapposte: può succedere infatti che una decisione automatizzata venga presa senza aver creato un profilo dell'individuo e, al contrario, una decisione automatizzata si trasforma in profilazione a seconda del modo in cui i dati vengono utilizzati[65].

A questo punto si può comprendere appieno la portata del primo paragrafo dell'articolo 22 GDPR che fissa: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona."

Il regolamento a tal proposito si preoccupa di offrire la garanzia di un intervento umano a quei trattamenti che incidono in modo rilevante sulla persona così da tutelare gli interessi dell'individuo che

62 Come osservato nel paragrafo 5.1.

63 Il Regolamento definisce la profilazione all'art. 4, paragrafo 4 come: "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad 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".

64 I Garanti europei specificano che la fattispecie della profilazione è integrata allorquando concorrano le seguenti tre caratteristiche:
-il trattamento sia svolto in forma automatizzata ,
-esso abbia ad oggetto dati personali,
-il suo obiettivo sia quello di valutare aspetti personali di una persona fisica.

65 Le linee guida, a questo proposito, riportano un esempio per chiarire i due concetti: una multa per eccesso di velocità rilevata sulla base delle prove provenienti da telecamere è una decisione automatizzata che non coinvolge profili. Si tratterebbe invece di profilazione se l'importo della multa fosse il risultato di una valutazione che coinvolge altri fattori quali le abitudini di guida, altre violazioni al codice della strada.

potrebbero risultare fortemente lesi da un processo totalmente automatizzato. A tal proposito degli esempi sono forniti del Considerando 71 GDPR "quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani."

Tale divieto tuttavia non è assoluto, in quanto proprio il paragrafo 2 prevede tre eccezioni. Un trattamento può avvenire con processi decisionali completamente automatizzati se :" a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento[66]; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato."

Si perimetra così un contesto dove tali tecniche sono notevolmente ristrette in assenza di un consenso esplicito dell'interessato: solo nel secondo caso vi si può prescindere[67]. Infatti, nel caso della lettera *a*, relativo alla conclusione o esecuzione di un contratto, la norma fissa il consenso dell'interessato alla manifestazione di volonta a concludere il contratto stesso affidando comunque anche in questo caso un pieno controllo sui dati che lo riguardano.

Quando il controllo dell'interessato è pieno in quanto il trattamento decisionale automatizzato si basa sul consenso[68], il terzo paragrafo assicura che: " […] il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione."

La norma quindi tende a specificare che il consenso non legittima il titolare ad essere incurante verso le situazioni particolari dell'interessato, anzi in questi casi la sua posizione va tenuta maggiormente in conto, fino a consentirgli che intervenga un umano a rivalutare le decisioni assunte dalle macchine.

Il terzo comma non specifica il caso della lettera *b)* in quanto sono proprio le norme attuatrici, nazionali o Europee, che oltre a contentire procedimenti decisionali automatizzati in assenza di consenso, devono predisporre le tutele e le garanzie necessarie da accordare all'interessato.

Sub – Diritto ad essere informato a seguito di una richiesta.

In conclusione, l'articolo 19 GDPR, prevede una garanzia accessoria che conferisce effettività e forza al potere di controllo dell'interessato che abbia esercitato uno suo diritto. In realtà più che un diritto

66 In riferimento al primo punto, i Garanti europei chiariscono che la necessità di utilizzare decisioni automatizzate per l'esecuzione o conclusione di un contratto deve essere interpretata in modo restrittivo ciò significa che il titolare deve essere in grado di dimostrare che la profilazione è necessaria e non sono disponibili mezzi alternativi meno invasivi.

67 Appare suprefluo specificare che in tal caso la garanzia che i diritti dell'interessato vengano adeguatamente tutelati è affidato ai legislatore sia Europeo che nazionale poiché il trattamentò con processi decisionali automatizzati, compresa la profilazione, è consentita, senza il consenso dell'interessato, solo in virtù di una norma autorizzativa. In materia sono state anche rilasciate le Linee Guidan del Comitato europeo della protezione dei dati n. 251 del 2017 che dettano le tutele minime che vanno sempre accordate all'interessato nel formulare norme autorizzative di tali trattamenti, così da consentire sempre un controllo all'interessato.

68 Il terzo paragrafo specifica: "Nei casi di cui al paragrafo 2, lettere a) e c)"

dell'interessato tale articolo si configura come un obbligo posto in caso al titolare di un trattamento che abbia ricevuto una richiesta di rettifica, cancellazione o limitazione del trattamento. La norma così esplicita: "Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda."

Si apre così una garanzia "forte", in perfetta armonia con l'obiettivo del regolamento di sviluppare una società digitale all'interno dell'Unione. Da un lato il titolare è tenuto, non solo, a valutare la richiesta rispetto alla sua attività di trattamento ma deve anche dare comunicazione dell'eventuale avvenuta cancellazione, rettifica o limitazione anche a tutti i suoi destinatari[69] che abbiano ricevuto dallo stesso quei dati. Per effetto sostanziale, il titolare si pone come *soggetto interposto* tra l'interessato e l'esercizio dei suoi diritti e i destinatari ai quali egli ha comunicato i dati relativi all'altro. Infine, a garanzia che tutto il sistema non venga intasato, si prevede che l'obbligo non sussiste qualora la comunicazione si "riveli impossibile" oppure che "implichi uno sforzo sproporzionato" al titolare. In ogni caso l'interessato può richiedere quali siano stati i destinatari del titolare per effettuare egli stesso eventuali e ulteriori richieste.

6. Il titolare e i principi generali sul trattamento dei dati.

Come si è osservato, il titolare risulta il perno della disciplina delineata dal GDPR in quanto, essendo il soggetto che pone in essere il trattamento, gli si domanda sia il rispetto dei diritti e delle libertà dell'interessato che l'osservanza delle norme sul trattamento. Prima di iniziare tale attività, infatti, deve porsi due interrogativi, il primo riguarda le condizioni che devono sussistene affinche un trattamento possa iniziare in modo lecito e la seconda attiene alla coerenza delle modalità concrete e specifiche attraverso cui lo stesso verrà effettuato, come specifica il Considerando n. 76[70].

Entrambe tali valutazioni non sono eventuali ma diventano un' attività necessaria poiche dalla loro inosservanza può derivare, a seconda dei casi e della gravità dell'illecito, la responsabilità civile, amministrativa o penale del titolare nonché ovviamente l'interruzione dell'attività di trattamento.

Viene così sancito a chiare lettere un principio di "accountability[71]". Gli articoli 5, par. 2 e 24 del

69 L'articolo 4 definisce il «destinatario» come: "la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. [...]"

70 Letteralmente: "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato."

71 Il termine *accountability*, è utilizzato nella versione in lingua inglese dell'articolo 5 GDPR. In italiano è stato tradotto come responsabilizzazione ma tale termine risulta insufficiente nel definire il duplice dovere che deriva dall'accountability e cioè che il titolare del trattamento è competente per il rispetto dei principi ed è, in ogni momento, in grado di comprovarlo. Il termine è

regolamento costituiscono i capisaldi di un nuovo sistema che impone al titolare del trattamento di sviluppare, non solo, un insieme di procedure che assicurino efficacemente il rispetto delle regole ma dovrà altresì munirsi di tecniche che gli permettano, all'occorrenza, di dimostrare l'osservanza della normativa dinanzi all'autorità garante.

L'onere probatorio in capo al titolare del trattamento è significativo, in quanto è tenuto a provare sia la conformità delle attività alle disposizioni del GDPR, ma anche l'efficacia delle misure adottate per la tutela dei dati personali detenuti.

Si osserva quindi come il regolamento mira a creare diversi livelli di misure che il titolare deve adottare sotto la sua responsabilità: ad un primo livello preliminare, deve osservare tutte le norme in materia di conservazione dei dati e, se intende effettuare sugli stessi dei trattamenti, deve stabilire se si trova in condizione di poterlo porre in essere in modo lecito e legittimo. Se sussistono tali circostanze e ancora prima che l'attività inizi, il titolare deve valutare necessariamente i rischi[72] che potrebbero correre sui dati a causa di tale attività, stabilendo, in concreto, se sono adeguate le misure tecnico-organizzativo e di sicurezza di cui si è munito. Se poi, da tale valutazione, risultano dei rischi elevati o, se il titolare lo decide per proteggere ulteriormente la posizione degli interessati, si apre un terzo livello di misure che il titolare deve implementare e che vanno dalla valutazione d'impatto *ex* articolo 35, alle misure di anonimizzazione o ancora all'adozione di carte etiche o codici di condotta. L'effettività della tutela è poi data dal fatto che il titolare deve sempre essere in grado di provare, a richiesta dell'interessato o dinnanzi all'autorità garante, di aver onorato tali adempimenti e di giustificare i motivi delle scelte operate o delle misure di cui si è servito.

Iniziando con ordine, vanno analizzate le norme relative alle condizioni generali in materia di conservazione dei dati, dove spiccano due articoli cardine del sistema, il quinto ed il sesto che fissano nel loro insieme 7 principi generali che vanno sempre rispettati..

L'articolo 5 prescrive sei di questi principi:

1. Principio di trasparenza: la trasparenza è una qualità richiesta alle modalità con cui vengono raccolti e utilizzati i dati personali. Il Regolamento richiede, in particolare, che siano facilmente accessibili e che le comunicazioni relative al trattamento siano comprensibili.

2. Principio di limitazione delle finalità dei dati: il Regolamento fissa che la raccolta dei dati degli utenti dovrà avvenire soltanto per finalità determinate, esplicite e legittime, e successivamente, il trattamento dovrà essere effettuato in modo che non sia incompatibile con tali scopi. Il quarto comma dell'articolo 6[73] a

più vicino al concetto di Rendicontazione di cui la "responsabilizzazione" è solo uno degli aspetti. Il punto fondamentale del concetto di accountability è in realtà posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance e di un buon modo di rispondere ai problemi che derivano dal trattamento dei dati.

72 Per un'accurata precisazione del termine "richio" consiglio la lettura del Considerano 75 che fornisce altresì numerosi esempi.

73 Letteralmente: "Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

tal proposito elenca una serie di parametri molto ampi che, se applicati, permettono di verificare la non incompatibilità di un trattamento alle finalità specificate. Tuttavia si tratta di un giudizio che spetta, in prima battuta, esclusivamente al titolare e di fatto potrebbero essere ampliate le possibilità di trattamenti che esulino dagli obiettivi fissati per la raccolta di quei dati. Ovviamente tale valutazione di legittimità compiuta dal titolare è totalmente sotto la sua rtesponsabilità.

3. Principio di minimizzazione dell'uso dei dati: non sarà più possibile rivolgere all'utente una richiesta eccessiva dei suoi dati: la richiesta dei dati deve essere "adeguata, pertinente e limitata a quanto necessario per il perseguimento delle finalità per cui i dati sono raccolti e trattati."

4. Principio di esattezza dei dati: i dati raccolti dovranno essere esatti e, se necessario, aggiornati. Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

5. Principio della limitazione della conservazione: i dati potranno essere conservati esclusivamente per il tempo necessario al raggiungimento delle finalità per le quali sono trattati.

6. Principio dell'integrità e della riservatezza: i dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

Il settimo principio viene poi enunciato nell'articolo 6, dove vengono fissate le basi giuridiche su cui un trattamento può fondarsi per essere definito lecito. In particolare, è lecito solo soltanto quando:

-l'interessato ha prestato un consenso informato;

-il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;

-il trattamento è necessario per adempiere un obbligo legale a cui è soggetto il titolare;

-lo stesso è necessario per la salvaguardia degli interessi vitali della persona fisica;

-è necessario per eseguire di interesse pubblico o per il perseguire un legittimo interesse del titolare.

Una volta che il titolare si sia adeguato a tali principi, dovrà valutare i rischi specifici che la sua attività di trattamento può comportare sui dati degli interessati, valutati, in concreto, le misure informatiche che intende adottare e l'adeguatezza delle misure sicurezza di cui vuole avvalersi.

6.1. Le responsabilità del tritolare.

Rispetto alle precise modalità di trattamento, l'articolo 24 del GDPR apre la disciplina specificando le

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'ar ticolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione."

incombenze che gravano sul titolare. La norma stabilisce che il titolare deve sempre, sia prima di effettuare un trattamento che durante lo svolgimento dello stesso, adottare quelle che sono le "misure tecniche e organizzative adeguate" per assicurare che le norme del regolamento siano rispettate.

Sul titolare quindi si concentra tutta la responsabilità relativa al fatto che il "trattamento sia effettuato conformemente al regolamento" e tale concentrazione non avviene solo al momento del primo trattamento ma permane per tutta la durata dell'attività così da far gravare sul titolare anche il dovere di riesaminare e aggiornare tali misure "qualora necessario."

Per poter ricercare quelle che sono le misure "adeguate", il titolare è tenuto a compiere una "valutazione dei rischi" che il trattamento può presentare per gli interessi delle persone fisiche. Tale valutazione deve essere compiuta sulla base dello specifico trattamento che il titolare vuole porre in essere, così da renderla il più possibile aderente e garantista nei confronti degli interessati, "tenendo (anche) conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento."

La responsabilità del titolare quindi va a parametrarsi sul rispetto dei diritti e libertà dell'interessato che diventano l'oggetto di una tutela finalizzata a ridurre i rischi al minimo possibile in ogni momento del trattamento. Non si tratta di accordare una tutela statica e formale ma di impostare una garanzia dinamica che sia in grado di muoversi con l'evoluzione della tecnologia e delle tecniche di comunicazione adottate dal titolare o dalla società dell'informazione.

Queste tuttavia sono solo le accortezze minime che il titolare deve rispettare poiché il secondo comma dell'articolo 24 specifica che, se risulta "proporzionale rispetto alle attivitò di trattamento" e quindi qualora vi siano dei rischi concreti, vanno anche attuate delle "politiche adeguate in materia di protezione dei dati."

Per politiche adeguate s'intende sia l'osservanza delle norme successive, quali ad esempio la pseudonimizzazione, minimizzazione o valutazione d'impatto, sia tutte le ulteriori misure che il titolare ritiene necessarie per rafforzare la tutela degli *users*[74] nello specifico contesto in cui opera, come ad esempio le carte etiche, i codici di condotta o i meccanismi di certificazioni[75].

6.2. Protezione *dal* software o protezione *nel* software?

Gli utenti che si ritrovano, per qualunque fine, a cedere i proprio dati personali si pongono sempre il

74 Lessema proveniente dal vocabolario inglese e tradotto come utente, solitamente utilizzato in ambiente informatico.

75 A parere di autorevole dottrina, F. Pizzetti, questa risulta l'interpretazione più appropriata del secondo comma anche alla luce di quanto dispone il terzo paragrafo dell'articolo 24: "L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento."

quesito su come poi quei dati saranno utilizzati dal titolare. Fintanto che il trattamento era completamente, o quasi, umano, l'user era confortato dalla circostanza che l'imperfezione umana non gli avrebbe mai consentito un controllo preciso di tutti i dati raccolti e si cedevano dati con estrema leggerezza ed inconsapevolezza.

L'avvento dei sistemi di *Big Data*, tuttavia, consentono una trattazione dettagliatissima di ogni dato, arrivando addirittura ad accrescere la propria efficienza al crescere del numero dei dati (ovviamente sempre che la qualità sia tale da non provocare disfunzioni del sistema) fino a creare articolati profili personali. Ciò ha generato delle insicurezze nei privati, i quali, non potendo conoscere le logiche di tali sistemi, si sentivano sprovvisti di tutela quando era il *software* a gestire i loro dati.

Il GDPR, nell'ottica di favorire lo sviluppo di una società digitale all'interno dell'Unione, ha tentato di ridare fiducia agli utenti predisponendo tutta una serie di tutele che possono essere inserite ed integrate direttamente nelle macchine che poi compieranno attività di trattamento.

Per arginare l'attività dei titolari e renderla più "*privacy focused"* interviene proprio l'articolo 25 che apre la via a due modalità preventive di tutela dei dati personali a seconda della gravità dei rischi che si corrono: la tutela fin dalla progettavione, la c.d. *Privacy by design* e quella per impostazione predefinita, c.d. *Privacy by default.*

Queste due tecniche, suppur sovrapponibili sotto alcuni profili, sono tenute ben distinte nei due commi dell'articolo 25. Il primo comma[76], definendo la *privacy by default* afferma che questa tecnica si estende dall'inizio alla fine di un trattamento ed ha una flessibilità tale da adattarsi ai mutamenti dei rischi che l'attività comporta. Ciò è reso possible inserendo il parametro della privacy all'interno della macchina, quale requisito da soddisfare, così da rendere ogni singolo trattamento conforme alle dispizioni.

La *privacy by default*[77]*,* differentemente, è una metodologia che viene applicata solo al momento della progettazione di un trattamento ed impone al titolare di architettare tutta la sua attività assicurandosi che "siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento." Dopo la "prima impostazione" il sistema tratterà automaticamente i dati secondo quelle disposizioni, ciò non significa che poi il sistema rimarrà immutabile rispetto alla "prima" impostazione predefinita ma può variare solo a seguito di una nuova impostazione fornita dal titolare.

76 L'articolo 25.1 GDPR prevede testalmente che: "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 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."

77 La disposizione contenuta nel secondo comma dell'articolo 25 afferma: "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica."

Il fine perseguito dal legislatore Europeo è proprio quello di creare un contesto di fiducia per gli *users* nei confronti dei *software* utilizzati per effettuare i trattamenti, configurandoli quale strumento progettato a loro tutela e non più come strumento di abuso da parte del titolare. Se prima l'automatismo delle macchine poteva generare paura nell'esattezza con cui effettua i trattamenti ora dovrebbe portare fiducia agli interessati poiché la stessa rigidità nell'operare, sarà impiegata per tutelare i loro diritti.

6.3. *Privacy by default.*

Il nucleo della tutela della *privacy by default* sta nell'imporre al titolare, in modo predefinito e preventivo, l'adozione delle misure tecniche necessarie a garantire che, per ogni finalità perseguita, siano utilizzati solo i dati personali utili a quello scopo.

La disposizione, precisa che "tale obbligo, vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità." Tale frase sembra richiamare il generico rispetto dei principi fondamentali del trattamento quali ad esempio il periodo di conservazione o il rispetto dei diritti degli interessati, quali il diritto di accesso ma la norma richiede che la loro osservanza sia garantita per impostazione predefinita sin dalla fase di progettazione. Ciò comporta l'obbligo per il titolare di valutare preventivamente, il rispetto dei diritti e garanzie degli interessati anche, e sopratutto, in riferimento alle misure tecniche e metodologie tecnologiche che intende utilizzare, così da garantire un'effettiva tutela.

Una siffatta interpretazione è corroborata dal considerando n. 78 che nella prima parte afferma_ "La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default."

Trattandosi di una tutela predefinita che viene accordata automaticamente ad ogni trattamento, questa va predisposta ancora prima che l'attività inizi e quindi naturalmente retroagisce alla fase di progettazione e strutturazione dei software preposti a trattare i dati. Se quindi formalmente l'obbligo si pone in capo al solo titolare del trattamento, tale disposizione va a parametrare tutta l'attività dei produttori di beni e servizi e dei programmatori che, se intendono immettere sul mercato degli algoritmi finalizzati a compiere attività di trattamento, devono architettarli per compiere tale attività conformemente al regolamento: nessun titolare altrimenti si servirebbe di quei macchinari.

Da un lato, solo il titolare, deve servirsi di tale tecnichè di protezione dei dati ma indirettamente si colpisce tutto il sistema di progettazione a monte, in quanto, proprio per le caratteristiche intrinseche della privacy by defalut, solo a quel livello si può garantire che la tutela venga successivamente accordata in ogni

fase successiva del trattamento. Se è vero quanto ha affermato il professor Cingolani[78] che la "tecnologia è neutra", il legislatore Europeo ha voluto mutare tale neutralità a favore dell'interessato, considerato parte debole dell'attività di trattamento.

Due ultime precisazioni completano la tutela da come dettato dell'articolo 25: da un lato si specifica che: "In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica." e dall'altro si prevede che: "Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo."

La prima richiede che il trattamento sia suddivisa in vari livelli di attività, dove solo allo *staff* autorizzato della fase più "profonda" è consentito accedere integralmente ai dati personali. Fuori da questa fase, i dati devono essere resi anonimi per tutta la restante catena del trattamento così da non consentire l'identificazione degli interessati cui si riferiscono ad un numero "indefinito" di persone fisiche.

Da ultimo si fa riferimento alle tecniche di certificazione che potrebbero essere adottate dal titolare per dimostrare la conformità della sua attività alle norme del regolamento. Tale disposizione ha una forte incidenza in relazione al principio dell'*accountability*, secondo cui, il titolare non deve solo rispettare il codice ma deve essere anche in grado di dimostrarlo all'interessato e all'autorità garante; un siffatto meccanismo di certificazione lo esonererebbe da tale gravoso onere probatorio.

8.4. *Privacy by design.*

La *privacy by design* (tradotta nella versione italiana del GDPR, privacy fin dalla progettazione) viene definita dal primo comma dell'articolo 25, che statuisce: "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 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."

Come appare evidente dalla dizione inglese, questa modalità impone al titolare di ideare e progettare, fin dal livello più basso, un'attività di trattamento che tenga accurato conto della tutela dei diritti degli interessati. Tale norma sembra lasciare un margine di libertà di progettazione in capo al titolare senza

78 Roberto Cingolani, è un premiato fisico Italiano e direttore scientifico dell'Istituto Italiano di Tecnologia. Ha espresso tale dichiarazione in numerose rassegne stampa.

tuttavia rinunciare alla tutela dei dati, vengono infatti suggerite nella disposizione delle modalità che potrebbero essere seguite nella progettazione ma l'unico modo per essere totalmente *compliant* con il regolamento impone una valutazione concreta tra i rischi derivanti delle attività svolte e le misure preventive poste in essere dal titolare.[79]

In sostanza queste metodologie permettono di ritagliare solo quelle che sono le tutele funzionali alle specificità dei trattamenti, così da assicurare libertà ed efficienza ad un titolare che non si vedrà invece obbligato a tutele estreme per trattamenti che hanno bassissimi rischi per i diritti degli interessati.

Va ovviamente ricordato che, in armonia con il principio dell'*accountability,* di cui si è parlato sopra[80], il titolare dovrà essere in grado di giustificare l'*iter* logico che lo ha portato ad aver adottato determinate misure di sicurezza piuttosto che altre in ragione dei rischi specifici del trattamento. La libertà di progettazione quindi viene controbilanciata da un puntuale obbligo di documentazione e di coerenza dell'attività di trattamento alle norme del GDPR per evitare eventuali sanzioni anche gravi.

L'articolo 25.1 fornisce alcuni esempi[81] di queste "misure tecniche e organizzative adeguate, quali la pseudonimizzazione" o "la minimizzazione". Non si tratta assolutamente di un elenco tassativo in quanto la norma continua specificando che il titolare è tenuto "a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati."

La pianificazione imposta al titolare consente una forma di tutela proattiva, poiché mira a individuare problemi futuri in modo da trovare anticipatamente le azioni idonee a risolverli, e preventiva, in quanto diretto a impedire il verificarsi o il diffondersi di "intoppi" non desiderati.

6.4.1. Pseudonimizzazione e anonimizzazione dei dati.

La prima metodologia richiamata dalla norma è la pseudonimizzazione, che viene dettagliatamente definita nell'articolo 4 comma 1, numero 5, 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

79 Il punto di forza che renge il regolamento uno strumento efficace e flessibile risiede proprio in norme come quella *ex* articolo 25.1 che riesce ad accordare una tutela forte all'interessato e lascia comunque libertà al titolare. Il precetto normativo si slega totalmente dalla misura tecnologica impiegata, che è destinata a mutare e svilupparsi velocemente ma si incardina su quelle che sono le "costanti" di un trattanento e quindi sulla tutela degli interessati e sul rispetto dei principi chiave. Non sono più i diritti a piegarsi allo sviluppo ma è il progresso a diventare servente ai diritti.

80 Si riveda il paragrafo 6. relativo alla posizione del Titolare.

81 Per avere un'idea più chiara di quali potrebbero essere le ulteriori "misure adeguate" rimando alla lettura di documento predisposto e costantemente aggiornato dalla AgID (Agenzia per l'Italia Digitale, che ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese) denominato "linee guida e best practice per progettare il software". Tale strumento risulta una guida perfetta per l'architettura di una siffatta tutela, in quanto mette in evidenza, le esigenze che vanno tutelate ad ogni livello del trattamento e permette di calcolare accuratamente la sicurezza, le minacce e le vulnerabilità del sistema.

identificata o identificabile“

Tale tecnica comporta la separazione tra i dati riguardanti una persona fisica da qualli che ne permettono l'identificazione, utilizzando i mezzi appropriati per impedirne la riunione: in estrema sintesi rendono un soggetto da individuato, attraverso i propri dati, a individuabile ma solo con determinate informazioni ulteriori. Il GDPR parla della pseudonimizzazione come di un'efficace tecnica per ridurre i rischi in due contesti diversi: sia con riferimento sia alla privacy by design e quindi, in generale, in materia di modalità del trattamento sia come misura di sicurezza. La duplicità di impiego di questa misura non ne cambia assolutamente la sostanza ma solo le finalità. Come modalità di trattamento, ha un'applicazione preventiva, fin dal momento della progettazione e consente al titolare di creare un'architettura protetta ancor prima di valutare il rischio concreto che l'attività comporta. Quale misura di sicurezza la pseudonimizzazione viene adoperata solo in un secondo momento e cioè quando il titolare, dopo aver predisposto tutte le “misure tecniche-organizzative” necessarie per il trattamento, ritiene, a seguito di una valutazione che porta alla luce fragilità elevate, necessarie misure aggiuntive per ridurre i rischi.

Quale che sia il momento applicativo di tale tecnica o la sua finalità, il suo pregio rimane quello di ridurre notevolmente i rischi che potrebbero derivare da un'attacco al sistema e di riflesso incrementa la tutela accordata alla *privacy,* intesa in senso stretto, degli interessati. Nonostante le sue proprietà, la pseudonimizzazione, rimane solo una tecnica di secondo livello, applicabile qualora non sia possibile anonimizzare i dati.

L'anonimizzazione è una matodologia che condivide molto con la pseudonimizzazione ma che, qualora applicata al trattamento ed alla conservazione dei dati, comporta dei vantaggi notevolmente maggiori. Una trattazione esaustiva di tale pratica, anche a paragone con la pseudonimizzazione, viene fornita dal Considerando 26: “È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. [...] I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.”

Salta subito all'occhio la disposizione contenuta nell'ultimo periodo dell'articolo e cioè l'inapplicabilità dei principi fissati nel GDPR per i trattamenti che avvengono su basi di dati “resi sufficientemente” anonimi. L'esonero dagli obblighi e dalle responsabilità però richiede la corretta anonimizzazione dei dati.

Un dato anonimo è, in linea teorica, un informazione riguardante un soggetto non identificato ma nemmeno identificabile da parte del titolare. Questa tecnica non esige una fase di separazione tra il dato ed il soggetto cui si riferisce ma il dato viene già raccolto o ricevuto, senza gli elementi identificativi dell'user. La

differenza sostanziale tra informazione pseudonimizzate e quelle anonime sta proprio in questo, la prima consente al titolare, se necessario, di risalire dal dato aggregato al dato del singolo soggetto identificato, con la seconda tecnica tale possibilità è esclusa, il titolare può lavorare, in ogni fase del trattamenbto, solo sul dato aggregato.

È proprio il Considerando 26 che si preoccupa di tracciare questa linea di confine, stabilendo che: "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."

L'opportunità di applicare una tecnica piuttosto che l'altra ad un'attività di trattamento comporta come sempre una valutazione concreta delle metodologie tecnico-organizzative impiegate per eseguirli. Tale opportunità viene però compicata nelle ipotesi in cui il trattamento preveda una "catena di titolari[82]" poiché

il secondo titolare beneficerà delle misure gia utilizzate nella prima parte del trattamento ma ben può accadere che solo alcuni trattamenti, o fasi di un singolo trattamento, abbiano bisogno di misure tecniche più garantiste della privacy, lasciando il resto del sistema più leggero e flessibile. In questi casi si parla in dottrina di *privacy by design a geomertia variabile* poiché per ogni attività di trattamento, o fase di un singolo trattamento, vanno tenute in mente le singole finalità e rischi, per scegliere solo le misure più adatte così da alleggerire l'intero sistema.

6.4.2. Minimizzazione.

L'ulteriore misura esplicitamente richiamata dall'articolo 25.1 è la minimizzazione. Questa tecnica, a differenza della pseudonimizzazione, è utilizzabile solo preventivamente ad un trattamento[83], poiché attiene ai rapportri tra i dati e le finalità del trattamento. Viene così sancita la necessità che i dati personali vengano raccolti esclusivamente nei limiti di quanto necessario per il raggiungimento dello scopo per i quali sono

82 Si parla di catena di titolari qualora, un titolare del trattamento operi nel quadro di una pluralità di trattamenti che ne condividano la finalità ma facenti capo a titolare diversi, oppure se opera nell'ambito di una catena di trattamenti, ciascuno con finalità diverse ma che, se connessi l'uno con l'altro, producono effetti ulteriori rispetto ai singoli "anelli" del trattamento. Il tema verrà trattato appropriatamente nel paragrafo 1.1. del terzo Capitolo.

83 Come richiede il Considerando 78: " […] Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali [...]".

stati raccolti.

Il GDPR dedica a tale tecnica l'articolo 5.1 lettera *c)* che fissa le tre regole fondamentale di rapporto tra raccolta dei dati e finalità dei trattamenti: in particolare i primi devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto" ai secondi.[84]

Ne deriva che, fin dal momento della pianificazione, il titolare dovrà stabilire quali siano i dati essenziali per il trattamento che si vuole effettuare, dovrà determinare se quel trattamento sia effettivamente necessario al raggiungimento dello scopo ed infine dovrà anche verificare che la finalità prefissata, di volta in volta, non sia raggiungibile con altri mezzi. Tale metodologia richiede quindi una forte sistematicità poiché per ogni finalità di un trattamento, o signola fase, andranno ritagliati e raccolti solo dati specifici.

Sotto questa ottica, in dottrina si è parlato anche di una *visione prismatica* della *privacy by design* perchè ogni singola attività di trattamento o ciascuna sua fase, può essere parametrata richiedendo solamente i dati minimi per quella specifica finalità; metaforicamente il prisma presenterà tanti più lati quanto più sara complicato il trattamento o pianificata l'intera attività.

6.5. Valutazione d'impatto ed i rapporti con la valutazione dei rischi.

Come sottolineato più volte, il regolamento permette al titolare di parametrare la tutela dei dati personali in relazione al livello di rischio specifico che presenta concretamente la sua attività. Il primo adempimento che va necessariamente eseguito prima che inizi un trattamento è proprio la valutazione dei rischi. Se all'esito di tale valutazione, si riscontra la presenza di elevate fragilità nel sistema, il titolare è tenuto, sotto la sua responsabilità, ad adottare tutte le misure ulteriori e necessarie per minimizzare il pericolo incombente sui dati trattati.

Per capire meglio cosa si intende per rischio, va osservata la definizione data nel *WP29 Guidelines on Data Protection Impact Assesment (DPIA)* che lo qualifica come uno "scenario descrittivo di un evento e le relative conseguenze, stimati in termini gravità e probabilità per i diritttti e le liberta degli interessati." Una tale definizione generica permette di inquadrare il rischio come un concetto molto elastico che va determinato sopratutto in riferimento ad alcuni elementi di contesto quali, l'origine dei dati, la tecnologia impiegata, la natura del trattamento, gravità e probabilità dei rischi e le conseguenze che si potrebbero riversare sulla posizione degli interessati.[85]

84 Così, ad esempio, se un titolare intenda inviare della posta elettronica a fine di marketing non avrà necessità di raccogliere dati uteriori all'indirizzo di posta elettronica dell'utente che abbia consentito a tale trattamento.

85 A tal proèposito, il primo paragrafo dell'articolo 35 così recita: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."

Qualora si rilevino dei rischi elevati[86], quindi, graverà sul titolare il rispetto di tutta un'ulteriore serie di adempimenti prima che il trattamento inizi[87], fondamentale fra tutte è la valutazione d'impatto (nota anche come DPIA, dall'arcnomo inglese: *Data Protection on Impact Assessment).* La valutazione d'impatto, in questa circostanza, si trasforma da attività ulteriore ed eventuale in obbligatoria e specifica, dovendosi riesaminare tutto l'assetto tecnico organizzativo con particolare riferimento ai rischi già rilevati dalla valutazione *ex* articolo 24.

Proprio per la sua funzione di rivalutare la solidità del sistema sulla base delle debolezze già rilevate, la DPIA si configura come attività sempre successiva alla valutazione dei rischi, impedendo così ad un titolare, di effettuare la prima in sostituzione della seconda: non hanno, infatti, un rapporto di gerarchia ma di sequenza necessaria.

L'articolo 35 procedimentalizza l'attività della valutazione d'impatto, stabilendo i casi in cui è necessaria e le modalità che vanno seguite per svilupparla. A tal proposito, il terzo comma dell'articolo presenta un elenco tassativo, seppur non esaustivo, di casi in cui il trattamento presenta di per sé dei rischi elevati per diritti e libertà degli interessati.

In particolare la disposizione precisa che: "La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche[88];

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10[89]; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico."[90]

---

86 Va sottolineato che il GDPR, sollecita l'esecuzione di una valutazione d'impatto anche per quei trattamenti che non presentano rischi elevati., ovviamente in tali casi non è un obbligo per il titolare.

87 In realtà, il titolare è tenuto ad attuare tale tutela anche durante un trattamento già in corso quindi se dovessero riscontrarsi dei rischi elevati, per circostanze sopraggiunte, è obbligato a rispettare tali adempimenti ulteriori da quel momento. Del resto è proprio il paragrafo 11 dell'articolo 35 che precisa: "se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento."

88 Del resto, tale trattamento viene considerato di per se rischioso per le libertà delle persone fisiche e lo si rileva anche nel diritto conferito agli interessato nell'articolo 22, in relazione ai processi decisionali automatizzati, il quale statuisce che: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automa tizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significa tivamente sulla sua persona."

89 I dati *ex* articolo 9.1 e cioè, "i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" ed i dati di cui all'articolo 10, relativo "alle condanne penali e ai reati o a connesse misure di sicurezza" hanno una forte carica discriminatoria in quanto se divulgate potrebbero esporre i soggetti a gravi compressioni delle loro libertà e per tale motivo presentano un rischio elevato. Tuttavia, tali trattamenti devono avvenire su larga scala.

90 Le *WP29 Guidelines on DPIA* chiarisce che tali ipotesi possono anche coesistere per uno stesso strattamento andando ad elevare proporzionalmente i livelli di rischio.

I punti di cui alla lettera *b* e *c* introducono il concetto di "larga scala" che tuttavia non trova alcuna definizione all'interno del GDPR se non nel Considerando 91 il quale, nella sua prima parte, qualifica che "ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato." Per poter valutare se un trattamento avvenga o meno su larga scala, aiuta il *WP29 Guidelines on DPIA* che, a tal fine, fornisce gli elementi da considerare: non ci si deve concentrare solo sul numero complessivo di soggetti coinvolti dall'attività ma va osservato in relazione ad altri elementi quali la percentuale con la popolazione nel suo complesso, il volume dei dati, le finalità perseguite, l'estensione geografica dell'attività e la durata dei trattamenti.

Rispetto al contenuto che tale valutazione deve presentare, si prescrive, al settimo comma dell'articolo 35, che vanno affrontate quattro questioni fondamentali: "Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione."[91]

Risulta così evidente che una DPIA si configura come una valutazione della valutazione per far emergere con più evidenza le misure ulteriori e necessarie da integrare al sistema di trattamento. La vera differenza però sta nel ruolo che assumono ulteriori soggetti, come l'autorità di controllo, nella procedura che porta ad una valutazione d'impatto.

6.5.1. *Segue*: La valutazione d'impatto ed i rapporti con l' Autorità Garante.

Ovviamente la valutazione d'impatto è un'obbligo che si pone in capo al solo titolare ma in talune ipotesi, risulta necessario l'intervento di altri soggetti al fine di portarla al termine.

Il soggetto più coinvolto in questa operazione è proprio l'Autorità Garante che ha in materi notevoli poteri di controllo e vigilanza sia generali che specifici a singoli trattamenti.

I poteri generali di regolazione affidati all'autorità di controllo sono delineati dai paragrafi da 4 a 7 dell'articolo 35 e si incardinano in quello che viene definito "meccanisco di coerenza." Partendo dal presupposto che l'elenco dei trattamenti che necessitano una DPIA, offerto dall'articolo 35.3, non è

91 Un'Autorità Francese, la CNIL, ha sviluppato un software per le pubbliche amministrazioni, e messo a disposizione di ogni titolare interessato, in grado di effettuare una valutazione d'impatto in base a dei parametri fissati negli algoritmi interni. Il software è stato tradotto in italiano grazie all'Autorità Garante ma si precisa che vale solo come strumento di supporto dovendosi, il focus della valutazione, parametrare sulle modalità concrete del trattamento.

assolutamente esaustivo, si riconosce all'Autorità di controllo nazionale il compito di predisporre autonomamente delle liste aggiuntive dove vengono indicate sia tipologie di trattamenti che devono necessariamente eseguire una valutazione d'impatto sia quelle che invece ne sono esonerate.

Il quarto paragrafo in particolare, prevede che "L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati" e successivamente il quinto paragrafo le gli conferisce il potetre di "redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati." Entrambe le disposizioni sono poi corredato da un'onere informativo posto in capo all'Autorità Garante nazionale che redige un elenco di trattamenti che necessitano o meno una valutazione d'impatto, e cioè quello di darne comunicazione al Comitato Europeo per la Protezione dei Dati (cd. "CEPD") di cui all'articolo 68 GDPR.

Il rapporto tra valutazione d'impatto ed Autorità di Controllo Nazionali ed Eurpoee è poi complicato dal sesto paragrafo che mira ad inalzare la tutela per alcune categorie di trattamenti, restringendo la libertà delle Autorità nazionali nella redazione degli elenchi *ex* artt. 35,4 e 35,5. In particolare, "se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione" si prevede che prima che gli stessi vengano adottati, l'Autorità di controllo deve attivare il meccanisco definito all'articolo 63, e cioè, il meccanismo di coerenza.

Tale meccanismo viene definito dall'articolo 64, ed è finalizzato ad integrare in modo attivo il Comitato Europeo per la Protezione Dati, al quale deve essere obbligatoriamente richiesto un parere qualora l'Autorità Nazionale intanda adottare elenchi per apposite sub-categorie di trattamenti[92]

Il parere deve essere richiesto da parte dell'Autorità Nazionali, dietro la redazione di un progetto di tali elenchi. Il Comitato avrà poi a disposizione un termine piuttosto rigido (essendo un parere che va richiesto obbligatoriamente non si sono volute paralizzare le attività dei titolare in caso di inoperatività del Comitato) per rispondere alla proposta presentata e precisamente "di otto settimane. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione." Il Comitato, inoltre, vota a

92 In realtà tale "meccanismo" va applicato anche i contesti, in particolare, dalla dizione della norma: "Il comitato emette un parere ove un'autorità di controllo competente intenda adottare una delle misure in appresso. A tal fine, l'autorità di controllo competente comunica il progetto di decisione al comitato, quando la decisione:
a) è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
b) riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;
c) è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;
d) è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 46, paragrafo 2, lettera d), e all'articolo 28, paragrafo 8;
e) è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);
f) oppure è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.

maggioranza semplice e si può prescindere dal suo parere nel caso si sia già espresso sulla medesima questione.

Tale strumento normativo ha un pregio innegabile e cioè, permette di adeguare costantemente il contesto normativo a tutte quelle che sono le imprevedibili evoluzioni del mondo tecnologico, evitando in ogni momento e in riferimento ad ogni tecnica operativa dei buchi normativi che potrebbero lasciare scoperti di tutela i dati degli interessati.

I rapporti tra titolare ed Autorità non si esauriscono qui, questi infatti sono i soli poteri generali di cui è dotata l'Autorità Nazionale cui si accostano dei poteri specifici in relazione a singoli particolari trattamenti. L'articolo 36 introduce un dovere specifico di consultazione preventiva dell'Autorità in capo al titolare in quei casi in cui i rischi presentati a seguito di una DPIA sono " elevat(i) in assenza di misure adottate dal titolare del trattamento per attenuare il rischio."

Dalla dizione della norma sembra necessaria e sufficiente la presenza di un rischio elevato per far nascere l'obbligo di consultazione preventiva ma ciò paralizzerebbe l'attività dell'Autorità che non sarebbe più in grado di gestire, in quei termini fissati in otto settimane[93], tutte le attività dei titolari. A conferma di ciò, soccorrono i Considerando 84[94] e 94 , quest'ultimo nello specifico esplicita che "Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'inter ferenza con i diritti e le libertà della persona fisica. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e poteri previsti dal presente regolamento, compreso il potere di vietare i trattamenti."

La scriminante quindi tra l'obbligatorietà o meno di una consultazione preventiva sta nella circostanza che "il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione" configurandosi così una sorta in impossibilità a ridurre quei rischi. L'Autorità in questa circostanza deve valutare la fondatezza dei timori presentati del titolare e l'impossibilità di integrare il sistema con strumenti idonei a ridurre, limitare o gestire i rischi entro limiti di tollerabilità. Se ritiene che i rischi siano "accettabili" oppure che il sistema possa

93 Può essere richiesta una proroga di ulteriori sei settimane nel caso in cui le circostanze del caso lo rendano necessario. Tuttavia in nessuna disposizione del regolamento si fa riferimento all'istituto del silenzio-assenso

94 Per completezza, il considerando (4 dal canto suo fissa che " […] Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo."

essere utilmente integrato, comunica al titolare la possibilità di iniziare il trattamento dopo che abbia applicato le evenutali ulteriori misure di sicurezza, altrimenti lo nega.

Nel caso in cui tale comunicazione non sia preventiva ma sopraggiunga a trattamento già iniziato, ad esempio perche tale rischio ineliminabile venga rilevato solo successivamente, l'Autorità di Controllo può anche ricorrere ai poteri riconosciutigli dall'articolo 58 per sospendere temporaneamente l'attività di trattamento.

7. L'Autorità di controllo.

Un elemento che indica in modo piuttosto evidente l'inteconnessione tra i protagonisti del GDPR in un costante gioco di *check and balance*[95], sta proprio nel fatto che l'esposizione ogni "nuova" figura delineata dal regolamento, è già stata introdotta nella spiegazione della precedente.

L'Autorità Garante non è un'innovazione portata dal GDPR in quanto naque già in virtù della Direttiva 45/95, la quale richiedeva ad ogni Stato Membro dell'allora Comunità Europea, di munirsi di tale struttura indipendente preposta alla vigilanza della corretta applicazione della normativa sulla privacy.

In Italia è stata istituita con la legge n. 675 del 1996, poi disciplinata dal d.lgs n. 196 del 2003, codice in materia di protezione dei dati personali, ed infine dal Regolamento 679/2016.

L'autorità è composta da quattro membri[96], eletti da ciascuno dei due rami del Parlamento, e al loro interno ne nominano uno come presidente, il voto del quale prevale in caso di parità. I membri devono essere scelti tra persone che assicurino indipendenza e che siano esperti riconosciuti nelle materie del diritto o dell'informatica, deve essere garantita la presenza di entrambe le qualificazioni[97]. Durano in carica sette anni e il mandato non può essere rinnovato.

Il suo compito primario, definito nell'articolo 51, è rimasto in parte invariato da quello definito nella Direttiva e cioè quello di "sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento " ma viene integrato da una nuova finalità, che è tra l'altro il nuovo fine di tutto il Regolamento, quello "di agevolare la libera circolazione dei dati personali all'interno dell'Unione."

Tali compiti devono essere svolti dall'Autorità di Controllo in armonia con tutte le altre strutture nazionali presenti in ogni Stato dell'Unione attraverso un coordinamento che parte dal Comitate Eurpoeo per la Protezione Dati, prospettando due diverse linee di rapporti e competenze, una verticale e gerarchica che consente al Comitato di indicare le politiche che le singole Autorità nazionali devono seguire nello

95 Letteralmente viene tradotto come "poteri e contropoteri."
96 L'attuale collegio si è insediato nel giugno 2012 ed è così composto: Antonello Soro, il presidente, Augusta Iannini, la vice presidentessa, Giovanna Bianchi Clerici, Licia Califano.
97 I requisiti di indipendenza e professionalità dei suoi membri vengono definiti nell'articolo 53 GDPR.

svolgimento delle loro attività ed uno orizzontale ed organizzativo che pone le regole di coorinamente tra le singole Autorità in particolare per quei trattamenti transfrontalieri che coinvolgono la competenza di più strutture nazionali.

L' articolo 68 del GDPR è dedicato a definire la composizione del Comitato che "è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.[98]" Alla definizione dei suoi compiti è preposto poi l'articolo 70 che fissa un elenco piuttosto lungo, comprendente 25 diverse attività, tra cui spiccano i forti poteri di comunicazione generale con la Commissione che si concretizzano in consulenze e pareri[99], pubblica linee guida, raccomandazioni e *best practices* in numerosi settori[100], coordina e controlla le azioni delle Autorità nazionali e ne promuove l'armonizzazione[101] ed infine ha il piu ampio e generale potere di "sorveglia(re) il presente regolamento e assicura(rne) l'applicazione corretta, fatti salvi i compiti delle autorità nazionali di controllo."

In merito ai rapporti orizzontali tra le Autorità di Controllo nazionali, bisogna preliminarmente anticipare che ogni Autorità ha una competenza ad esercitare i proprio compiti e poteri, limitatamente al territorio dello Stato in cui è istituita in armonia con l'articolo 55. Il Regolamento tuttavia mira anche a districare gli spiecevoli inconveniente che potrebbero generarsi dall'intervento di due o più autorità per quei trattamenti che presentano alti profini di transnazionalità, evitando preventivamente la paralisi del sistema.

La tecnica utilizzata è stata rinominata in dottrina come *One-Stop Shop* e viene definita nell'articolo 56 il quale incardina "(nel)l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento, (l'organo) competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60." Ciò non implica tuttavia che le altre Autorità di controllo, diverse dalla capofile, perdano i loro poteri ma semplicemente li dovranno andare a coordinare, secondo i principi di trasparenza e collaborazione, con i poteri di quest'ultima che rimarrà l'unica interlocutrice diretta con il titolare e l'unica legittimata a notificargli decisioni con riferimento alla sua attività.

7.1. Compiti e poteri in generale.

Il ruolo dell'Autorità nazionale si concretizza quindi nella vigilanza e nella sorveglianza dell'intero sistema così da garantire che i trattamenti siano effettuati da un lato nel rispetto dei diritti degli interessati e dall'altro nello sviluppo della società informatica secondo il principio della libera circolazione dei dati. Tale ruolo però è arricchito da una serie di compiti ancellari e specifici, elencati dettagliatamente nell'articolo 57,

98 In accordo con l'articolo 73, "il collegio elegge un presidente e due vicepresidenti tra i suoi membri a maggioranza semplice."
99 Si vedano a tal proposito le lettere *b), c), q), r), s)* dell'articolo 70, primo comma del GDPR.
100 A tal proposito richiamo le lettere *d), f), g), h), i), l), j), k), m)* dell'articolo 70, primo comma del GDPR.
101 Le lettere *t), u), v), w)* dell'articolo 70, primo comma del GDPR si occupano della materia.

quali promuovere la consapevolezza e favorire la comprensione del pubblico, dei titolari del trattamento e fornire consulenze agli Stati[102], trattare i reclami proposti e svolgere indagini, incoraggiare l'istituzione di meccanismi di certificazione e codici di condotta. Tuttavia la lettera *v)* dell'articolo 57.1 specifica che non si tratta di un'elenco chiuso, in quanto è legittimata a "svolge(re) qualsiasi altro compito legato alla protezione dei dati personali."

Il compito che risulta più rilevante ai fini della trattazione però è contenuto nella lettera *i)* che le consente di "sorveglia(re) gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali." Si dimostra con tutta coerenza quindi l'intento di far gravare sulla figura del Garante, il compito fondamentale di adeguare costantemente la tutela dei diritti e la libera circolazione dei dati sia alle nuove tecnologie disponibili che alle prassi commerciali, per evitare che si creino abusi o vuoti normativi nel tempo.

Tutti questi compiti possono essere perseguiti però nel rispetto delle norme che attribuiscono i poteri fondamentali alle Autorità di controllo nazionali, e cioè nel rispetto dell'articolo 57 del Regolamento.

Nell'analisi di tale articolo si riesce a osservare come i poteri dell'Autorità siano parametrati con intensità e portata diversa a seconda dei compiti che è chiamata a svolgere, talvolta assumendo competenza generale mentre in altre circostanze entrando solo nel particolare di singoli trattamenti.

La norma divide tali poteri in tre categori, nelle prime due vengono definiti i poteri d'indagine e correttivi che l'Autorità può esercitare nei confronti dei singoli trattamenti, partendo dal poter ottenere dal titolare "l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti" fino ad arrivare ad "imporre una limitazione provvisoria o definitiva al trattamento" o ad "infliggere una sanzione amministrativa pecuniaria."

La terza categroia attiene ai poteri atuorizzativi o consultivi, dove l'Autorità pone in essere un'attività più programmatica, volta ad avere un'applicazione più generale, in vista degli sviluppi ulteriori della materia. Rientrano a pieno titolo in questa categoria, il rilascio di pareri su progetti di codici di condotta, il rilascio diretto di certificazioni o l'accreditamento di organismi di certificazione ed infine i già richiamati pareri consultivi per quei trattamenti che presentano alti rischi per gli interessati[103].

Risulta così più chiaramente il duplice ruolo che rivestono oggi l'Autorità di controllo, da un lato sono l'organo preposto a sorvegliare la corretta applicazione del Regolamento nel presente ma allo stesso tempo sono il ponte necessario che collega la normativa di oggi allo sviluppo tecnologico del domani.

102 Precisamente "al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento."

103 Si veda poco sopra il paragrafo 6.5.1.

CAPITOLO II

Le tecnologie della società digitale.

1. Le vecchie e le nuove frontiere dell'Intelligenza Artificiale.

La storia dell'informatica ed i suoi successi sono il risultato di ricerche ed esperimenti che si inquadrano in una finestra storica davvero molto esigua, poco meno di un secolo ma nonostante ciò ha determinato uno dei cambiamenti sociali e culturali più rilevanti di tutta la civiltà umana.

Ufficialmente, la nascite della disciplina viene fatta coincidere con un evento ospitato nella Dartmounth, un' Università Americana del New Hampshire, il *Dartmouth Summer Research Project on Artificial Intelligence*, anche se negli anni appena precedenti erano già iniziate le prime ricerche[104].

L'obiettivo comune di questi studi, era quello di costruire una macchina che avesse, in alcuni domini applicativi, delle capacità di ragionamento ed elaborazione simili a quelle umane, come dimostra la ricerca condotta tra il 1964 ed il 1966 dall'informatico tedesco Joseph Weizenbaum che ha dato alla luce Eliza Doolittle.

Il sistema Eliza è un'Intelligenza Artificiale in grado di comunicare con l'uomo attraverso un liguaggio naturale, nel caso in inglese, sfruttando una serie di tecnologie piuttosto all'avanguardia ma nonostante ciò la macchina era in grado solo di comparare le informazioni tra *input* ed *output* senza elaborarle.

Più in generale, l'approccio seguito in quel tempo per l'elaborazione degli algoritmi, era quello esplorativo, dove si richiedeva alla macchina di sondare in modo dettagliato ed esaustivo tutto uno spazio di ricerca. Per arrivare alla soluzione finale, si chiedeva al sistema di prendere ogni alternativa possibile e nel caso in cui non portasse al risultato sperato, il *software* riusciva, attraverso una tecnica che viene chiamata *backtraking*, a ritornare indietro sui suoi passi così da poter esplorare ulteriori tentativi.

Questa laboriosa tecnica di esplorazione, per quanto efficace, risultò, relativamente efficiente solo in domini applicativi piuttosto ristretti. Uno spazio di ricerca moderatamente ampio, portava la macchina ad dover esplorare un numero di alternative troppo grande e questo le diventava proibitivo, tale evento viene denominato in informatica come esplosione combinatoria.

Se a questo problema si aggiunge anche la circostanza che negli anni 60 la potenza e la velocità di elaborazione di una macchina era notevolmente più ridotta di quella odierna, si comprende bene perchè questi primi anni di ricerca non portarono tutti i risultati ambizioni che gli scienziati si erano prospettati.

Per comprendere meglio la limitatezza degli spazi in cui un'intelligenza articifiale sarebbe stata capace di operare, si prende convenzionalmente ad esempio gli algoritmi di gioco su scacchiera come dama

104 Solo per richiamare le più importanti: nel 1950 Alan Turing pubblica, sulla rivista *Mind*, nell' articolo *Computing machinery and intelligence,* il suo Test per valutare se una macchina intelligente può ufficialmente definirsi tale; nel 1951, parte il progetto SNARC portato avanti da *Minsky* e *Edmonds* per la creazione della prima macchina a neuroni artificiali.

o scacchi.

Un sistema per poter giocare, deve elaborare di volta in volta ogni possibile posizionamento dei pezzi sulla scacchiera, cui è associato a uno punteggio. Alla vittoria si associa il punteggio +, alla sconfitta -.

Nel momento in cui l'algoritmo deve scegliere come muoversi, valuta tutte le possibili alternative a sua disposizione, le contromosse che potrebbe compiere l'avversario, le sue contro contromosse alla mano successivo, e così via sempre più in profondità, potenzialmente fino a fine partita. Esplorando più in profondità possibile, un semplice algoritmo valuta ogni segnale negativo e positivo che è stato registrato in ogni nodo passaggio dopo passaggio per poi trovare la mossa migliore e cioè quella che contenga il maggior numero di segnali positivi.

Purtroppo l'albero delle possibili alternative diventa troppo grande già dopo pochi livelli di profondità, pertanto la valutazione del segnale avviene prematuramente, e la scelta è solo parzialmente la migliore. Solo per riportare qualche esempio numerico, all' inizio di una partita a scacchi, una macchina ha a disposizione 30 possibili mosse. Se poi è stata programmata per riuscire a calcolare anche le 5 mosse successive che vengono compiute dopo la sua, si ritroverà a dover esplorare milioni di miliardi di alternative (un numero equivalente a $10^{(15)}$), generando un'esplosione combinatoria difficilmente gestibile anche con elaboratori odierni, dotati di capacità di calcolo straordinarie[105].

Ad un iniziale entusiasmo sulla ricerca delle IA, che ha portato a finanziamenti anche molto elevati[106], provenient sopratutto da strutture governative, si è succeduto un periodo di delusione. I risultati non erano nemmeno lontanamente quelli attesi, ed i limiti riscontrati sembravano assolutamente invalicabili allo stato dell'arte: le intelligenze artificiali erano in grado solo di risolvere problemi futili e sembrava totalmente impossibile inserirli in contesti complessi. Il periodo intercorrente tra il 1974 ed il 1980 è noto come il primo inverno dell'informatica, i finanziamenti terminarono e le ricerche si ridussero notevolmente.

Ciò che porto nuovo vigore alla ricerca scientifica fu la progettazione del sistema esperto, XCON, sviluppato da *Carnegie Mellon* per la *Digital Equipment Corporation,* che aveva la capacità di risolvere una serie di problemi in determinati ambienti, sfruttando la conoscenza e l'esperienza dell'operatore umano. Per fare capire la portata di questo nuovo sistema, la società risparmiò circa 40 milioni di dollari.

Un simile risparmio ha fatto gola a numerosissime società che hanno iniziato a stanziare fondi, che complessivamente superano la soglia del miliardo di dollari, per la ricerca informatica e per sviluppare sistemi esperti in grado di garantire una riduzione sostanziale dei costi d'impresa.

Un sistema esperto utilizza delle strategie logico-operative diverse da quella esplorativa ed è denominata *knowledge-based systems*: per risolvere un problema, non vanno ricercate tutte quelle che sono

105 È per questo che oggi si affiancano a queste tecniche esplorative, degli approcci euristici per il pruring di rami e le tecniche di apprendimento automatico.

106 Ad esempio, nel 1967, il governo Giapponese finanziò un progetto della *Wasada University* finalizzato ala creazione di un *Robot* umanoide multifunzionale (con capacità di comunicare, muoversi, afferrare etc). Oppure nel periodo tra il 1963 al 1970, il MIT fu finanziato per oltre 5 milioni di dollari, dalla *DARPA (Defense Advanced Research Projects Agency)*.

le alternative ipotizzabili ma vanno sfruttate quelle che sono le conoscenze contenute dal sistema in materia così da individuare da subito le scelte più probabili.

Attraverso questo metodo veniva decisamente inibito il problema dell'esplosione combinatoria, tuttavia i limiti degli elaboratori del tempo permettevano la costruzione di *hardware* capaci di contenere solo un limitato numero di informazioni nei *dataset* quindi i sistemi riuscivano ad operare solo in campi operativi ristretti.

Dal 1980 e fino alla fine del decennio, la ricerca fu florida e iniziò una nuova fase di finanziamenti ancora più ingente di quella precedente[107] ma la situazione non durò per molto. Stavolta a determinare il secondo inverno dell'Intelligenza Artificiale furono due colossi del settore IBM e Apple che nel 1987 iniziarono ad immettere sul mercato i primi *personal computer* che possedevano capacità di calcolo simili a quelle dei sistemi esperti ma con un costo drasticamente ridotto.

Va tuttavia segnalato che non fu solo l'avvento di questi *computer* a determinare il declino dei sistemi esperti in quanto questi avevano il limite di non poter essere aggiornati agevolmente e quindi andavano sostituiti in brevi periodi di tempo.

Assistiamo ora alla terza primavera dell'IA, la più lunga, in quanto è iniziata oltre 25 anni fa, nel 1993 e perdura tutt'oggi. La rinascita di vigore della materia, fu possibile sia grazie ad una forte integrazione tra l'informatica ed altre discipline (dando vita, ad esempio, alla ricerca operativa) sia in ragione delle potenziate capacità di calcolo delle macchine.

Le tecniche di progettazione degli algoritmi infatti non variano troppo rispetto al passato, vengono solo perfezionate ed adattate a macchine che hanno delle possibilità d'elaborazione infinitamente superiori.

Ad esempio, oggi una macchina Intelligente per definirsi tale ha bisogno di almeno una fase di *learning,* cioè, una fase di apprendimento, ma va osservato come tale tecnica esista già da oltre 30 anni, solo che risultava impossibile fare un *training* ai sistemi prima di essere commercializzati, poiché, con la velocità di calcolo dell'epoca, sarebbe stato necessario un lasso di tempo eccessivo.

I limiti di ieri sono stati colmati dalla tecnologia del domani e questo era già stato ampiamente prospettato da molti esperti, primo tra tutti Gordon Moore[108] che, nel 1965, pubblicò su una rivista scientifica una sua osservazione empirica che diventò ben presto una legge. Oggi infatti, in informatica è indicata come prima legge di Moore il seguente enunciato:

"La complessità di un microcircuito, misurata ad esempio tramite il numero di transistori per chip,

107 Oltre al fatto che l'istituto governativo statunitense di difesa, il *DARPA,* riprende i finanziamenti alla ricerca che aveva interrotto attorno al 1974, il Giappone stanziò un totale di 800 milioni di Yen per progettare una macchina in grado di conversare e tradurre tesi in varie lingue e l'Inghilterra seguì le stesse finalità stanziando altri 350 milioni di sterline.

108 Gordon Moore, che all'epoca era a capo del settore *R&D* della *Fairchild Semiconductor* e tre anni dopo fondò la *Intel*, scrisse infatti un articolo su una rivista specializzata nel quale illustrava come nel periodo 1959-1965 il numero di componenti elettronici (ad esempio i *transistor*) che formano un *chip* fosse raddoppiato ogni anno.

raddoppia ogni 18 mesi (e quadruplica quindi ogni 3 anni).”[109]

L'elevazione a legge di tale enunciato è dovuta dal fatto che tra il 1965 al 2018, lo sviluppo tecnologio ha sempre mantenuto questo standard di crescita, infatti ora i chip hanno dimensioni dell'ordine di alcune decine di nanometri[110] ed una potenza di calcolo davvero straordinaria[111]. Va sottolineato anche come, nonostante stiamo per raggiungere il limite fisico, nella creazione di *chip* sempre più piccoli, la scienza si stia già muovendo verso la ricerca di nuovi elaboratori, primo tra tutti quello quantistico che ha capacità di calcolo potenziali praticamente infinite.

Ciò che più rileva è che in questa terza primavera dell'Intelligenza Artificiale, ci stiamo godendo i frutti più maturi di una ricerca che va avanti da molti anni, e ciò è dimostrato dai grandi successi che si sono registrati. Partendo con ordine, il primo traguardo è stato ottenuto dalla *IBM* quando nel 1997, il suo sistema *Deep Blue* riesce a vincere a schacci contro il campione mondiale Garry Kasparov.

Il sistema era capace di calcolare lo *score* di 200 milioni di disposizioni sulla scacchiera al secondo. La potenza di calcolo era strabiliante per l’epoca ma, come dimostra la legge di Moore, ora è inferiore a quella di un moderno smartphone.

Il programma inoltre riusciva ad andare in profondità nella predizione delle mosse successive con una media di 6-8 livelli e l'esposione combinatoria era contenuta grazie a tecniche euristiche sofisticate, ottenute dopo una lunga fase di *learning*.

Nel 2005, durante la *DARPA Grand Challenge*, un veicolo a guida autonoma è riuscito a percorrere oltre 131 miglia in un percorso tracciato nel deserto e solo due anni dopo, nel 2007, nel corso della *DARPA Urban Challenge*, un veicolo a guida autonoma è riuscito a percorrere 55 miglia nel traffico urbano e nel rispetto della segnaletica stradale.

Sempre la *IBM* ha ottenuto un successo pazzesco nel 2011, quando il suo sistema *Watson*, partecipa a un complicatissimo quiz televisivo chiamato, *Jeopardy*. Il colosso dell'informatica Statunitense aveva lanciato una sfida a tutti i precedenti vincitori del quiz ed in un evento durato tre puntate, *Watson* li ha sconfitti tutti.

Questa brillante IA è dotata di software per l’elaborazione del linguaggio naturale, rappresentazione della conoscenza, ragionamento automatico, e di tecnologie di apprendimento nel campo delle risposte a

109 Moore, G. E. (1965). *Cramming more components onto integrated circuits*. *Proceedings of the IEEE*, *86*(1), 82-85.

110 Unità di misura di lunghezza pari a un miliardesimo di metro.

111 Ad esempio è stato creato nel 2017 un *chip* di circa 5 nanometri, dai ricercatori di *Ibm*, in collaborazione con *Samsung* e *Global Foundries*. Secondo il prototipo presentato durante il *“2017 Symposia on VLSI Techonology and Circuits”* a Kyoto, il chip del futuro sarà capace di integrare ben 30 milioni di *transistor*, diventando così molto più potenti ed efficienti di quelli attuali da 10 nanometri ed in grado di alimentare autovetture, intelligenza artificiale e sensori 5G degli smartphone.

domande a dominio aperto senza restrizioni sull'argomento. Per far capire quanto sia straordinaria la sua capacità di comprensione di linguaggio e di ragionamento va specificato che il gioco *Jeopardy* inverte la normale logica di un quiz. Il presentatore infatti fornisce solo la risposta e sarà compito dei partecipanti andare a ricostruire la domanda corretta a quella risposta.

Durante il quiz, Watson era in grado di poter lavorare solo in *offline mode* e quindi aveva accesso a 200 milioni di contenuti, tutti caricate in RAM: enciclopedie, dizionari, thesauri, tassonomie, ontologie e articoli giornale. La risposta viene fornita dal sistema attraverso un meccanismo probabilistico in cui sono formulate tre ipotesi di risposta e successivamente, analizzate tutte le informazioni contenute in RAM, il sistema sceglierà quella con una percentuale di successo più alta[112].

Dopo il suo successo Watson ha "deciso" di dedicarsi ad altro ed infatti nel febbraio 2013, la IBM ha annunciato che la prima applicazione del sistema *Watson* sarà nella gestione delle decisioni nel trattamento del cancro ai polmoni al *Memorial Sloan-Kettering Cancer Center*[113].

L'ultimo esempio è emblematico della velocità del progresso in questa "primavera" dell'informatica. *Deep Blue* fu la macchina che nel 1997 stupì il mondo dopo aver sconfitto il campioni di scacchi Kasparov, ma nel 2016 *Google* ha progettato un'intelligenza artificiale che è stata in grado di sconfiggere il campione mondiale in un gioco ancora più sofisticato e complicato chiamato *Go*, impossibile da approcciare con algoritmi di "forza bruta." *Go* è un antico gioco cinese, con regole semplici ma molte più mosse possibili rispetto agli scacchi, cosa che, in termini pratici, richiede un approccio molto più intuitivo.

Infatti, mentre *Deep Blue* usa strategie di ricerca in profondità integrata da sistemi euristici, *AlphaGo* è basato principalmente su tecniche di *machine learning*[114]. Inizialmente sono addestrate in modo supervisionato due *deep neural network*[115], cercando di imitare le mosse di professionisti a partire da partite memorizzate e rese disponibili dai *GoServer* su Internet, comprendenti oltre 30 milioni di mosse. Poi il sistema gioca milioni di partite contro sé stesso utilizzando un apprendimento rinforzato per migliorare la strategia.

Ovviamente ogni primavera dell'informatica è sempre stata accompagnata da ingenti finanziamenti, sopratutto governativi ma in questo caso assistiamo ad un' inversione di tendenza. I *big* dell'ICT[116] (*Microsoft, Apple, Facebook, Google, Amazon, IBM, Samsung, etc*.) investono molto nel settore reclutando talenti e acquisendo start-up, con un fenomeno noto come *grab of talents.*

112 Si veda anche *infra* paragrafo 2.1. per una spiegazione più dettagliata del modo in cui un *software* riesca a scegliere una risposta piuttosto che un'altra nella parte relativa ai *pattern* e al *pattern recognition.*

113 Per maggiori dettagli sulle sue applicazioni, si consulti http://www.ibm.com/watson/watson-oncology.html

114 Risulterà un termine un po' ostico da comprendere se si è digiuni della materia ma nella sua traduzione più semplice significa "apprendimento automatico." Si veda *infra* paragrafo 2.1. per approfondimenti.

115 Anche questo concetto sembra molto difficile da comprendere ma rimando alla lettura *infra* paragrafo 2.2 per una maggiore comprensione del sistema.

116 Significato di ICT: *Information Communication Technology*. Indica l'insieme delle tecnologie che consentono il trattamento e lo scambio delle informazioni in formato Digitale.

Non è ancora chiaro se questo fenomeno potrà danneggiare o rendere ancora più florida la terza primavera delle IA ma per ora, molti studiosi, sembrano assolutamente certi che questo sviluppo sia irrefrenabile e primo tra tutto è il matematico e romanziere Vernor Vinge che in un saggio del 1993 parla di "singolarità tecnologica". Il concetto è molto semplice, è un momento, congetturato nello sviluppo di una civiltà, in cui il progresso tecnologico accelera oltre la capacità di comprendere e prevedere degli esseri umani.

La singolarità avrebbe, a parere di Vinge ed altri studiosi, l'effetto catastrofico di invertire il rapporto uomo-macchina, rendendo il primo servo del secondo in quanto cognitivamente inferiore[117].

Qualunque sarà l'epilogo di questo affascinante periodo storico, il compito che mi accingo a svolgere è proprio quello di rispondere all'appello formulato nel 2015 nella *Open Letter on Artificial Intelligence,* scritta e firmata da numerosi personaggi illustri quali *Hawkins, Musk, Hinton, Bengio, etc*. In questa lettera si effettua una considerazione, le IA possono avere o un effettivo miglioramento della vita umana oppure possono divenire causa di distruzione e povertà[118], è proprio per tale motivo che questi scienziati si raccomandano di dedicare fin da ora tutte risorse possibili allo studio del problema del "controllo" di super-intelligenze artificiali da parte dell'uomo.

2. L'Intelligenza di un artificio.

Prima ancora di trattare la parte pratica di come funzionano queste macchine intelligenti va analizzato l'approccio che i ricercstori hanno adottato per affrontare la questione. La domanda più ostica a cui gli informatici hanno dovuto dare risposta è proprio quella di definire il concetto di Intelligenza.

Questo concetto racchiude in se una serie piuttosto complessa di attività che sono difficilmente spiegabili nel loro complesso anche in tempi recenti; oltre al ragionamento in senso stretto, inteso quale capacità di comprendere un problema per poi trovarne una soluzione, il cervello umano è in grado di effettuare considerazioni, riflessioni e critiche, attraverso il meta-ragionamento che ha dato vita, a quelle che sono le più grandi opere artistiche, musicali e letterarie dell'unamità.

Il nostro pensiero infatti è in grado di interiorizzarsi e di percepire gli stimoli derivanti da sentimenti e desideri, permettendo una forma di Intelligenza squisitamente umana ed a tratti anche irrazionale. Non ci si aspetterebbe mai che una macchina, si innamori di un'altra macchina o che riesca a comporre opere d'arte del livello di un Dante ma in realtà difficilmente si può concepire che una macchina sia in grado di provare, in generale, un' emozione[119].

117 Il concetto di singolarità informatica ed alcune riflessioni sul futuro dello sviluppo tecnologico sono fornite anche dal celebre inventore, informatico e saggista statunitense Raymond Kurzweil in una lunga serie di saggi.

118 Letteralmente "*The letter affirmed that society can reap great potential benefits from artificial intelligence, but called for concrete research on how to prevent certain potential "pitfalls": artificial intelligence has the potential to eradicate disease and poverty.*"

119 Tale concetto venne spiegato in modo affascinante nel 1949, dal famoso neurochirurgo Sir Geoffrey Jefferson, nel suo scritto *No Mind for Mechanical Man*, esponeva una serrata critica ad un precedente articolo che riguardava la macchina universale di

Proprio per questo va sottolineato come la ricerca non si sia concentrata troppo sulla parte introspettiva del pensiero (per ora) ma ha concentrato tutti i suoi sforzi nella parte esteriore del pensare umano, cercando di incardinare le tecniche di ragionamento in algoritmi in grado di riprodurlo..

Ad oggi, infatti, l' Intelligenza Artificiale può essere definita come la disciplina che racchiude le teorie e le tecniche per lo sviluppo di algoritmi che permettano alle macchine di riprodurre attività intelligente, per lo meno in specifici domini e ambiti applicativi. La riproduzione di queste attività è quindi solo parziale rispetto all'attività intellettuale propria dell'uomo: ciò che più interessa riprodurre solo le capacità di apprendimento, di riconoscimento e di scelta.

Diviene così evidente che urge una classificazione formale delle funzioni astratte di ragionamento e apprendimento dell'uomo per poter costruire su di essi dei modelli computazionali in grado di concretizzare tali forme di ragionamento e apprendimento.

A tal proposito Aristotele delineò tre diverse modalità di ragionamento che permettono all'uomo di apprendere e conoscere informazioni nuove partendo da quelle già note. Tali sono il ragionamento deduttivo, quello induttivo e l'abduzione che differiscono tra loro solo per il diverso grado di probabilità con cui si passa dai dati noti (premesse maggiori) ai dati ignoti (premesse minori).

Partendo con ordine, nel ragionamento deduttivo, il *cd.* sillogismo, la verità delle premesse (caso generale) garantisce la verità della conclusione (caso particolare)[120]. Tale metodo è il fondamento di gran parte delle dimostrazioni e teoremi della matematica ma non ci permette di scoprire o prevedere fatti nuovi e quindi di ampliare le nostre conoscenze, impedendo la migrazione dal noto all'ingoto.

Nel ragionamento induttivo, diversamente da quello deduttivo, le premesse, forniscono un'evidenza più o meno forte a sostegno della conclusione ma non ne garantiscono necessariamente la verità[121]. Tale sistema comporta quindi un rischio in quanto si tratta di un ragionamento solo possibile, le cui conclusioni dipendono dal grado di probabilità delle informazioni contenute nelle premesse.

La forma più comune di ragionamento induttivo è la generalizzazione[122], con cui si estendono informazioni su un gruppo di cose, persone, *etc.*, conoscendo solo quelle relative ad una porzione di quel gruppo. Non si ha una verità assoluta tra caso particolare e conclusioni ma consente di esplorare parti del non noto partendo dalle informazioni note, tuttavia con il rischio di sbagliare.

Questo permette di estrarre concetti portandoli da un domino all'altro[123].

Turing: "Fino a quando una macchina non potrà scrivere un sonetto o comporre un concerto suggeriti da emozioni realmente provati, e non per una scelta casuale di simboli, non potremo ammettere che una macchina eguagli il cervello umano; cioé che non solo scriva queste cose, ma che sappia di averle scritte. E' certo che nessun meccanismo potrebbe provare piacere (e neppure manifestarlo artificialmente, un facile espediente) verso i propri successi e angosce quando gli saltano le valvole, né animarsi davanti alle lusinghe, o rattristarsi per i propri errori, o essere affascinato dal sesso, o incollerirsi o deprimersi quando non può ottenere ciò che desidera."

120 L'esempio classico di un sillogismo è REGOLA: Tutti gli uomini sono mortali - CASO : Socrate è un uomo. Il risultato è che "Socrate è mortale."

121 CASO: Socrate era un uomo. RISULTATO: Socrate morì. Ne deriva, secondo il ragionamento induttivo che la regola è che "Tutti gli uomini sono mortali."

122 Un' altra forma di induzione molto potente è il ragionamento per Analogia, che consiste nel trarre conclusioni su qualcosa in base alle sue somiglianze con qualcos'altro.

123 In questo caso se la REGOLA fosse: Tutti gli uomini sono mortali, ed il RISULTATO: Socrate morì, ne deriverebbe che (CASO): Socrate era un uomo.

Anche nel caso del ragionamento abduttivo, l' *iter* logico è solo probabilistico, ma invece di generalizzare ci si muove attorno alla regola, ipotizzando che un'implicazione generale valga anche per il caso specifico. Si parte così da una base certa di conoscenza e si cerca di arrivare al caso concreto anche se non è sicuro che questo possa essere applicato alla fattispecie. In sostanza si estendono le informazioni note anche a quei casi ignoti che potrebbero, o no, appartenere a quella stessa caregoria potrando ad una conlusione solo probabile ma nuova.

L'Intelligenza di una macchina quindi va valutata quasi esclusivamente sul modo in cui gli algoritmi riescono a incardinare ed integrare i ragionamenti *standard* appena esposti, nel riuscire a renderli fluidi all'interno di un elaboratore e al tempo stesso nella capacità del sistema di colmare le lacune di ragionamenti complessi o di informazioni incomplete con adeguate tecniche euristiche.

L'altro parametro di valutazione di un'Intelligenza Artificiale stà nella quantità ma sopratutto nella qualità[124] delle informazioni che contiene, poiché sarà proprio sulla base di queste che si andrà a fondare ogni ragionamento, *rectius* premessa maggiore, della macchina.

2.1. Il Test di Turing: successi e criticità.

In quegli anni, la disputa che si stava accendendo in dottrina, sulla possibilità concreta di realizzare una macchina Intelligente, ha portato molti scienziati ad interrogarsi sulle reali capacità di queste macchine cercando di verificare quando e in quale misura questo risultato potesse considerarsi raggiunto.

Ebbene, non esistendo una definizione universalmente accettata di "Intelligenza", la questione diveniva piuttosto complicata poiché risultava difficile convincere un'intera platea delle reali possibilità di una macchina con dei semplici test cognitivi. Una brillante soluzione a questo limite fu delineata da Alan Turing che piuttosto di trovare un test in grado di convincere l'essere umano, lo inganna.

Il cosiddetto Test di Turing, fu infatti ispirato a un gioco di società, il "gioco dell'imitazione", nel quale un interrogatore pone domande a due persone di sesso diverso, per individuare chi di questi sia l'uomo e chi la donna, senza che il primo abbia contatto diretto con i secondi (gli interlocutori ricevono la domanda e rispondono mediante telescrivente).

Ciò che rende il gioco più complesso sta nel fatto che i due interlocutori hanno due fini diversi: uno è sincero, agevolando l'identificazione da parte dell'intervistatore, e l'altro mente, impedendola.

Una volta completato il test, l'interrogatore deve individuale chi dei due interlocutori è l'uomo e chi la donna. Il gioco si ripete N volte, se l'intervistatore sbaglia il sesso dei partecipanti X volte, il suo tasso di errore è pari a X/N.

124 Vedi *infra* paragrafo 4.

Solo a questo punto può iniziare la seconda fase del Test di Turing, dove si sostituisce uno dei due partecipanti con un computer. In questo modo l'intervistatore deve capire se a rispondere è un uomo oppure una macchina. Il procedimento non muta: l'intervistatore formula le sue domande tramite telescrivente e gli interlocutori rispondono con lo stesso mezzo. Alla fine del gioco dovrà, ancora una volta, identificare i partecipanti.

Il gioco si ripete N volte e se l'intervistatore sbaglia l'identificazione dei partecipanti Z volte, il suo tasso di errore percentuale sarà pari a Z/N.

Le due fasi sono assolutamente necessarie (anche se in realtà è molto più nota la versione semplificata del test di Turing[125]) perchè forniscono due valori che possono essere direttamente confrontati, così da osservare quante volte l'interlocutore umano è stato più o meno "abile" nell' ingannare l'interrogatore rispetto alla macchina. Secondo Turing, un' Intelligenza Artificiale si realizza quando un sistema informatico riuscirà a ingannare l'interrogante facendogli credere di essere una persona quando la percentuale di errore nel gioco in cui partecipa la macchina è simile o inferiore a quella del gioco per individuare l'uomo e la donna ($X/N \cong o < Z/N$.)

Alan Turing aveva previsto che entro il 2050 le macchine avrebbero potuto superare il suo test. In effetti le sue predizioni si sono quasi avverate nel corso degli anni, grazie ad un caso che ha dato una svolta nella storia delle IA: si tratta di Eugene Goostman, un software ideato da Vladimir Veselov ed Eugene Demchenko, programmato per sembrare un tredicenne ucraino al fine di ingannare i giudici della Royal Society, l'Accademia delle Scienze britannica.

Questi ultimi, ponendo domande specifiche contemporaneamente sia ad Eugene che ad un uomo, dovevano capire chi dei due fosse la macchina. Il risultato su strabiliante, per la prima volta un calcolatore avrebbe passato il test di Turing, in quanto Eugene avrebbe convinto il 33% dei giudici di essere umano nel corso di 150 conversazioni.

Non mancano comunque le critiche e le smentite riguardo al superamento di Eugene del test, in quanto la soglia fissata del 30 per cento, non sarebbe mai stata menzionata da Turing nei suoi scritti. Il matematico inglese sosteneva che la prova si sarebbe dovuta considerare passata solo se la macchina fosse stata in grado di far cadere in errore l'esaminatore con almeno la stessa frequenza con cui questi confonderebbe un uomo e una donna.

Dunque, il 33%, per quanto significativo, non è il traguardo ma è solo un notevole passo avanti verso il traguardo di creare una forma di Intelligenza talmente complessa e sofisticata da arrivare ad ingannare un essere umano in merito alla sua natura Artificiale.

125 Si tratta di un test molto più snello: si compone di una sola fase e vede come protagonisti solo un interrogatore umano ed un interlocutore robotico. L'interrogatore non sa di parlare con una macchina e gli pone delle domande, sempre mediante telescrivente, per cercare di individuarlo. La macchina risponde, ovviamente mediante telescrivente e cercando di non farsi identificare agli occhi del giudice umano. Il test termina compie al momento in cui l'interrogatore identifica l'interlocutore.

3. Gli algoritmi di *Machine Learning.*

Il Machine Learning, è una tecnica di apprendimento automatico che sta rivoluzionando il mondo con applicazioni innovative in molteplici settori, dal commercio online alla ricerca scientifica[126]. L'idea centrale si fonda sul costruire algoritmi capaci di estrarre informazioni e nozioni da un insieme di dati, consentendo ai sistemi informatici che li utilizzano di effettuare predizioni.

In sintesi, algoritmi che imparano dai dati, e che sono capaci di "scovare" informazioni nascoste nei dati stessi con velocità ed efficienza maggiore di quanto possa osare un qualsiasi essere umano. Più precisamente, la sua elaborazione prevede due fasi necessarie, la fase di *training*, dove il *software* apprende a partire da esempi e dati immagazzinati, per poi arrivare alla fase successiva dove diviene in grado di generalizzare e gestire nuovi dati e problemi nello stesso dominio applicativo.

Mediante tali fasi, si prospetta un meccanismo che permette ad una macchina intelligente di imparare e migliorare le proprie capacità e prestazioni nel tempo. Ovviamente ogni sistema di *machine learning* si fonda su algoritmi e tecniche informatiche diverse ma in ogni caso lo schema comune è quello di partire da nozioni primitive, per poi prendere una specifica decisione piuttosto che un'altra, a seconda dello scopo per cui sono realizzati. Insomma, il *Machine Learning* è un termine "ombrello" che comprende molti di questi algoritmi generici[127].

A seconda del tipo di algoritmo utilizzato per la fase di *learning*, si possono prospettare quattro differenti metodologie di apprendimento automatico: supervisionato, non supervisionato, quasi supervisionato e per rinforzo. I quattro modelli sono utilizzati in settori differenti a seconda delle finalità della macchina su cui si deve operare, garantendo così sempre le performance più elevate e il migliore efficienza per la risposta agli stimoli esterni.

L'apprendimento supervisionato (anche noto come *Supervised learning*) permette di fornire al sistema una serie di nozioni specifiche e codificate, ossia di modelli ed esempi che permettono di costruire un vero e proprio *dataset*[128]. In questo modo, quando la macchina si trova di fronte ad un problema, non dovrà fare altro che attingere alle esperienze inserite nel proprio sistema, analizzarle, e decidere quale

126 Il *Machine Learning* ha avuto un ruolo nella scoperta sperimentale del "bosone di Higgs", in cui l'impiego di queste tecniche in analisi dati ha portato ad un aumento della sensitività sperimentale che ha permesso la scoperta in anticipo e con meno dati di un elemento che ha portato al premio Nobel per la fisica a Peter Higgs e François Englert. Per maggiori informazioni rimando all'articolo completo (https://magazine.unibo.it/archivio/2018/08/01/le-nuove-frontiere-del-calcolo-nascono-dalla-fisica-delle-particelle).

127 Se si possiede una buona conoscenza della lingua inglese, allego il videocorso del professore Andrew Ng, professore della Standford University e riconosciuto esperto del settore, che spiega in modo semplice sia il funzionamento del *machine learning* in generale sia i modelli matematici applicati ai singoli algoritmi per ottenere sistemi con funzionalità specifiche. https://www.coursera.org/learn/machine-learning .

128 Un *Dataset* (traducibile in italiano anche con esperienza del sistema) è sostanzialmente un archivio, una collezione di dati che viene utilizzata in vario modo nel mondo dell'informatica. Anche i *Dataset*, possono essere costruiti secondo modelli logici e relazionali diversi, esistendo sia dataset logici e ordinati secondo matrici, sia dataset randomici che mischiano informazioni in modo causale per generare dati nuove e non prevedibili.

risposta dare sulla base di esperienze già codificate[129].

La capacità di questi sistemi sta proprio nell' effettuare ipotesi induttive, ossia ipotesi che possono ottenersi elaborando una serie di problemi specifici per ottenere una soluzione idonea ad un problema di tipo generale.

L'apprendimento non supervisionato (in inglese *Unsupervised learning*) permette che le informazioni inserite all'interno della macchina non siano codificate, cioè la macchina può attingere alle informazioni ma senza avere alcun esempio del loro uso pratico e, quindi, senza avere conoscenza dei risultati attesi a seconda della scelta effettuata[130].

Dovrà essere la macchina stessa, quindi, a catalogare ed organizzare in modo probabilistico tutte le informazioni in proprio possesso, imparandone il loro significato, il loro utilizzo e, soprattutto, il risultato a cui esse portano.

L'apprendimento senza supervisione offre una maggiore libertà di scelta alla macchina, poichè le classi non essendo note a priori, devono essere apprese automaticamente. e imparare, quindi, quali sono i risultati migliori per le differenti situazioni che si presentano.

Una perfetta sintesi tra le due tecniche di apprendimento appena illustrate, è rappresentata dalla *Semi-supervised learning* o apprendimento parzialmente supervisonato che fonda il suo *dataset* su dati misti, in cui una minima parte è già etichettata e una larghissima maggioranza è costituita da dati non etichettati, apportando al sistema un notevole vantaggio per migliorare le previsioni fatte sui dati non codificati.

L'apprendimento per rinforzo rappresenta il sistema più complesso, in quanto consente che la macchina sia dotata di sistemi e strumenti in grado di migliorare il proprio apprendimento e, soprattutto, di comprendere le caratteristiche dello spazio circostante[131].

Alla macchina vengono forniti elementi di supporto, quali ad esempio sensori, microfoni o localizzatori GPS che permettono di rilevare quanto avvenga nell'ambiente esterno ed effettuare scelte per un migliore adattamento all'area intorno a loro.

L'obiettivo perseguito da un modello di *Machine Learning* però rimane sempre lo stesso: rilevare un dato in ingresso che prende il nome di *pattern* (tradotto in italiano come modello) e di associarlo con varie tecniche a tutte le informazioni che possiede all'interno di un *dataset.* Negli ultimi anni si è sviluppata una disciplina autonoma, il *Pattern Recognition*, che presenta elevatissimi profili di incidenza con l'apprendimento automatico in quanto fornisce ottime techiche di ricognizione sia di *pattern* singoli che di sequenze di *patterns*.

Ad esempio, un approccio di ricognizione dei *pattern* prevede di classificare singoli dati secondo

129 Gli algoritmi che fanno uso di apprendimento supervisionato vengono utilizzati in molti settori, da quello medico a quello di identificazione vocale.

130 Un esempio tipico di questi algoritmi lo si ha nei motori di ricerca. Questi programmi, data una o più parole chiave, sono in grado di creare una lista di link rimandanti alle pagine che l'algoritmo di ricerca ritiene attinenti alla ricerca effettuata. La validità di questi algoritmi è legata alla utilità delle informazioni che riescono ad estrarre dai dataset, nell'esempio sopracitato è legata all'attinenza dei link con l'argomento cercato.

131 Questo tipo di apprendimento è tipico delle auto senza pilota, che grazie a un complesso sistema di sensori di supporto è in grado di percorrere strade cittadine e non, riconoscendo eventuali ostacoli, seguendo le indicazioni stradali e molto altro.

proprietà comuni, dando vita a strumenti quali *software* di riconoscimento vocale e facciale, di diagnosi medica o di traduzione di testi[132].

I sistemi di *Machine learning* poi si suddividono ancora a seconda dei rapporti che presentano tra la fase di *learning* e la fase in cui divengono operative a servire lo scopo per cui sono state progettate.

Il modo più semplice per comprendere come le macchine imparano è vedere l'apprendimento per quello che è: ogni persona nel corso della vita, impara dal mondo che lo circonda: ed estrae informazioni che poi utilizzarle nella sua vita. Per questo motivo, l'apprendimento è un processo *iterativo*, che si ripete e migliora la nostra conoscenza all'aumentare delle informazioni che raccogliamo.

Più facciamo esperienza e più impariamo, tuttavia nel mondo delle Intelligenze Artificiali si può osservare come non tutte le macchine, mantengano le capacità di imparare per tutta la loro vita, delineando così tre diverse classificazioni di questi sistemi: *batch,* incrementali e naturali.

Batch è un sistema che effettua la fase di *training* solo per una volta, su un *dataset* fisso e solitamente *off-line,* quindi dotato di informazioni relativamente limitate e non necessariamente aggiornate con il tempo.

Ciò, tuttavia non significa che la macchina non apprenda o che non sia in grado di effettuare delle classificazioni efficaci dei dati in input ma implica solo che lo fa una volta e, terminato il *training*, il sistema passando in *working mode*, non è più in grado di apprendere ulteriormente, aggiornandosi con la nuova conoscenza.

Questi sono ad oggi i sistemi più sicuri e diffusi, in quanto non permettono che la macchina possa "impazzire" a seguito di *learning* erronei o di immissione di dati inesatti o sovversivi. Un sistema di tipo *batch* trova nel suo limite, il non potersi aggiornare, il suo massimo punto di forza qualificandosi come un sistema statico ma potenzialmente sicuro.

Le altre due categorie di *Machine Learning*, prevedono accanto ad una prima fase di *training* su un *dataset* selezionato e ritagliato direttamente dai programmatori, altre fasi di "studio". Una volta passate in *working mode* quindi riescono a regredire ad una fase di *learning* secondo due modalità ben distinte: nel primo caso la macchine riuscirà a conservare un numero abbastanza ampio di informazioni, durante la sua attività prima di risottoporsi alla fase di *training*. In questo caso prima che lo studio ricominci, il *dataset* può essere snellito manualmente dalle informazioni errnoe, inutili o fuorvianti che il dispositivo può aver raccolto.

Nel secondo caso invece la macchina fara tesoro della sua esperienza, nel momento stesso in cui compie un operazione in *working mode*, apprendendo subito dall'esperienza .

È ovvio come queste due ulteriori forme di *Machine Learning* creino qualche tipo di resistenza ad entrare sul mercato in quanto potrebbero, con elevate probabilità, incappare in *bias* totalmente imprevedibili e non derivanti da errori di programmazioni ma dall'esperienza che ogni macchina vive. Uno banalissimo scherzo telefonico ad una macchina incaricata di rispondere ad un centralino, potrebbe risultare fatale per la

132 Si vedano altri approcci di ricognizione quali: il *clustering* (raggruppamento), quando si vuole raggruppare i dati che presentano caratteristiche simili oppure la regressione, cioè prevedere il valore futuro di un dato avendo noto il suo valore attuale.

sua capacità intrinseca di ragionare.

Ciò spiega anche il fatto che spinge i programmatori ad effettuare fasi di *learning* non solo su *dataset* prefissati ma anche statici, essendo quasi tutti caricati in modo *offline* sulla macchina. L'apertura alla mole di dati così eterogenea, volubile ed a volte imprecisa come quella contenuta nel Web, non è sicuramente gestibile per le tecniche di *Machine Learing* moderne.

3.1. Ambiti operativi del *Machine Learning.*

La corsa alla ricerca dello sciluppo di Intelligenze Artificiali, ha creato nel tempo diverse scuole di pensiero sulle reali capacità ed utilizzo di questi sistemi, passando dai sostenitori delle IA generali, o forti, alle cosidette IA deboli.

È Generale, quella scuola di ricerca che studia la realizzazione di una macchina capace di replicare completamente l'intelligenza umana, capace cioè di avere coscienza di se.

L'intelligenza artificiale debole, invece, si concentra sull'uso di software per studiare o risolvere specifici problemi o ragionamenti come ad esempio, nell gioco degli scacchi, Deep Blue[133]. Non realizza alcuna auto-consapevolezza e non dimostra il tutti i livelli di capacità cognitive proprio dell'essere umano, ma è esclusivamente un *problem-solver,* un risolutore di problemi concreti e, solo parzialmente, intelligente.

Alcuni sostengono che i programmi di intelligenza artificiale debole non possano essere chiamati propriamente "intelligenti", in quanto non possono realmente pensare. Rispondendo alla tesi secondo cui programmi come Deep Blue non siano realmente pensanti, Drew McDermott scrisse: "Dire che Deep Blue, giocando a scacchi, non stia effettivamente pensando è come dire che un aereo non voli perché non sbatte le ali."[134]

Altri notano invece che *Deep Blue* è meramente un potente albero di ricerca euristico, e che affermare che riesca a "pensare" agli scacchi è come affermare che gli organismi unicellulari "pensino" al processo di sintesi proteica; entrambi sono inconsapevoli di tutto, ed entrambi seguono un programma codificato al loro interno.

Nonostante le dispute, molti fra gli studiosi riconoscono l'IA debole come l'unica possibile[135], affermando che le macchine non potranno mai divenire realmente intelligenti[136]. Proprio per questo motivo

133 Si veda sopra, paragrafo 1.

134 A sostegno di questa tesi vediamo anche altri filosofi, i quali sostengono che, se l'IA debole è possibile, allora debba essere possibile anche l'IA forte. Daniel C. Dennett (filosofo e scienziato cognitivo statunitense, nato a Boston nel 1942), nel suo *"Consciousness Explained"*, ritiene che, se non c'è nessuna scintilla magica o anima, allora l'Uomo altro non è che una macchina, e si chiede perché questo Uomo-macchina debba avere una posizione privilegiata su tutte le altre macchine possibili per quanto riguardi l'intelligenza o l'avere una "mente".

135 John Rogers Searle (filosofo statunitense, nato a Denver nel 1932) sostiene nella sua argomentazione nota come la "Stanza Cinese" che gli elaboratori trasmettino dati codificati che descrivono cose. I dati codificati in quanto tali, sembrano essere senza significato se viene a mancare un riferimento incrociato alle cose cui si descrivono. Questo porta Searle a dire che non c'è alcuna comprensione e significato nell' elaboratore di informazione. Come risultato egli dichiara che anche se una macchina riesca a superare il Test di Turing non debba essere necessariamente definita intelligente in senso umano.

136 In realtà, ad oggi gli studi hanno mostrato poco interesse verso l'AGI (acronimo per Artificial General Intelligence, in italiano Intelligenza Artificiale Generale), perlopiù seguendo la tesi per cui una mente umana è troppo complicata per essere replicata

nella nostra realtà storica ogni algoritmo di Machine Learning viene sviluppato con l'unico obiettivo di risolvere i compiti concreti e specifici. I compiti possono essere dai più vari e, proprio per questo motivo non esiste un modo unico in cui le macchine imparano.

Il *machine learning* è impiegato principalmente per la risoluzione di tre diverse tipologie di problemi: classificazione, raggruppamento e regressione.

Nella classificazione, gli output sono divisi in almeno due o più classi. Il sistema di apprendimento deve produrre una strategia che consenta di assegnare gli input non ancora analizzati ad una (o più) di queste classi. Questo problema viene affrontato solitamente in maniera supervisionata: l'esempio più semplice di classificazione è costituito dal filtraggio *anti-spam*, dove gli input sono i messaggi di posta elettronica e le classi sono divise in "*spam*" e "non *spam*".

Mediante la regressione, che è anch'essa un problema supervisionato, si mira ad analizzare una serie di dati suddivisi in variabili dipendenti e in una o più variabili indipendenti, allo scopo di stimare un'eventuale relazione funzionale esistente tra le variabili dipendenti e quelle indipendenti. Si cerca, cioè, di prevedere il valore futuro di un dato avendo noto il suo valore attuale o altre informazioni utili; un esempio è rappresentato da quei *software* destinati a prevedere il tasso di risposta di una campagna di marketing, sulla base dei dati relativi ai suoi clienti.

Infine il raggruppamento, noto anche con il nome tecnico di *clustering*, consente appunto di raggruppare una serie di informazioni che presentano delle caratteristiche simili. La tecnica quindi prevede di dividere in gruppiun insieme di input ma diversamente da come avviene per la classificazione, i gruppi non sono conosciuti dal sistema, rendendolo tipicamente un compito non supervisionato. In marketing, ad esempio, il raggruppamento viene sfruttato per l'individuazione di nuovi clienti e mercati potenziali.

Ovviamente questi sono considerati i modelli più semplici e basilari di risoluzione dei problemi, sfruttabili da sistemi di Machine Learning: la ricerca sta portando alla luce tecniche sempre più innovative ed i modelli sono integrati in modo sempre più efficiente e funzionale. Ovviamente il limite alla progettazione di un' Intelligenza Artificiale Generale è ancora presente ma negli ambiti specifici in cui riescono ad operare si compiono passi da gigante.

3.2. Le reti neurali e gli algoritmi di *Deep Learning*.

Uno degli aspetti più complessi che è risultato fin dalle prime ricerche sull' Intelligenza Artificiale attiene alla creazione di un vero e propro cervello informatico, un sistema che possieda caratteristiche di apprendimento almeno pari a quelle umane.

Molti studiosi si interessarono della materia fin dai primi anni '50, ritenendola l'unica soluzione per

integralmente. In ogni caso, alcuni gruppi indipendenti di ricercatori stanno portando avanti progetti in questo campo: si possono citare, tra le organizzazioni che perseguono ricerche in materia, l'*Adaptive AI*, *Artificial General Intelligence Research Institute (AGIRI)* , *CCortex, Novamente LLC* ed il *Singularity Institute for Artificial Intelligence*.

rimediare ai limiti delle esplosioni combinatorie[137] che si generavano nell'approccio delle macchine ai problemi anche più elementari.

Concettualmente si cercava di creare un'IA che, non si fondasse su degli algoritmi rigidi ma che riuscisse ad affrontare problemi ed individuare soluzioni in modo naturale, come l'essere umano. Non si richiede di trovare sempre una risposta precisa al problema ma è come se le si chiedesse di capire il problema per individuare una soluzione che sia "good enough", cioè abbastanza giusta per risolvere il problema[138].

D'altronde è esattamente coerente allo stile di apprendimento e di ragionamento che caratterizza l'essere umano: sarebbe impossibile che una persona calcoli ogni variabile di una scelta che deve prendere, però ne prende una sulla base del fatto che sia sufficientemente ponderata e valutata.

Per realizzare un sistema funzionale e complesso come il cervello umano, si è deciso di riprodurne anche la sua composizione organica. La biologia definisce una rete neurale come ogni gruppo interconnesso di cellule nervose, chiamati neuroni, contenute nel nostro cervello e risultano la sede della nostra capacità di comprendere l'ambiente e i suoi mutamenti, e di fornire quindi risposte adattive calibrate sulle esigenze che si presentano.

Si noti poi che in informatica, una rete neurale artificiale è stata definita dal professore Robert Hecht-Nielsen come: "[…] un sistema costituito da una serie di elementi di elaborazione semplici e altamente interconnessi[139], che elaborano le informazioni mediante la loro risposta di stato dinamica agli input esterni."

In sostanza questi nodi vengono distribuiti su diversi livelli che si suddividono in tre categorie: il livello più "basso" è quello di Ingresso (*Input Layer*) il quale è progettato per ricevere le informazioni provenienti dall'esterno al fine di imparare a riconoscere ed elaborare il dato esterno.

In posizione intermedia si trova uno o più Livelli Nascosti (*Hidden Layer*) che svolge la vitale funzione di collegare il livello di ingresso con quello di uscita e aiutano la rete neurale ad apprendere ed elaborare le relazioni complesse analizzate dai dati.

Alla fine della rete, troviamo il Livello di Uscita (*Output Layer*) che mostra il risultato di quanto il programma è riuscito a imparare.

Una volta che una rete neurale viene costruita fisicamente rimane inizialmente vuota come lo può essere un hardware senza un software o, in termini ancora più pratici, come un corpo senza la sua mente.

137 Si veda *supra* paragrafo 2..

138 Molto del ragionamento umano può essere compreso come soluzioni euristiche a problemi intrattabili. Ad esempio Thagard propone alla base del naturalismo cognitivo un problema computazionale di coerenza che opportunamente formalizzato risulta essere un problema intrattabile. Il punto di vista sulla cognizione umana considerata come soluzione euristica a problemi intrattabili è ben presente nella IA sin dalle sue origini. Tale teoria è basata sull'idea del *satisficing* (Simon, 1957) ovvero sull'impossibilità di trovare delle soluzioni esatte ai problemi reali affetti da esplosione combinatoriale, e sul doversi quindi accontentare di soluzioni "imperfette" che vengono trovate con strategie euristiche.

139 Attraverso la perifrasi "una serie di elementi di elaborazione semplici e altamente interconnessi", il professor Robert Hecht-Nielsen si riferisce proprio di neuroni, chiamati in informatica anche come nodi o unità di rete.

Nessuna macchina infatti può eseguire compiti senza delle istruzioni o un apprendimento preventivo che regolino il suo comportamento e, nel caso delle reti naurali, questo apprendimento viene a concretizzarsi nel deep learning.

Questa forma di apprendimento può definirsi come un caso particolare di machine learning, dove le reti neurali, le quali devono avere almeno due livelli, sono i sistemi di calcolo sui quali essi sono implementati ed operano algoritmicamente[140].

Fissati il numero di livelli e dei nodi, l'addestramento di una rete neurale consiste nel determinare il valore dei pesi che determinano il mapping desiderato tra input e output.. Per mapping desiderato si intende la specifica collocazione dei neuroni all'inteno della rete che permette alla stessa di assolvere la funzione per cui è stata posta in essere.

Vediamo ora come questo apprendimento riesca a modellare la funzionalità e l'efficienza di una rete neurale. I dati analizzati, entrano dal livello più basso, quello di ingresso, che li riconosce e li trasferisce ai livelli ulteriori al fine di elaborarli e confrontarli.

Dopo che l'informazione ha attraversato tutti gli strati della rete neurale, il sistema restituisce i dati di output attraverso il livello di uscita ma il punto cruciale sta nel fatto che durante questo passaggio il sistema viene leggermente mutato.

Ad ogni connessione tra neuroni è associato un peso che determina l'importanza del valore di input. I pesi iniziali sono impostati casualmente ma ogni neurone, ha una funzione di attivazione che, in poche parole, gli permette di definire un output per una serie di dati in ingresso da esso analizzati.

Nel momento in cui viene elaborato il dato in uscita, inizia la parte complessa di una rete neurale: il suo apprendimento. L' apprendimento avviene infatti, solo quando c'è un qualche tipo di feedback, ossia una risposta che permette di verificare se si appreso quello che si voleva imparare[141].

In termini pratici anche noi nella vita reale ci serviamo di questi feedback per vedere se abbiamo appreso qualcosa. Ipotizzamo ad esempio, la situazione di un bambino che impara a scrivere per la prima volta. All'inizio avrà serie difficoltà a riprodurre i caratteri, quindi proverà a scrivere le lettere solo dopo aver osservato come vengono eseguite dalla maestra. Il bambino quindi cercherà di riprodurre quegli stessi movimenti osservati e continuerà così finchè non ci avrà "preso la mano".

È proprio qui che si fondano i feedback, per prenderci la mano, il bambino dovrà provare nuove

140 Alcuni specifici algoritmi di apprendimento, chiamati dal professor Schmidhuber anche *very deep learning,* vengono solitamente integrate per reti neurali che presentano almeno dieci livelli nascosti (si consideri che allo stato attuale si superano i 150 livelli nascosti.)

141 Quanto alla preferibilità, le reti neurali sono preferibili al cosiddetto approccio *knowledge-based* all'intelligenza artificiale quando si tratta di identificare, riconoscere ed isolare caratteristiche precise in fenomeni fisicamente determinabili (immagini, suoni, insiemi di dati) perché essenzialmente frammenta e riaggrega i dai in *input* nei *pattern*, poi ignora i pattern irrilevanti all'individuazione del fenomeno richiesto e successivamente integra i *pattern* rilevanti così da presentare in output la miglior descrizione possibile della caratteristica voluta in partenza, mentre l'approccio classico avrebbe voluto identificare le caratteristiche richieste tramite singoli programmi ordinari che utilizzano specifiche regole formali per considerare tutti i casi possibili, risultando così estremamente inefficiente per problemi di pattern recognition sufficientemente complessi.

tecniche modificando i suoi movimenti iniziali. A seguito del cambiamento apportato, andrà comparando la mossa eseguita con il risultato che sperava di raggiungere e, vista la differenza tra i due, cercherà di variare le sue mosse, evitando gli errori già compiuti. Maggiore è la differenza tra il risultato ottenuto e quello sperato, e più radicale dovrà essere la modifica delle tue mosse.

Le reti neurali sono programmate per apprendere con la stessa metodologia attraverso un algoritmo chiamato Backpropagation[142] che consente di confrontare il risultato ottenuto da una rete con l'output che si vuole in realtà ottenere.

Una volta valutata la differenza tra i due risultati provvede a modificare i pesi delle connessioni tra i livelli della rete partendo da quello di output ma procedendo a ritroso mutando anche i pesi dei livelli nascosti e infine quelli dei livelli di input.

La maggior parte delle reti neurali sono, poi, completamente connesse, cioè ogni neurone appartenente al livello nascosto risulta connesso con ogni neurone del livello di uscita così che il mutamento della rete possa influenzare il maggior numero di nodi del sistema.

Più connessioni, o meglio pesi, esistono tra i vari nodi, più il sistema riuscirà a modellarsi uniformemente ad ogni ciclo di attività permettendo ad ogni neurone di "capire i suoi errori".

3.3. Il *Data Mining.*

Se un lato della ricerca muove i suoi passi verso la creazione di una macchina in grado di apprendere sfruttando la tecnica e la conoscenza umana, esiste una parte dell'informatica che si preoccupa di andare oltre, verso l'individuazione di metodi in grado di estrarre nuova conoscenza da quella gia disponibile all'uomo.

Il *Data Mining* si colloca proprio in questa prospettiva ed è definito come "il processo di estrazione di conoscenza da banche dati di grandi dimensioni tramite l'applicazione di algoritmi che individuino le associazioni nascoste tra le informazioni rendendole visibili."

Il vantaggio di queste tecniche è palese, un' elaboratore ha una velocita molto più grande rispetto alla mente umana a lavorare grandi quantità di informazioni per categorizzarle e trovare i possibili legami e relazioni che le uniscono, basti pensare ad una delle scoperte più importanti dell'ultimo decennio, la scoperta del bosone di Higgs che è stata notevolmente favorita, secondo alcuni anche anticipata di qualche anno, da tecniche informatiche di ricerca ed estrazione dati.

Si prevede così un attività di estrazione inintellegibile da grandi banche dati: nessuno a parte un'

142 Sebbene i primi neuroni artificiali risalgano agli anni 40', fino a metà degli anni 80' non erano disponibili algoritmi di *training* efficaci. Nel 1986 Rumelhart, Hinton & Williams hanno introdotto l'algoritmo di *Error Backpropagation* suscitando grande attenzione nella comunità scientifica.

elaboratore, infatti, potrebbe maneggiare, in tempi accettabili, le moli sterminate e di tipologia eterogenea di dati contenuti negli archivi.

Il fine del *data mining* è quello scovare associazioni, anomalie e schemi ricorrenti (*pattern*), partendo da informazioni "criptiche", disseminate senza ordine apparente in un *database* per poi arrivare ad una conoscenza sfruttabile per vari fini[143].

L'intero processo viene chiamato KDD (acronimo di *Knowledge Discovery in Databases*) e in realtà non si esaurisce con la procedura di *data mining* vera e propria poiché la sequenza conta diversi passi. La sequenza inizia con l' identificazione dell'obiettivo che si vuole raggiungere così da permettere al sistema una selezione dei dati utili a raggiungerlo. Dopodichè avviene una pulizia dei dati e la preelaborazione che consente un' ulteriore separazione fra dati validi e quelli inutili, sulla base dei modelli che si prendono a riferimento.

Ora che il *dataset* specifico è stato impostato ed i dati sono stati opportunamente tradotti in un linguaggio comprensibile al sistema avviene la fase più importante, quella di *data mining* vera e propria. Viene ora impostatio il *software* più adeguato per il singolo caso, il quale scandaglia la banca dati in modo selettivo per fornire la risposta cercata[144].

Terminata questa fase, vanno poi interpretati i risultati osservando se l'obiettivo è stato raggiunto: nel caso di risposta negativa, il sistema procederà con la reiterazione ed eventuale modifica, dei passi precedenti fintanto che non fornirà in *output* una risposta adeguata al fine per cui è stata preposta.

L' utilità del *data mining* nell'identificare associazioni nascoste ha una portata generale poiché può essere utilizzata per scovare nuova conoscenza in ogni area dello scibile umano ad esempio nell'ambito della statistica, il *data mining* velocizza le analisi demografiche e ricerca informazioni precluse alle normali metodiche statistiche, riuscendo a fornire validi modelli predittivi.

Si nota fin da subito che l'apprendimento automatico e il *data mining*, in alcuni punti, si sovrappongono in modo significativo ma mentre l'apprendimento automatico si concentra sulla previsione basata su proprietà note apprese dai dati, il data mining si concentra sulla scoperta di proprietà prima sconosciute nei dati.

Il data mining spesso sfrutta anche i metodi dell'apprendimento automatico, ma con obiettivi differenti come d'altro canto, l'apprendimento automatico utilizza i metodi di *data mining* come tecniche di apprendimento non supervisionato o per aumentare l'accuratezza dell'apprendimento.

143 L'apprendimento automatico viene a volte unito al *data mining*, che si focalizza maggiormente sull'analisi esplorativa dei dati ed utilizza principalmente il paradigma di apprendimento chiamato "apprendimento non supervisionato".

144 Il *data mining* solitamente si compone di più sottopassaggi, anche ripetuti diverse volte, per affinare la procedura e verificare man mano i risultati raggiunti;

4. La qualità dei dati: il vero motore dell'Intelligenza Artificiale.

Va sottolineato fin da subito che le tecniche e le metodologie che consentono l'apprendimento costituiscono solo una metà, seppur fondamentale, di un' Intelligenza Artificiale.

Questi algoritmi infatti permettono ad una macchina di apprendere da determinati archivi di dati delle regole di comportamento per riportare in *output* delle risposte coerenti con le informazioni ottenute in *input.* Una macchina quindi che possieda delle capacità cognitive forti deve necessariamente essere sostenuta da una base di dati adeguata a permettergli di affrontare i problemi che le vengono posti.

Banalmente non si potrebbe mai insegnare ad una macchina a giocare a schacchi se le si "danno in pasto" le regole della dama ma va osservato anche che qualora le si forniscano le regole giuste, non ci si potrebbe mai aspettare che il sistema possa competere con giocatori esperti se non si integra la sua memoria con strategie efficienti.

Non serve una massa generica ed informe di dati ma l'intelligenza di un artificio è fortemente condizionata dalla qualità e dalla specificità delle informazioni che contiene e che può effettivamente elaborare.

In termini generali, se le regole di apprendimento e di ragionamento di un'intelligenza artificiale permettono di passare utilmente da una premessa minore a quella maggiore[145], l'esattezza e la qualità dei dati consentono che le premesse minori siano attendibili e utilizzabili in modo efficiente nell'attività cognitiva.

Le informazioni di base devono essere ritagliate da esperti del settore che riescano a creare dei *dataset* con informazioni sia specifiche per il compito che si vuole svolgere ma allo stesso tempo complete ed variegate.

È davvero complicato prevedere in anticipo quale sia il giusto equilibrio tra le informazioni che devono essere inserite in un'elaboratore e questo spiega come negli ultimi anni abbia preso piede una nuova figura professionale fortemente specializzata, il *Data Scientist.*

Tra i numerevoli compiti che può svolgere questa nuova figura, sopratutto in ambito *Big Data*, rientra sicuramente quello di evitare che all'interno di un archivio dati preposto al *training* di una macchina vi sia un forte sbilanciamento di informazioni (*bias*) verso determinate risposte.

Ciò risulta di fondamentale importanza se si osservano i risultati a cui si può arrivare: nel 2015 suscitò un incredibile clamore il caso degli algoritmi di Picture Recognition di Google, i quali, classificarono un coppia afro-americana come dei gorilla.

L'errore, o meglio il *bias*, nel modello è probabilmente dovuta ad una limitata presenza di immagini raffiguranti persone afro-americane rispetto ad altre etnie o specie animali, nei dati che il team di ricerca di Google selezionò per addestrare il suo modello.

145 Prendendo a tal proposito le tecniche di ragionamento Aristoteliche richiamate nel paragrafo 2.

Va poi osservato che il danno causato ad una macchina da dati inesatti o non coerenti è duplice: nello schema tradizionale di funzionamento *input-output* è ovvio che la qualità dei dati che la macchina può elaborare determina direttamente la qualità delle risposte che può fornire all'utente, ma l'evoluzione informatica ha integrato in questo schema tradizionale una fase di apprendimento, tale che la risposta fornita in *output* diviene parte della sua conoscenza.

Lo schema quindi muta verso una logica di *input-outpu-input* e, per effetto di questa reazione, l'errore arriva anche a compromettere l'intera capacità di "ragionare" della macchina, allontanandola dallo scopo per cui è stato progettato.

In ultima analisi, a prescindere dalla correttezza degli algoritmi, "la mancanza di qualità dei dati nella costruzione di una Intelligenza Aftificiale, trasforma un errore *occasionale,* in errore *sistematico*, o *algoritmico*, in un *bias permanente*, da cui potrebbe non essere semplice tornare indietro."[146]

La terza primavera delle IA in definitiva è stata possibile non solo grazie all'evoluzione tecnologica che ha portato alla luce elaboratori con capacità di calcolo sempre più evoluti ma anche grazie ad un immensa espansione di dati che si sono generati sul web che ha consentito la creazione di archivi mastodontici.

Ma da dove arrivano tutti questi dati? Tale domanda tuttavia, non ammette una risposta "facile" poiché l'esposione dei dati è una conseguenza di diversi fattori ed è determinata da numerosissime cause.

Si può dire in breve che ogni accesso su internet e, nello specifico, in ogni sito lascia delle tracce del nostro passaggio che possono essere arricchite da ulteriori informazioni che decidiamo (in realtà non è sempre una scelta "voluta") di lasciare per vari scopi.

Vediamo di analizzare i principali canali di approvigionamento di queste informazioni senza tuttavia nessuna pretesa di completezza data l'estrema complessità del settore.

4.1. Il *Web* e l' *Internet of Persons*.

Nell'ultimo ventennio stiamo assistendo ad un progressivo spostamento della nostra identità nel mondo digitale, dalla nascità di Internet ad oggi infatti i cambiamenti sono stati radicali.

Alla fine degli anni '80 dello scorso secolo, Internet nasce a scopi militari e scientifici al fine di permettere uno scambio di informazioni veloce ed efficiente ma rimane sconosciuto ai "non addetti ai lavori" per circa un decennio[147]. Lo sviluppo della rete anche in ambito civile è stato possibile solo con

146 D'ACQUISTO, Giuseppe, et al. *Intelligenza artificiale, protezione dei dati personali e regolazione*. G Giappichelli Editore, 2018. Specificatamente il saggio relativo alla "Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati."

147 A dire il vero, in Italia, già prima del 1986, esisteva una sorta di accesso alla rete internet: delle reti locali sfruttate da pochi appassionati pionieri, uno degli esempi più noti è il *Videotel*, un monitor con tastiera incorporata che si collegava alla rete

l'ingresso nel mercato dei primi modelli di computer fissi sufficientemente prestanti ed economici, verso la metà degli anni '90 che sfruttavano i servizi di Internet mediante il cavo telefonico.

In pochissimo tempo però la ricerca sta compiendo una vera e propria rivoluzione sia con riferimento alle capacità e prezzi degli elaboratori che con riguardo alla velocità di connessione[148] che non sembra non volersi arrestare anno dopo anno.

Ad oggi, l' accesso ai servizi di connessione senza limiti di utilizzo a prezzi ridotti e apparecchiature sempre più pratiche e portatili, primi tra tutti gli *smartphones* o i *tablets*[149]*,* hanno consentito una capillarità del fenomeno che può essere compresa solo numericamente: dai 2 milioni di utenti nel 1997, 5 milioni nel 1999, 12 milioni nel 2002, 17 milioni nel 2007 fino ad arrivare, nel 2017 agli utenti, stimati in un numero che va dai 30 a 35 milioni[150].

L'aumento delle utenze ha conseguentemente incrementato il numero dei servizi che possono essere scambiati *online,* dall' e-commerce su piattaforme immense quali Amazon, allo streaming in tempo reale di Netflix, le piattaforme di *gaming* supportate dalla Blizzard oppure ancore le *App social* come Facebook ma questi sono solo piccoli esempi di quello che si può trovare in rete.

Gli utenti possono decidere di navigare in rete liberamente, senza costi eccessivi e con possibilità esplorative infinite avendo accesso ad una quantità di siti, servizi e contenuti inimmagindbile.

Per accedere a questi servizi, però, viene sempre richiesta l'attivazione di *account,* talvolta gratuiti, dove vanno inseriti alcuni nostri dati personali di vario genere, in base alle finalità specifiche dell'attività: è ovvio che, qualora richiediamo un servizio, come avviene nel mondo “reale”, noi cediamo delle nostre informazioni al fine di usufruire dello stesso.

Queste informazioni vengono poi memorizzate nel sistema e successivamente elaborate e/o trasferite, ad esempio nel caso di una consegna a domicilio di un bene, è necessario confidare l'indirizzo al venditore, il quale deve elaborare la richiesta e trasferire i dati abitativi dell'utente al trasportatore che effettuerà praticamente la consegna.

Questo è uno dei modi in cui i nostri dati vengono immessi nel sistema e si ritrovano a fluttuare nella rete ma non è assolutamente l'unico. La raccolta dei dati vede un mercato spietato: secondo uno studio commissionato da *DG Connect,* l'organo che si occupa di monitorare il mercato europeo delle comunicazioni, nel 2016 il comparto dati nell'UE ha prodotto quasi 60 miliardi di euro, e nel giro di un triennio potrebbe raggiungere quota 100 miliardi[151].

telefonica attraverso un modem a una velocità di 1.220 baud.

148 In merito alla telefonia mobile, si è passati dai primi telefoni dotati di connessione Wap (nel 2000), fino ai 4G/LTE di oggi. Una linea fissa consente all'utente una connessione che può arrivare ai 100 *MBPS (Mega Bytes Per Second)* a dispetto dei primi *Videotel* dotati di una velocità di connsessione pari a 1200 *BAUD* (1,2 *Mega Bytes Per Second*).

149 Negli ultimi 15 anni, infatti, lo sviluppo tecnologico di Internet passa soprattutto dal mobile che hanno addirittura portato al sorpasso di smartphone e tablet sui computer per quantità di ricerche su *Google*.

150 Una cifra che tiene conto anche dell'espansione del mondo mobile. Le stime sono riprese dal sito di Telecom Italia di cui allego il link https://www.telecomitalia.com/tit/it/innovazione/rete/internet-day.html .

151 Questo software permette di calcolare il valore dei tuoi dati personali. http://ig-legacy.ft.com/content/f0b6edc0-d342-11e2-

Ogni dato risulta utile in questo mercato, quelli relativi alle nostre consultazioni dei siti internet, agli acquisti che effettuiamo, ai viaggi che prenotiamo, alle nostre proprietà, ai processi giudiziari cui siamo stati eventualmente sottoposti, al nostro stato civile, ai figli, alla fascia di reddito, ad eventuali malattie, alle preferenze politiche, religiose, sessuali e tanto altro.

Le modalità con cui vengono generati questi dati, quindi, sono svariate ma si possono raggruppare in tre grandi aree: i dati della tipologia *"people-to-people",* quelli che si generano a seguito di attività o conversazioni dirette tra gli utenti sulle reti social come *Instagram, Messenger, Facebook, etc.,* i dati *"people-to-machine"*, che invece attiene ai dati che si generano nell'interazione tra l'uomo e l'elaboratore, per riprendere l'esempio di prima, la creazioni di un *account* di qualsiasi tipo ed infine i dati *"machine-to-machine"* che vengono creati indipendentemente dall'interventi attivo di un essere umano.e comunicano in quella che viene denominata *Internet of Things.*

Le prime due categorie di dati sono le più semplici da comprendere perchè è l'intervento umano che origina queste informazioni. È il modo convenzionale in cui abbiamo vissuto il Web fino a pochi anni fa: ad ogni nostra azione corrisponde una traccia e quindi un dato che ci riguarda ed ha portato fino ad oggi a somme di dati personali che superano l'ordine di qualche Zettabytes[152].

Viene appunto definito come Internet Of Persons, poiché il fruitore ultimo dei servizio Internet è solo e direttamente l'essere umano, sia che voglia caricare del materiale in rete, sia che intenda scaricarlo o semplicemente visualizzarlo.

La terza categoria, suscita più interesse e va analizzata separatamente in quanto apre la strada ad un modo diverso di vivere la rete: viene definito Internet delle Cose o Web 2.0 e consiste sostanzialmente nell'accesso delle macchine alla rete Internet.

Senza un intervento diretto dell'essere umano, i dispositivi riescono a collegarsi nella rete, caricando e/o scaricando un'immensa quantità di nuovi dati che secondo alcune stiume si prevede che entro il 2020 porterà ad una mole pari a 44 Zettabytes.

Il tema verrà analizzato approfonditamente nel paragrafo 4.2..

4.1.1. I *Cookies.*

Letteralmente *Cookie* può essere tradotto in Italiano come "biscotto" ma nell'ambito dell0 informatica viene convenzionalmente tradotto come "gettone".

Per capire il funzionamento di questi strumenti, va ripreso il concetto fondamentale, specificato nel

b3ff-00144feab7de#axzz2W4xIIvg9&from=Il+business+dei+dati+person%3A+ecco+il+nostro+prezzo+per+il+marketing .

152 Lo zettabyte è un'unità di misura dell'informazione o della quantità di dati dell'ordine di 1'000'000'000'000'000'000'000 byte = 1021 byte = 1 triliardo di byte.

paragrafo precedente: per accedere alla maggior parte dei servizi in rete è richiesta autenticazione, cioè la capacità di identificarsi da parte di un determinato utente da tutti gli altri *users* che sono registrati nel servizio*,* si tratti di e-banking, e-commerce o social network.

Proprio la doverosità di "presentarci" dinnanzi ad un sito che offre un servizio online tramite la sottomissione di credenziali di accesso, nella forma di nome utente e password, crea la necessità di proteggere tali dati.

Ciò è fondamentale per garantire la sicurezza del proprio account, perché un attaccante in grado di carpire la nostra password, è effettivamente in grado di impersonarci presso di esso, acquisendo i nostri stessi privilegi.

Tuttavia, proteggere appropriatamente la propria password è necessario ma non sufficiente: ciò deriva direttamente dalla morfologia del protocollo *HTTPS*, su cui tutto il web è costruito, caratterizzata dall'assenza di stato.

La sua natura *State-less* comporta che due richieste *HTTPS* inviate da uno stesso servizio risultano sempre scollegate tra loro, come se fossero due richieste indipendenti. Di conseguenza, dopo aver verificato la nostra password, i servizi online si "dimenticano" di noi e le richieste successive non riconoscono più le nostre credenziali d'accesso precedentemente inserite.

Molti fornitori di servizi in rete hanno deciso di migliorare l'accesso e l'esperienza dei suoi utenti risolvendo il problema del mancato riconoscimento attraverso l' implementazione di una strategia basata proprio sull'utilizzo di *cookies*.

Un *cookie* non è altro che un piccolo frammento di informazione che può venire salvato da un sito all'interno del nostro *browser*[153]. Il *browser provider* fornirà poi automaticamente il *cookie* ad ogni richiesta *HTTPS* dove risulta necessaria l'identificazione dell'utente.

Se un *cookie* contiene abbastanza informazione per identificare un utente in maniera univoca, ogni richiesta dallo stesso *HTTPS* viene così auto-identificata dal sistema e non è necessario che l'utente li reinserisca. Quasi ogni sito oggi fa uso dei *cookies* e richiede ai suoi utenti di accettarli al fine di poter visualizzare i contenuti che lo stesso contiene.

Ovviamente questa tecnologia può essere utilizzata in innumerevoli modi e, il più delle volte, è finalizzata a migliorare la qualità e l'esperienza di chi usufruisce del servizio raccogliendo informazioni sugli utenti che visitano il sito.

Abbiamo quindi *cookies* che permettono ai siti web di effettuare statistiche sulle visite o per conoscere il tempo speso dagli utenti sulla pagina, quelli che ricordano le impostazioni sulla lingua o le

153 Il browser può sembrare un concetto complicato leggendo la sua definizione: un software pensato in maniera specifica per poter recuperare, caricare e navigare determinate risorse caricate su siti Internet che vengono identificati attraverso un apposito URL. In termini generali è quell' applicazione che ci permette di navigare in Internet, alcuni esempi sono S*afari, Mozilla Firefox, Opera, Google Chrome, Internet Explorer etc...*

modifiche all'interfaccia di un'applicazione web o ancora i *cookies* pubblicitari, per fornire annunci o messaggi sponsorizzati che rispecchino le preferenze dell'utente.

Questa informazione però risulta piuttosto delicata quando contiene i nostri dati identificativi su specifici siti e ci permette di usufruire di servizi che spesso sono a pagamento. Per fare un esempio, se il tuo sito bancario utilizzasse i *cookies* per salvare (sempre sul tuo *browser* ovviamente, non nel loro) le credenziali di accesso al servizio *e-banking*, il furto di quel frammento di informazioni permetterà l'accesso ai tuoi conti bancari.

Se gli attaccanti di ieri per potrer "rubare" la nostra identità su Internet dovevano ricercare le password con metodi complicatissimi, oggi possono attaccare direttamente quei frammenti di dati salvati nei *browsers* che consentono l'auto-identificazione presso il servizio che li ha registrati.

Solo per completezza va anche osservato che spesso alcuni siti malevoli, spingono gli elaboratori degli utenti a scaricare delle informazioni sotto forma di *cookies* che tuttavia hanno lo scopo di monitorare tutte le nostre attività sul *browser*, anche esterne al sito che le ha salvate, al fine di carpire più informazioni possibili sulla nostra identità informatica.

4.2. L' *Internet Of Things*.

La perifrasi, Internet degli oggetti, esiste da poco più di un decennio, e si riferisce sostanzialmente ad un' evoluzione nell'uso di Internet: gli oggetti evolvono le loro capacità grazie alla possibilità di comunicare, attraverso la rete dati che possiede e di usufruire di informazioni esterne, provenienti da altri dispositivi.

Cose, oggetti, strumenti che acquisiscono una sorta di intelligenza, o meglio di furbizia secondo una traduzione più precisa del termine "*smart*", sono cioè dotati della capacità di rilevare informazioni e di comunicarle assumendo un ruolo attivo grazie al fatto di essere *online* e di inviare e ricevere dati sulla rete, al fine di svolgere poi azioni conseguenti. Attraverso queste tecnologie si permette di unire mondo reale e virtuale, giusto per fare qualche esempio, è uno strumento IoT, il frigorifero che ricompra i prodotti quando "si accorge" che sono finiti e lo è una casa che accende i riscaldamenti appena "ti localizza" uscire dall'ufficio.

In questo modo viene data un' "identità elettronica" a tutti gli strumenti IoT connessi in Internet così da permettere che certi dati arrivano da uno specifico strumento e solo da quello, cosa fondamentale in una società dove i dispositivi sono quasi totalmente *standardizzati:* ciò avviene attraverso, ad esempio, *RFID*[154] (Identificazione a radio frequenza) ed altre tecnologie (come il più noto il *QR code*).

154 Per maggiori informazioni su questa tecnologia allego un sito molto dettagliato: https://www.internet4things.it/iot-library/rfid-cosa-e-come-funziona-esempi-applicativi/ .

La tecnologia dell' IoT è figlia della sensoristica (definita nel settore anche come l'era pre-Internet of Things) che è la disciplina che studia i dispositivi in grado di effettuare *data collection* in modo preciso e mirato in funzione di specifici ambiti applicativi: rientrano in tale categoria, apparecchiature dedicate a rilevare dati legati alla temperatura di ambienti, alla viabilità, alla qualità dell'aria e così via.

In questa fase i sensori riescono solo a rilevare informazioni e a trasformarle in dati digitali, manca, in questa fase la connessione in rete. Si tratta di strumenti che in forme e modalità diverse sono interrogati "manualmente" e con una capacità comunicativa dei dati collezionati limitata all'utente che li richiede

Il passaggio dalla sensoristica all'Internet delle Cose è segnato appunto dalla connessione sulla rete: il sensore rileva i dati e successivamente li comunica all'utente, ad altri eventuali dispositivi interconnessi e infine li conserva in rete anche senza un'espressa richiesta umana di eseguire tali operazioni[155].

La capacità di un dispositivo di raccogliere dati che a loro volta possono essere rivenduti, risulta abbastanza allettante per il venditore che potrebbe guadagnare due volte dalla vendita di un siffatto dispositivo: una al momento della vendita fisica dell'apparecchio e la seconda al momento della vendita dei dati che l'utente ha generato nel corso dell'utilizzo.

Ecco come può spiegarsi l'avvento sul *mercato* di tutti i dispositivi *Smart,* cioè tutti quei dispositivi connessi alla rete di "nuova generazione" che oltre ad aprire le porte al cosiddetto Web 2.0, cioè quella parte di rete fruibile anche da dispositivi diversi dai computer tradizionali, porta anche ad una raccolta di dati e tracce sempre più invasivo.

Ogni oggetto destinato ad una funzione specifica può raccogliere dati e di conseguenza può essere trasformato in uno *Smart Product:* si pensi a quanti prodotti oggi contengano tale suffisso*,* non solo orologi o semafori ma anche intere città[156] possono essere "intelligenti", la categoria è talmente vasta che le maggiori società di ricerca, come *Accenture*, sostengono che si arriverà a oltre 25 miliardi di apparati Iot entro il 2020.

Conseguentemente tanto più cresce la diffusione di apparati e sensori "intelligenti" ancora di più cresce la mole di dati che dovranno essere gestiti ed aumenta il numero di applicazioni che dovranno essere sviluppate per elaborarli. Questo processo è possibile grazie a connessioni in rete che consentono le trasmissioni dei dati su stazioni di *cloud*[157].

La tecnologia del *cloud computing* è fondamentale in questo ambito, poiché offre una considerevole velocità di calcolo e i server nel *cloud* possono ricevere, archiviare e processare in tempo reale l'enorme quantità di dati che arriva dagli oggetti *smart*.

Infine, i servizi *cloud,* o direttamente i dispositivi stessi, possono tra l'altro collegarsi a software di analisi dei dati (come *Google Universal Analytics*) trasmettendo dati ed informazioni dalla vita reale

155 Spesso in queste circostanze il consenso è chiesto *una tantum* e successivamente la macchina continuerà a raccogliere i dati per tutta la durata del suo utilizzo da parte dell'utente.

156 Ad esempio, in Svizzera, già esistono dei semafori intelligenti, che diventano verdi quando si accorgono che una macchina è vicina al semaforo, e se dall'altro lato non sta passando nessun' altra macchina.

157 Il *cloud computing* è "la distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e molto altro, tramite Internet ("il *cloud*"). Le società che offrono questi servizi di calcolo sono dette provider di servizi cloud e in genere addebitano un costo per i servizi di cloud computing in base all'utilizzo." per maggiori informazioni visita il sito: https://www.digital4trade.it/tech-lab/cloud-computing-cose-e-quali-sono-i-benefici/ .

direttamente ai software di analisi, aprendo la strada ai Big Data.

Ecco come la massa di dati statici che viene accumulata all'interno di questi archivi digitali viene elaborata da *software* per ricavare informazioni nuove ed accurate a fini statistici, di *marketing*, di miglioramento delle prestazioni dei dispositivi, al *profiling* dei gusti personali degli user e così via.

4.3. Prospettive future e criticità.

L'internet delle cose, trova sempre più consenso e rappresenta sempre più una occasione di sviluppo. Aumentano i dispositivi connessi, e c'è una forte fiducia in Italia[158] verso le tecnologie IoT più consolidate ma si avvisa una certa resistenza a provare l' Internet delle cose più innovativo.

Gli ambiti applicativi dell'Internet delle cose si possono suddividere in 3 gradi di maturità: applicazioni consolidate, applicazioni sperimentali e applicazioni embrionali. In Italia le applicazioni consolidate coincidono con le più semplici e di immediata realizzazione[159], le applicazioni attualmente in fase sperimentale sono quelle che più si avvicinano al paradigma dell'Internet of Things[160] e le embrionali si concretizzano nei progetti futuri.

Tra gli ambiti della tecnologia IoT che stenta a decollare a causa di una scarsa collaborazione tra gli attori pubblici e privati si rritrovano le tecnologie nell'ambito eHealth**,** cioè l'IoT per salute e medicina. Attraverso questi dispositivi, si effettua il telemonitoraggio dei pazienti, il quale potrebbe ridurre drasticamente i costi ospedalieri ed allungare la vita delle persone prevenendo e curando le malattie sul nascere. È, d'altro canto, solo una questione di tempo per vedere questi dispositivi sempre più presenti in questo scenario ed in tanti altri.

Come tutte le cose belle, anche l'IoT presenta delle criticità e degli aspetti negativi. Gli oggetti smart sono riconosciuti univocamente dalla Rete attraverso un ID e hanno una loro identità digitale. Se immagini questi oggetti come vivi e in Rete, non ti stupisce che soffrano di fragilità sul fronte della privacy e su quello della sicurezza.

Sopratutto la sicurezza è un problema serio: ogni dispositivo connesso in rete risulta un valido punto di accesso per poter entrare nella disponibilità dei dati che lo stesso conserva. Qualcuno potrebbe entrare nei tuoi oggetti e controllarli.

Forse non è grave che un hacker si introduca nel tuo frigorifero, ma pensa agli effetti potenzialmente disastrosi, se controllasse la tua automobile o i semafori stradali oppure se conoscesse gli orari in cui casa non è sorvegliata e trovasse altresì il modo di controllare da remoto il sistema di allarme disattivandolo.

158 Almaviva lancia la prima piattaforma italiana per l'Internet delle cose. La nuova piattaforma tutta italiana si chiama Giotto, e riesce a connettere diversi dispositivi e farli interagire tra loro e con le persone, i servizi e le applicazioni.

159 Si possono prendere ad esempio, la videosorveglianza e la sicurezza nelle *smart home***,** finalizzata al controllo e all'antintrusione, la tracciabilità di beni, il monitoraggio della viabilità cittadino in ambito *smart city*.

160 In questa categoria, troviamo i contatori intelligenti, i cd. *smart meetering* per misurare i consumi, le soluzioni domotiche, la sicurezza delle persone, l'analisi dei parametri di guida.

La ragione della lentezza nello sviluppo di queste apparecchiature è proprio legato ai limiti di privacy e sicurezza. I produttori di oggetti smart e il legislatore sono impegnati proprio su queste tematiche, per garantire lo sviluppo dell'Internet delle cose, attraverso sistemi più sicuri, e una normativa appropriata.

In ogni caso, gli aspetti negativi non riguardano soltanto questioni tecniche o normative. Gli oggetti, sempre più smart, compiono azioni in piena autonomia e unitamente alla robotica sono riusciti in molti campi a sostituirsi all'uomo.

L'aspetto sociale è decisamente il punto cruciale che pone dei freni all'evoluzione informatica: il tema è affrontato da moltissimi autori e studiosi tra cui Massimo Gaggi che nel 2018 ha pubblicato il suo libro "*Homo Premium – come la tecnologia ci divide"*.

*S*tando a quanto scritto nel nuovo libro, siamo di fronte ad un processo evolutivo sociale che sembra portare verso un progresso discutibile: da *Homo sapiens* a *Homo premium*.

In particolare viene sottolineato come *"*Dopo i robot che sostituiscono i lavoratori manuali, ora l'intelligenza artificiale si diffonde nell'area di quelli intellettuali e dei servizi: analisti, medici, commercialisti, agenti di viaggio, giornalisti, avvocati. Verso una nuova stagione di diseguaglianze: sacche di povertà da disoccupazione o lavori precari sottopagati da un lato, una élite benestante che usa la tecnologia per vivere meglio e più a lungo dall'altro."

Eccolo, quest'ultimo sarebbe l'*Homo premium*, che va avanti consapevole della sua maggiore capacità socio-economica, che gli consente di mangiare meglio, di fare un uso più frequente della tecnologia, fino a poter richiedere analisi genetiche per impedire l'insorgenza di malattie o ancora per programmare un erede senza "errori".

Per quanto siano affascinanti questi scenari distopici dove la società viene costretta a mutare adottando modalli totalmente nuovi ed, a tratti, spaventosi non potranno essere approfonditi in questo elaborato.

Nella parte finale cercherò invece di osservare come il GDPR si pone dinnanzi all'intelligenza delle macchine e sopratutto come questi sistemi, agendo fuori dal diretto controllo umano ed essendo dotati di una grande mole di dati siano messi in sicurezza prima di poter conoscere liberamente nel Web e nel mondo reale.

CAPITOLO III
I rapporti tra il GDPR e le IA: la sicurezza come cardine del sistema.

1. I soggetti ancillari del titolare: Il Responsabile.

La cornice delineata del GDPR ed analizzata nel primo capitolo, mette in luce i tre soggetti fondamentali del sistema, l'interessato, il titolare e l'Autorità di controllo, tutte concatenate da un gioco di poteri e contropoteri volti a garantire un valido equilibrio del sistema, tra libera circolazione dei dati e tutela di diritti e libertà delle persone fisiche.

Per porre rimedio, in particolare, ai trattamenti che presentano elevati rischi per le libertà fondamentali delle persone fisiche, primi tra tutti le tecnologie intelligenti, analizzate nel secondo capitolo, è preposto il titolare del trattamento.

Questo soggetto è sicuramente il perno del sistema, basti pensare che sarà egli stesso a stabilire, sotto la sua responsabilità e a seguito di una valutazione, se il suo trattamento presenta rischi elevati ma può essere aiutato, a vario titolo, nella sua attività di trattamento da altri soggetti, qualificati nel GDPR.

Uno dei soggetti più importanti che può affiancare il titolare, arrivando a rivestire un ruolo attivo nel corso di un'attività di trattamento, è il Responsabile, che viene definito nell'articolo 4, paragrafo 1, numero 8, come “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”.

Oltre alla sommaria definizione contenuta nell'articolo 4, il suo ruolo e le sue funzioni sono dettagliatamente specificate nell'articolo 28, il quale lo definisce un soggetto terzo rispetto all'attività di raccolta dei dati ma che viene individuato dal titolare, tra soggetti che che presentino adeguati requisiti e competenze tencico-organizzative, per effettuare un'attività di trattamento per suo conto e suo nome.

Il rapporto tra Titolare e Responsabile devono necessariamente essere formalizzati all'interno di un “contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri” dove vengono sottolineati i vincoli che ne derivano tra cui la durata, la natura e le finalità del trattamento, il tipo di dati trattati, la possibilità per il Responsabile di nominare altri sub-responsabili[161] e tutti gli aspetti rilevanti in materia.

In particolare risultano di notevole importanza gli obblighi che incombono sul responsabile, il quale deve applicare al trattamento tutte le misure di sicurezza adeguate a norma dell'articolo 32, assistere il titolare in tutte le misure tecniche e organizzative al fine di permettergli di soddisfare le richieste degli

161 In realtà tale esigenza può anche ricorrere solo successivamente e per tale motivo il paragrafo 2 dello stesso articolo prevede espressamente la possibilità di autorizzare tale nomina in un momento successivo e con atto scritto separato

interessati concernenti l'esercizio dei loro diritti, deve inoltre informare il Titolare qualora ritenga che le istruzioni che ha ricevuto possano violare il GDPR, il diritto dell'Unione o quello nazionale ed infine è anche tenuto a redigere i registri dei trattamenti che ha effettuato per conto del titolare a norma dell'articolo 30, paragrafo 2.

Si nota così che il Responsabile non è una figura cui sono preposti compiti ulteriori rispetto a quelli del titolare; sono semplicemente figura fortemente specializzata che agevolano l'attività di un Titolare, snellendone i doveri e garantendo la conformità del suo operato al Regolamento Europeo e alle norme nazionali.

1.1. *Segue*: La catena di titolari.

Un sistema complesso di trattamenti come quello che si configura attualmente non poteva non prendere in considerazione la figura dei contitolari, cioè due o più soggetti che decidono di porre in essere tra loro un trattamento configurandone congiuntamente le finalità, i mezzi e le modalità dello stesso.

Tale figura viene introdotta dal GDPR nell'articolo 26 e mira a racchiudere in un unico trattamento, tutte le attività di due o più contitolari che siano strettamente legate da finalità convergenti, evitando così un'eccessiva frammentazione dei trattamenti.

Come sottolinea autorevole dottrina[162], tale configurazione della contitolarita non si adatterebbe perfettamente alle concrete modalità di trattamento che potrebbero essere effettuare da macchine intelligenti: queste modalità infatti si caratterizzano per la circostanza che ogni titolare compie individualmente una serie di trattamenti e mettendo insieme tutte queste operazioni si consente di raggiungere una finalità nuova diversa e condivisa tra tutti i titolari.

La soluzione prospettata in dottrina è quella di interpretare in modo estensivo l'articolo 26 così da ricomprendere nelle fattispecie di “unico trattamento” quelle ipotesi in cui trattamenti individuali, dotati di finalità specifiche, siano parte di una catena, tale che i risultati di ogni specifica attività verranno poi correlati al fine di raggiungere un obiettivo comune.

In definitiva si arriverebbe ad avere un rapporto di contitolarità ponendo l'accento non sull' unicità dei trattamentamenti ma sulla convergenza dei fini.

Fuori dai problemi interpretativi che possono scaturire dalla lettura del primo periodo dell'articolo 26, viene subito specificati che il rapporto tra contitolari deve confluire in un accordo che sottolinei in modo trasparente le rispettive responsabilità.

162 F.PIZZETTI, G- D'ACQUISIO, *Intelligenza Artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore – Torino, 2015

A chiusura, i paragrafi 2 e 3 si pongono a garanzia dell'interessato in quanto oltre a prevdere che questi siano resi edotti di eventuali accordi di contitolarita, gli viene riconosciuta, altresì, la facoltà di rivolgersi indifferentemente e singolarmente a uno dei contitolari per "esercitare i propri diritti ai sensi del presente regolamento".

Si può comprendere efficacemente la ragione che porta a valorizzare la figura di una catena di trattamenti se si considera che in un futuro, forse non molto distante, potrebbero divenire anelli di questa catena, e quindi contitolari, dei dispositivi Intelligenti. Viste le capacità elaborative, la possibilità di operare in totale indipendenza e la capacità identificativa[163] di cui sono dotate queste macchine, questo compito non risulterebbe troppo difficile.

La situazione però si potrebbe complicare dal momento in cui questa macchina, essendo parte del sistema di trattamenti, sarebbe responsabile congiuntamente agli altri contitolari, delle violazioni del GDPR derivanti dalle loro azioni.

Ovviamente questo scenario mira solo ad offrire uno spunto di riflessione teorico, allo stato attuale, non vi sono informazioni che potrebbero supportare tale tesi.

1.2. Il Responsabile per la Protezione dei Dati.

La terza figura che può legarsi all'attività di un titolare, è il *Data Protection Officer* (letteralmente il "Responsabile della protezione dei dati" ma in seguito verrà chiamato con l'acronimo inglese *DPO*, per evitare confusioni con il responsabile del trattamento). Pur aggiungendosi alla figura del titolare non agisce nel suo esclusivo interesse ed è incaricato di specifici doveri e compiti.

Vedremo tra poco che il *DPO* è una figura altamente specializzata che agisce in totale indipendenza, secondo l'articolo 38: "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti", e quindi a differenza del Responsabile del trattamento non è legato da alcun tipo di rapporto con il titolare.

Il suo fine, infatti, è quello di monitorare le attività di trattamento in cui è chiamato ad operare affinchè possa valutare la conformità dell'attività con il GDPR: sia coadiuvando il titolare a progettare le attività o a ridurre i rischi ma anche segnalando alle Autorità di controllo le violazioni che ritrovi *ex post*.

Al *DPO* viene dedicata la Sezione 4, del IV Capo del GDPR che definisce cristallinamente sia i casi in cui tale soggetto deve obbligatoriamente intervenire in un'attività di trattamento che le sue funzioni specifiche.

163 Rispetto alla possibilità di un dispositivo di essere identificato univocamente all'interno della rete rimando alla lettura del paragrafo 4.2 del secondo capitolo dove si parla di *RFID*.

Partendo dal fatto che ogni titolare ha la facoltà di nominare un *DPO*, anzi gli organismi Europei del settore[164], incentivano e consigliano tale scelta in quanto tale figura riesce a dare una grande effettività a tutto il sistema, configurandosi quale controllo esterno e specializzato a tutte le attività di trattamento in cui opera, va analizzato tuttavia che l'articolo 37 del GDRP stabilisce i casi in cui la designazione è obbligatoria.

In tre casi specifici la figura del *DPO* deve necessariamente essere integrata nell'organizzazione di un trattamento ed in particolare, nel caso in cui il "trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico"[165] o qualora "le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala" oppure, per ultimo, se "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10*."*

Va chiarito fin da subito il forte legame esistente tra *DPO* e le tecnologie esaminate nel secondo capitolo, tra cui spiccano *Big Data, Machine Learning e IoT* poiché questi strumenti integrano sempre la fattispecie di "monitoraggio regolare e sistematico degli interessati su larga scala" oppure il "trattamento su larga scala di categorie particolari di dati".

Sono a supporto di questa prospettiva anche le richiamate Linee Guida del WP29 nel definire il concetto di "larga scala", già sancito nel Considerando 91 del Regolamento come quel trttamento "che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti."

Risulta così necessario ricercare la corretta interpretazione del ruolo e dei compiti del DPO in quanto risulta una delle figure più direttamente coinvolte da trattamenti che vengono effettuati attraverso le più recenti tecnologie ed ha un ruolo chiave nel processo d'integrazione tra informatica e aziende/organizzazioni.

Purtroppo l'ampiezza di tale figura e la ristrettezza dei tempi non mi permettono un'elaborazione completa del *DPO*[166] ma tratterò solo dei profili più rilevanti che intercorrono tra questi e l'utilizzo delle

164 A tal proposito risulta doveroso richiamare le Linee Guida elaborate dal WP29 sulla figura del *Data Protector Officer*, il quale statuisce che "consente una modernizzazione del modello basato sulla responsabilità yale che consente un'adattamento dell'attività di trattamento al Regolamento, divenendo il cuore dell'intera disciplina per le molte organizzazioni che se ne avvalgono.

165 La norma specifica poi che sono escluse: " le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali."

166 Ad esempio non verranno analizzate dettagliatamente le ipotesi in cui un unico *DPO* può essere nominato al fine di monitorare e assistere l'attività di trattamento di più organismi pubblici o per un gruppo di imprese o ancora per associazioni e organismi rappresentanti categorie di titolari. Basti sapere che un unico *DPO* può far capo ad una serie di trattamenti ed in particolare per trattamenti connessi che presentando finalità condivise a patto che ogni titolare, stipuli separatamente, sulla base delle sue attività e responsabilità, un contratto di servizio con lo stesso *DPO*.

macchine intelligenti.

1.2.1. Il ruolo e le funzioni del Responsabile per la Protezione dei Dati.

Il *DPO* può essere sia una persona fisica che una persona giuridica (anche se poi all'interno di tale persona giuridica deve comunque essere individuata una persona fisica preposta a svolgere in concreto le funzioni di *DPO* nello specifico contratto) ed è legata ad uno specifico titolare o da un rapporto diretto di lavoro o mediante un contratto di servizio, in ogni caso rimane un soggetto che agisce in totale indipendenza e non deve pertanto trovarsi in situazioni di conflitto d'interesse.

La sua nomina, è necessariamente legata al possesso di determinati requisiti e completenze tecniche per assolvere i compiti cui è preposto. Qui si richiede una conoscenza specifica valutata caso per caso da parte del titolare del trattamento: questo, dovrà trovare, sotto la sua diretta responsabilità, il soggetto che possieda le competenze normative e di prassi giudiziaria in materia di tutela dei dati personali[167] che sia proporzionale alla complessità tecnica e organizzativa del suo specifico trattamento.

Rivestendo la qualifica sia il punto di contatto necessario tra l'attività di trattamento e l'Autorità di controllo che di supporto del titolare, risulta fondamentale che il *DPO* conosca ogni specifico aspetto tecnico e ne riesca a comprendere ogni sfaccettatura delle attività monitorate, al fine di poter effettivamente valutare la conformità dei trattamenti alla normativa Eurpoea e Nazionale: non esiste uno *standard* comune ma occorrono valutazioni specifiche.

Percorrendo l'articolo 39, si possono enucleare le cinque funzioni principali che il *DPO* è chiamato a svolgere nel corso della sua attività, sono solo le principali in quanto il WP29 sottolinea espressamente che l'elenco non è esaustivo.

Le prime tre lettere del primo paragrafo, articolo 39, ed il secondo paragrafo attengono ai rapporti che il *DPO* presenta con il titolare ed in generale all'interno della sua struttura organizzativa: in particolare la lettera *a)* stabilisce il compito di "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati".

Alla lettera b), impone di "sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai

167 Ovviamente si fa riferimento non solo al GDPR ma anche all'eventuale normativa integrativa sia Europea che Nazionale.

trattamenti e alle connesse attività di controllo".

Da ultimo, alla lettera c) si stabilisce che debba "fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".

Il secondo paragrafo dell'articolo 39, prevede poi che "Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo" e ciò al fine di coadiuvare attentamente l'attività del titolare per poterlo supportare nella riduzione dei rischi che il trattamento può presentare.

Le due lettere finali invece chiariscono i rapporti che questo soggetto deve intrattenere con le Autorità di controllo: specificamente la lettera *d)* impone un generale dovere di "cooperare con l'autorità di controllo;" e la lettera *e)* gli conferisce di "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione".

A questi compiti se ne aggiunge un sesto che attiene ai rapporti tra *DPO* e interessati, definito nell'articolo 38: "Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento".

Se si osservano unitamente tutte le funzioni che un *DPO* è chiamato a svolgere si nota fin da subito, come esso non sia preordinato a svolgere un'attività di controllo spietata sui trattamenti effettuati dal titolare ma piuttosto, risulta il suo principale collaboratore per assicurare l'adeguatezza del sistema alla tutela dei dati personali e per sensibilizzare l'operato futuro.

Va comunque sottolineato che nonostante la funzione principale di supporto, rimane sempre e comunque indipendente, ciò è confermato dal fatto che il suo secondo interlocutore è l'Autorità di controllo per il quale svolge la funzione di "punto di contatto per le questioni relative al trattamento."

Un'altro profilo della sua indipendenza si evince dal fatto che delle eventuali violazioni rispondono solo e soltanto il titolare ed eventualmente il responsabile ma mai il *DPO*. L'unica responsabilità in cui potrebbe mai incorrere il *DPO* è quella professionale per il modo in cui svolge i suoi compiti.

1.2.2. Il valore del Responsabile per la Protezione dei Dati in rapporto alle macchine Intelligenti.

Il *DPO* dunque, quando nominato, risulta decisamente il punto di equilibrio di tutto il sistema ma vanno osservati i suoi margini di operatività qualora sia nominato per assistere trattamenti basati su tecniche

Intelligenti come *Big Data* e *Machine Learning*.

Il suo ruolo può essere davvero fondamentale in due visioni diverse ma complementari: da un lato riunendo una serie di trattamenti frammentati, svolgendo per gli stessi le funzioni di *DPO* unico e garantendo l'omogeneità del sistema e dall'altro nella possibilità che diventi il diretto supervisore di macchine in grado di eseguire autonomamente dei trattamenti su dati personali, fornendo un costante controllo umano sulle sue azioni.

La prima funzione che potrebbe essere chiamato a svolgere, quella di essere nominato *DPO* per una pluralità di titolari, risulta di particolare importanza sopratutto nella catena dei trattamenti, dove le attività serapate di due o più titolari sono legati da una finalità ultima comune.

In questi casi, la frammentarietà delle attività dei singoli titolari potrebbe creare difficoltà a ricostuire l'omogeneità della catena nel suo complesso, sopratutto nella redazione dei registri o nell'imputazione delle reciproche responsabilità per eventuali violazioni.

Il *DPO* in questa prospettiva, per essere nominato, dovrebbe avere un'esperienza adeguata a gestire la complessità di tutta la catena e riuscirebbe a "vedere dall'alto" tutto il sistema nel suo insieme, comprendendo sia i rischi legati a signole attività che quelli complessivi e valutandone le rispettive miusre di sicurezza a tutela dei dati, individuando altresì le eventuali fragilità dal passaggio di un anello all'altro della catena e le responsabilità individuali.

Quando poi il *DPO* si troverà a comunicare con l'Autorità di controllo, sarà in grado di darle un'adeguato rendiconto delle attività.

La tecnica della riunione può essere molto utile qualora ogni trattamento separato sia adottato con tencniche notevolmente pervasive (ad esempio *Big Data*) ma esistono anche ipotesi dove è la separazione che riesce ad offrire dei vantaggi alla catena.

Nel caso di una catena che vede una serie di trattamenti semplici dove solo l'ultimo anello opera con tecniche complesse, sarà più opportuno nominare due distinti *DPO* così da tenere ben separate le responsabilità dei vari titolari e per non confondere le complessità delle attività.

Si nota così che l'elasticità delle norme sulla nomina del *DPO*, permette di architettare sistemi *ad hoc* di controllo senza mai perdere le garanzie di tutela dei dati personali poiché al crescere della complessità dovranno aumentare i requisiti professionali del soggetto, in grado eventualmente anche di gestire trattamenti effettuati con strumenti di *Data Analysis*.

Per analizzare la seconda prospettiva, va ripreso il concetto che ogni singolo trattamento può prevedere la nomina di un *DPO*.

Abbiamo osservato[168] che dispositivi Iot e alcune macchine Intelligenti riescono ad agire

168 Rimando alla lettura integrale del Capitolo secondo di questo elaborato.

autonomamente dall'intervento umano, conservando, elaborando e trasferendo dati, tutte attività che sono riferibili ad un titolare di trattamenti: in questa circostanza quindi si potrebbe prevedere che il programmatore del dispositivo oppure il dispositivo stesso, se la sua Intelligenza lo permette, nomini un DPO al fine esclusivo di monitorare la congruita dell'attività posta in essere dalla macchina al GDPR.

La circostanza che un *DPO* possa esercitare le sue funzioni rispetto a queste macchine risulterebbe molto interessante in quanto fornirebbe la garanzie della presenza umana in una serie di attività che spesso sfuggono al nostro controllo, fornendo fiducia e sicurezza verso questi dispositivi.

Se poi si considera che queste due prospettive sono complementari e anzi, nel tempo, ci si aspetta che si integrino a vicenda costituendo catene di trattamenti sempre più lunghe e complesse, si vede come, sotto questo punto di vista, il GDPR, purchè interpretato in modo opportuno, sia uno strumento assolutamente valido ad adattarsi agli sviluppi che il futuro può portare.

Infine bisogna anche sottolineare che i compiti affidati al *DPO* dal GDPR , in particolare dall'articolo 39, non costituiscono un'elenco chiuso ma anzi è proprio il WP29 nelle Linee Guida n. 243 ad incoraggiare i titolari ad arricchire le funzioni del *Data Protector Officer* in modo da consentirgli il pieno svolgimento del suo ruolo. Anche questa eventualità è un'apertura della normativa agli sviluppi futuri, sia tecnologici che sociali o organizzativi.

2. Tecniche e finalità di un attacco informatico.

L'esplosione tecnologica e lo spostamento della nostra identità e nel mondo digitale ha sicuramente portato concreti vantaggi per il progresso sociale e scientifico ma di contro ha suscitato l'interesse di persone malintenzionate ed esperte del mondo di *Internet*.

Questi soggetti hanno reagito alla crescita esponenziale dei dati e quindi, alla relativa crescita del mercato in materia, adottando una serie di strategie per attaccare singoli dispositivi o interi archivi di informazioni al fine di ottenere i vantaggi per cui l'attacco è preposto.

Non è possibile in generale determinare a priori le finalità di un attacco informatico in quanto ogni attaccante le determina caso per caso, in base alle ragioni etiche o economiche che li guidano, mirando talvolta a distruggere (nel gergo tecnico "*bucare*") interi archivi di dati, processi automatizzati o siti ed altre volte a rubare il maggior numero di dati possibile al fine di poterli utilizzare, rivendere o riscattare al legittimo proprietario.

Anche le tecniche adottate sono le più disparate[169]: ovviamente anche questi soggetti fruiscono delle

169 Il team di *Avast*, noto antivirus scaricabile gratuitamente, ha stilato a tal proposito un elenco delle minacce presenti *online* per aiutare gli utenti a difendersi da eventuali attacchi informatici. https://www.avast.com/c-malware .

tecnologie più avanzate disponibili nel mercato e spesso possiedono delle capacità tecniche molto elevate che gli consentono di sfruttare dispositivi e codici di programmazione nel modo più efficiente.

Si possono dividere gli attacchi informatici in due ampie categorie, anche se queste sono perfettamente integrate tra loro: esistono gli attacchi informatici diretti, che richiedono l'intervento dell'attaccante umano per tutta la durata del cd *Cyber*-attacco, e proliferano poi gli attacchi indiretti che possono essere assimilabili alle trappole[170]. L'attività dell'attaccante è preventiva e mira alla programmazione di un *software* che poi verrà caricato su internet al fine di essere scaricato, camuffando la sua identità di software malevolo, dal maggior numero di utenti.

Ecco perche la definizione fornita da Karnouskos di *Cyber*-attacco è così ampia, e consiste in "una qualunque manovra, impiegata da individui od organizzazioni anche statali, che colpisce sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite atti malevoli, provenienti generalmente da una fonte anonima, finalizzati al furto, alterazione o distruzione di specifici obiettivi violando sistemi suscettibili.

Tali azioni sono classificabili in *Cyber campaign*, guerre cibernetiche o cyberterrorismo a seconda del contesto. Gli attacchi informatici spaziano dall'installazione di *Spyware*[171] su di un PC fino a tentativi di demolizione delle infrastrutture di intere nazioni".

Gli attaccanti vengono solitamente denominati con il termine "ombrello" di *hacker* ma va notato che al loro interno si suddividono in tre classi a seconda della loro pericolosità, con riferimento alle abilità tecniche e conoscenze specifiche, e riespetto alle finalità che intendono soddisfare con l'attacco.

I più pericolosi sono sicuramente i *Cracker*, ossia i veri e propri "pirati informatici", esperti di programmazione, di sistemi e di sicurezza, in grado di introdursi in reti di computer senza autorizzazione allo scopo di danneggiare un sistema informatico. Il fine è quello di danneggiare o distruggere il sistema e possono essere spinti da varie motivazioni, dal guadagno economico con operazioni di spionaggio industriale all'approvazione all'interno di una comunità di *cracker*.

Questi non vanno confusi con gli *Hacker* in senso stretto, i quali sono contraddistinti da una cultura e un'etica legata all'idea del *software* libero, che eludendo o violando illegalmente ovvero senza autorizzazione reti di computer, mirano a sottrarre programmi o dati per renderli pubblici[172].

Da ultimo, troviamo una figura piuttosto fastidiosa per singoli utenti ma che tuttavia non rappresenta una grave minaccia per il sistema nel suo complesso: i *Lamer*. Un *lamer* opera con conoscenze informatiche

---

170 Uno dei più famosi è chiamato, non a caso, *Trojan* in riferimento alla trappola ideata dagli Achei, il cavallo di Troia appunto, esplicata da Omero nel mito Graco, Iliade. Un *trojan* è un tipo di virus che cerca di passare per una risorsa utile, sicura o di intrattenimento mentre tenta di causare danni o rubare dati.

171 Uno *Spyware* è un tipo di *malware* difficile da rilevare che raccoglie informazioni sulle abitudini di navigazione, sulla cronologia dei siti visitati e di natura personale, utilizzando spesso *Internet* per trasferire le informazioni a terze parti senza che l'utente ne sia a conoscenza.

172 In realtà in materia si sono sviluppate con il tempo due sottocategorie di *hacker*, i *black hat,* cappucci neri, che sono quelli appena descritti ed i *white hat,* cappucci bianchi, che sono esperti, incaricati da determinate aziende o organizzazioni per violare i loro sistemi informatici al fine di testarne le misure di sicurezza. Tali soggetti risultano davvero molti utili in ambito della *Cyber security.*

limitate e basilari, con lo scopo di provocare danni a un computer o un sistema protetto per divertimento. Non possedendo adeguate conoscenza spesso arrivano ai loro scopi usando programmi fatti da altri seguendo guide che circolano per il web.

Il tema è delicatissimo e va adeguatamente tenuto sotto controllo: il pericolo di un attacco informatico è tanto più ampio quanti più dati personali, sopratutto sensibili, sono contenuti all'intendo degli archivi hardware che possediamo. I *Big* della società digitale, come *Facebook, Google, Amazon, Apple* e tanti altri, sono sicuramente i soggetti più difficili ma allo stesso tempo più ambiti da colpire, perchè con un unico attacco si riescono a carpire un numero gigantesco di informazioni sensibili e quindi si massimizza il numero dei danni, o guadagni, a dipendere dalla prospettiva.

Tanto per richiamare un esempio, nel 2009, gli *hacker* presero di mira *Google China*, penetrando nei server ben protetti dell'azienda. I cybercriminali, utilizzando dei *Worm*[173]. erano riusciti a forzare il sistema di sicurezza di *Google*, rubando e compromettendo una serie di informazioni riservate: in particolare, il colosso riferì che i cybercriminali avevano perso di mira gli account *Gmail* di molti attivisti, impegnati a difendere i diritti umani nel Paese Cinese. Molti esperti notarono sul punto che l'attacco poteva essere stato architettato dallo governo di Pechino.

2.1. Segue: Svolgimento e diffusione dei *Cyber* attacchi.

Per comprendere meglio come si concretizzano questi attacchi va sottolineato che in generale si possono articolare in cinque distinte fasi.

La prima fase necessaria è senza dubbio, l'individuazione del bersaglio da colpire perchè è strumentale alla fase di studio. I cybercriminali cominciano così a raccogliere più informazioni possibile sull'azienda e soprattutto sul suo sistema di sicurezza per progettare e impostare l'attacco.

Scelte le modalità operative da adottare, sulla base delle informazioni raccolte, inizia la seconda fase: l'intrusione. In questa fase, i cybercriminali entrano silenziosamente, magari sfruttando tecniche di *Phishing*[174], si appropriano delle credenziali del *network* di protezione o installano dei *software* malevoli sui computer aziendali con l'obiettivo di ottenere il controllo dei dispositivi da remoto. Si tratta di una fase molte delicata, dalla stessa dipende il successo o il fallimento della violazione.

La terza fase si concretizza nello monitoraggio e nello studio del *network* aziendale: Agendo come un utente autorizzato, l'attaccante studia il *network*, mappando i server, individuando i *database* e analizzando la rete di protezione. Lo scopo principale è quello di allargare il più possibile la compromissione. Il cybercriminale in questa fase, come se fosse un *Virus*[175] umano. Normalmente, il tutto si verifica in

173 Un *Worm* (letteralmente "verme") è una particolare categoria di *malware* in grado di autoreplicarsi. Ha una funzione analoga a quella di un virus ma, a differenza di questo, non necessita di legarsi ad altri programmi per diffondersi, ma a tale scopo utilizza altri mezzi come ad esempio tramite e-mail e una rete di computer.

174 Il Phishing è un approccio utilizzato dagli attaccanti per spingere gli utenti a rivelare informazioni personali, quali password o dati delle carte di credito o dei conti correnti bancari. Tale operazione avviene inviando mail fasulle o indirizzando l'utente su un sito web fasullo.

175 Convenzionalmente un *Virus* informatico è un programma o una sezione di codice caricato nel computer senza che il

settimane o anche mesi prima che l'attacco vero e proprio si svolga.

Una volta ottenute le credenziali di un utente autorizzato e dopo aver raccolto le informazioni necessarie sul server inizia la quarta fase dove gli *hacker* prendono effettivamente il controllo dei sistemi informatici dell'azienda. A questo punti i pirati informatici compromettono tutti i canali del *network* di protezione governando l'accesso a tutti i *server* dell'impresa.

L'ultima fase attiene proprio all'attacco finale: i cybercriminali escono allo scoperto, mettendo in pratica il loro obiettivo finale ad esempio inibendo le attività dell'azienda criptandole tutti i dati mediante dei *Ransomware*[176], e chiedere dei soldi in cambio della decriptazione.

Se l'attacco arriva in questa fase, risulta troppo tardi per fermare la minaccia informatica che è iniziato già da molto tempo prima di uscire allo scoperto. Il problema sta poi nel fatto che gli attaccanti, spesso, riescono ad eseguire tutto ciò senza lasciare minima traccia del loro passaggio e rimanendo ignoti agli occhi dell'azienda colpita e quindi impuniti.

Worm, *rootkit*[177], *virus* e ancora, *spyware*, *trojan* e *phishing*: sono queste alcune delle minacce informatiche più diffuse capaci di danneggiare, spesso in maniera irreversibile, i dispositivi degli utenti non protetti. Una serie di *malware* che gli attaccanti possono utilizzare a proprio vantaggio, per avere accesso a informazioni sensibili come password e dati delle carte di credito.

La diffusione del *malware* risulta in continuo aumento: si calcola che nel solo anno 2008 sul *Web* siano girati circa 15 milioni di *malware*, *Kaspersky Lab* una nota azienda che produce *anti-virus* e sistemi di sicurezza, nelle statistiche relative al primo quadrimestre del 2018 ha rilevato 796,806,112 attacchi online lanciati da dispositivi localizzati in 194 diversi Stati in tutto il mondo[178], anche già nel Marzo del 2010, *Symantec*[179] ha nominato Shaoxing (Cina), come la capitale mondiale del *malware*.

Microsoft ha dichiarato che, nel Maggio 2011, ogni 14 download da internet uno è probabile che contenga del codice maligno. I social media, *Facebook* in particolare, stanno constatando un continuo incremento delle tattiche usate per diffondere il malware. Nonostante il numero sia di per sé allarmante, va notato che è destinato inesorabilmente a crescere nel tempo.

La preferenza di usare il *malware* come strumento per compiere crimini su *Internet*, insieme alla sfida del software *anti-malware* che cerca di tenere il passo per contrastare i nuovi programmi malevoli,

---

proprietario ne sia a conoscenza o lo abbia autorizzato. Alcuni *virus* causano solo fastidi, mentre la maggior parte è dannosa e ideata per infettare e prendere il controllo dei sistemi vulnerabili: può diffondersi in molti computer e reti duplicandosi, proprio come un virus biologico che passa da persona a persona.

176 I *Ransomware,* chiamati anche *rogueware* o *scareware,* limitano l'accesso al sistema informatico di un utente e richiedono il pagamento di un riscatto per rimuovere il blocco.

177 Un *rootkit* è un programma progettato per fornire agli *hacker* accesso come amministratore a un computer senza che l'utente ne sia consapevole.

178 Tra le stime pubblicate sempre da *Kaspersky Lab*, risultano 282'807'433 i siti *Internet* riconosciuti come maligni dai servizi *Web* di *anti-virus*, individua nel numero di 204'448, gli utenti infettati da *malware* finalizzati al furto di denaro attraverso gli accessi *online* ai conti bancari e sottolinea anche come siano stati presi di mira anche i nostri dispositivi mobili, qualificando in 1'322'578 il numero di applicazioni maligne installate sui nostri *smartphones* e *tablets*. Per le stastistiche complete rimando al sito del K*aspersky Lab*: https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/ .

179 *Symartec* è uno dei *leader* mondiali nella presestazione e progettazione di servizi di sicurezza intormatica.

hanno portato alla necessità di prendere delle contromisure sia da parte dei singoli utenti, sia dalle aziende: questo significa che dovranno offrire servizi web con una adeguato livello sicurezza per la tutela del cliente.

Il risultato dell'aumento e della facile diffusione dei malware, imponge un'analisi approfondita sui sistemi di sicurezza da usare per proteggere, da un lato la attività aziendali ma sopratutto per tutelare i diritti e le libertà fondamentali delle persone che verrebbero direttamente lesi da questi comportamenti.

Ovviamente il GDPR, perseguendo la duplice finalità della libera circolazione dei dati e della protezione dei diritti e delle libertà delle persone fisiche, non poteva non inserirsi nel settore regolando le misure che il titolare, il responsabile o, se del caso, il *DPO* devono adottare al fine di rendere il trattamente sicuro da ingerenze esterne.

3. La Sicurezza Informatica.

La sicurezza riveste un ruolo davvero fondamentale nel Regolamento in quanto come si è visto, gli effetti di un attacco informativo possono essere molteplici e tutti invasivi sia per la libera circolazione dei dati sia per i diritti e le libertà degli interessati.

Le misure di sicurezza rientrano tra i doveri specifici del titolare (e ovviamente anche del responsabile, qualora nominato) e devono essere disposte per proteggere i trattamenti ed, in generale, i dati che conserva, il tutto, sotto la sua diretta responsabilità. Più precisamente, come già osservato nel primo Capitolo [180], il GDPR pone l'accento sul principio di Accountability e cioè sul dovere del titolare non solo di garantire ma anche di essere sempre in grado di dimostrare di aver rispettare i princìpi del Regolamento e di conseguenza anche con riferimento alle misure ritenute idonee.

Le norme del Regolamento che si preoccupano di disciplinare la materia vanno dall'articolo 32, propriamente relativo alle misure di sicurezza, all'articolo 34, queste due ultime disposizioni attengono alle comunicazioni obbligatorie a seguito di una violazione di dati, e nel loro complesso formano la seconda Sezione del Capo IV.

Si noti fin da subito che anche la disciplina delle misure di sicurezza ha subito grandi cambiamenti rispetto alla precedente normativa Europea (principalmente la Direttiva 45/96) e quella Nazionale[181] e questo in ragione sia delle mutate finalità del GDPR che per meglio adattarsi agli sviluppi tecnologici intervenuti nel tempo.

Oggi, nel sistema legislativo, le misure di sicurezza se da un lato si riferiscono essenzialmente a tutti gli strumenti difensivi, posti a tutela dei dati dell'interessate, dall'altro assume anche una dimensione più

180 Si veda nello specifico il paragrafo 6.1. del primo Capitolo.

181 Ad esempio, nel GDPR muta il concetto di "Misure Minime", che invece caratterizzava il D.lgs 196/2003 (il cd. Codice Italiano sulla Privacy). Le "misure minime" si trasformano in "misure adeguate" anche se comunque si possono enucleare un insieme minimo di azioni che risultino adeguate a soddisfare le esigenze di responsabilità, rectius *Accountability,* posto dalle norme.

pratica e funzionale in quanto ricomprende anche la qualità e l'affidabilità dei dati che si trattano.

Abbiamo già visto nel secondo Capitolo[182] come la scarsa qualità dei dati possa creare seri danni al sistema nel suo complesso: più dati inadeguati circolano nei vari archivi, più l'errore cognitivo del singolo trattamento finisce per diventare un errore diffuso e sistematico. Questo è sicuramente configurabile come un problema di sicurezza.

Se la violazione di un sistema informatico, a seguito di un cyber.attacco, può essere un valido indicatore di un sistema di sicurezza inefficace, come sottolineano le Linee Guida elaborate dal WP29 in materia di "*Personal Data Breach Notification*" con la frase "*a breach is a type of security incident*[183]", va tenuto ben presente però che le misure di sicurezza vanno predisposte prima che un trattamento abbia inizio e costituiscono una condizione di legittimità dello stesso.

A tal proposito l'articolo 32 recita: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio"

Si vede così il profondo legame necessario intercorrente tra i rischi e le misure di sicurezza: non sarebbe possibile predisporre delle misure di sicurezza preventive se non si ha contezza dei rischi che si corrono nel porre in essere un trattamento ed inoltre, chiarifica che le misure possono definirsi adeguate solo se rapportare alle specifiche criticità del sistema.

È proprio da questi profili che non si può operare una lettura dell'articolo 32 senza analizzarlo congiuntamente con l'articolo 24, relativo alla valutazione dei rischi, ed eventualmente con l'articolo 35, relativo alla DPIA, poiché queste sono le premesse logiche per l'operatività delle misure adeguate di sicurezza.

Il parafrago 2 dell'articolo 32, dal canto suo, specifica poi che tali misure "tecniche e organizzative" devono essere finalizzate ad impedire i rischi "in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati"[184].

Le misure di sicurezza quindi sono volte alla protezione dei dati personali in sè e di conseguenza mirano alla salvaguardia dei diritti e delle libertà non solo degli interessati ma di tutte le persone fisiche dei cui dati si tratta, cercando di evitare che i rischi rilevati nelle fasi di valutazione si possano concretizzare.

---

182 In particolare, si cofronti il paragrafo 4. del secondo Capitolo.

183 Letteralmente "Una violazione è un incidente legato alla sicurezza."

184 Si veda a tal proposito anche il Considerando 83, che anch'esso richiama "il rischio di distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale."

In merito alle concrete metodologie da applicare per configurare un adeguato sistema di sicurezza informatica, la norma specifica solamente la pseudonimizzazione e la cifrature.

Rispetto alla pseudonimizzazione, abbiano gia osservato[185] come questa tecnica abbia una doppia funzionalità: da un lato permette di ridurre i rischi che un determinato trattamento può presentare e dall'altro è una tecnica che consente di rendere i dati e le attività più sicure rispetto ad eventuale attacchi informatici. Rimando alla lettura del parafrago richiamato per i dettagli applicativi della tecnica.

Mediante il termine cifratura si fa riferimento ad un'ampia categoria di tcniche le quali hanno come fine ultimo quello di andare a codificare determinate informazioni così da rimanere incomprensibili a tutti tranne che ai possessori dei codici di decifratura.

Esistono oggi due grandi famiglie di tecniche crittografiche informatiche, sulla base del genere di chiave utilizzato per criptare/decriptare le informazioni: si ha da un lato la crittografia a chiave simmetrica, o a chiave segreta, dove la chiave del mittente per criptare il messaggio e quella del destinatario per decriptarlo è unica, si parla invece di crittografia a chiave asimmetrica, o a chiave pubblica, quando esistono due chiavi di cifratura distinte, quella di cifraturala è pubblica mentre quella di decifratura è privata.

Si tratta comunque solo di esempi in quanto l'elenco non è assolutamente tassativo, le tecniche che verranno in concreto utilizzate, dal titolare e/o dal responsabile dipendono esclusivamente dalle caratteristiche e dai livelli di rischi che il trattamento presenta purchè presentino determinate caratteristiche speficicate nelle lettere b) e c) del primo paragrafo dell'articolo 32

In particolare devono presentare “la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento” e quella “di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.”

Si noti come le priorità della sicurezza non attengono solo alle tecniche di tutela dei dati ma anche e sopratutto alla “resilienza dei sistemi” e cioè di un'adeguatezza degli apparati hardware e degli strumenti tecnologici a supportare determinati trattamenti e a resistere ad evenutali minacce o malfunzionamenti tecnici.

In chiusura poi si pone l'articolo 32.1 lettera d) il quale prevede che venga effettuata “una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.”

La norma a questo punto richiede che le misure di sicurezza, parametrate sui rischi concreti che il trattamento presenta, risultino non solo potenzialmente adeguato ma che lo siano effettivamente, imponendo al titolare di attuare ulteriori procedure per valutare il sistema opportunamente integrato da tali misure: questo può essere attuato sia simulando degli attacchi informatici al sistema[186] sia attraverso ulteriori

185 Si osservi il paragrafo 6.4.1. del Capitolo Primo.
186 Questo compito, spesso viene svolta da quella fazione di hacker denominati *white hat* e definita nel paragrafo precedente.

valutazioni più teoriche. Saranno poi indispensabili controlli periodici per poter dichiarare la conformità di gestione rispetto alle esigenze derivanti dal trattamento dei dati

Sembra un iter piuttosto complicato e gravoso per il titolare in quanto composto da almeno tre distinte fasi: si parte da una prima valutazione qualitativa del rischio potenziale lordo, cioè senza considerare le misure di sicurezza applicate, individuando le tipologie e le quantità dei dati per poi definire i rischi potenziali che potrebbero colpire le persone fisiche dalla perdita di sicurezza dei dati. Si procederà poi a rafforzare i punti che presentano le maggiori fragilità integrandoli con le misure adeguate di sicurezza.

In base alle misure di sicurezza applicate e ai controlli eseguiti, andremo a ridurre la probabilità dei rischi rilevati. Va a questo punto ricalcolato il Rischio effettivo netto, cioè ridotto dalle contromisure di sicurezza applicate.

La differenza del livello di rischio, dal lordo al netto, rappresenta l'efficacia delle misure applicate e dovrebbe evidenziare l'adeguatezza degli investimenti apportati per assicurare la sicurezza.

Per valutare i rischi e porre in essere misure tecniche e organizzative volte a garantire un adeguato livello di sicurezza servono dunque competenze ed esperienze tecniche specifiche, ecco perché il Comitato Europeo per la Protezione Dati suggerisce la nomina di un *DPO* anche in assenza di specifico obbligo.

La perfetta adeguatezza con cui il Regolamento si pone dinnanzi alle sfide del futuro è dovuta proprio all'estrema elasticità con cui le norme sono modellate: viene rifuitata l'idea di *strandard* minimi prefissati in astratto ma l'accento si pone sempre sui casi concreti, lasciando ai titolari libertà di azione ma al tempo stesso tale attività è sotto la loro diretta responsabilità, qualora in cui risultasse inidonea a prestare le necessarie garanzie.

3.1. Gli sviluppi della sicurezza nel contesto delle Intelligenze Artificiali.

Il principio di necessaria adeguatezza delle misure di sicurezza rispetto ai rischi potrebbe comportare che dei trattamenti effettuati attraverso Intelligenze Artificiali o software Intelligenti richiedano conseguentemente la necessità di misure di sicurezza basate anch'esse su Intelligenze Artificiali, e cioè particolari software che riescano ad rintracciare e neutralizzare automaticamente attacchi informatici e malware.

Si è abituati a ricollegare le tencologie dell'intelligenza artificiale a programmi che consentono la guida automatica di autoveicoli oppure di riconoscimento della voce come gli assistenti vocali presenti in alcuni smartphones come Cortana[187] o Siri[188]. In realtà, l'evoluzione delle Intelligenze Artificiali si rivolge

187 Cortana è un programma di assistenza per l'utente con riconoscimento del linguaggio naturale programmato da Microsoft per alcunii sistemi operativi basati sul sistema operativo di Windows.

188 Siri è un *software* di assistenza digitale che comunica con l'utente attraverso il linguaggio , sviluppato dalla Apple Inc. presente sui dispositivi dalla stessa messi sul mercato quali, iPhone, iPad, Mac etc.

anche alla protezione dei dispositivi e dei dati.

La difesa è uno dei principali obiettivi fissato dagli esperti nell'elaborazione delle nuove proposte tecnologiche e sicuramente le abilità presentate dai sistemi di machine learning e deep learning trovano, nella sicurezza informatica, terreno fertile per operare.

D'altronde non è difficile da immaginare: se i *pattern*[189] consentono alla macchina di rilevare ed elaborare un dato in input fino al punto di riconoscere il parlato umano, basterà modificare il pattern in modo tale da fargli riconoscere le attività anomale e/o i dati sospetti presenti nel nostro dispositivo o negli archivi di dati.

Da molti anni gli esperti di sicurezza sfruttano tali tecnologie per raffozare la protezione e offrire una difesa innovativa in grado di modellarsi alle tante minacce che circolano nel mondo del web. Nel settore si può richiamare un "vecchio amico", analizzato nel secondo Capitolo[190]: si tratta ancora una volta di *Watson*, realizzato da IBM, vincitore del gioco a premi Americano *Jeopardy* nel 2011 e già adattato anche nel campo delle analisi mediche, veste ora anche un ruolo importante anche se immesso nel settore della sicurezza informatica (*Watson for Security*).

Lo strumento permette agli operatori umani di avere una piattaforma su cui operare al fine di allontanare le varie minacce: in realtà il programma, per ora, non si occupa autonomamente di sorvegliare i sistemi e la rete, ma necessita di essere attivato dall'utente per specifiche attività tra quelle preimpostate.

Il software effettua un'analisi accurata di tutti i dati posti sotto osservazion, fornendo all'utilizzatore una relazione completa sulle attività che sono state effettuate all'interno del sistema stesso. Il programma poi fornirà tutte le informazioni, ma spetta, ancora una volta, alla persona trarre le opportune conclusioni e decidere le azioni da seguire.

Non è comunque l'unico programma applicato nel campo della sicurezza informatica che sfrutta l'Intelligenza Artificiale ma *Watson* è diverso rispetto agli altri programmi[191], perche riesce ad analizzare la totalità del traffico della rete e di dati da cui analizza ed apprende quali siano i normali flussi.

In generale però l'Intelligenza Artificiale in questo ambiente, entra in opera al fine di rilevare le anomalie all'interno di tutti i dati raccolti e valutati, divenendo un eccelso alleato nel caso in cui si installino automaticamente software scaricati dal web o anche nell'ambito di protezione dei dati delle aziende, soggetti ad attacchi di spionaggio industriale.

Mediante queste tecniche si ha la capacità di esaminare, in modo sistematico, il 100% dei dati, per individuare le minacce[192] ovunque esse siano, e di predisporre tutte le azioni conseguenti per eliminarle e

189 Si veda il paragrafo 3. del secondo Capitolo.

190 Si rimanda al Secondo Capitolo, paragrafo 2. per maggiori dettagli,

191 Come ad esempio *Darktrace* il quale viene fondata nel 2013 da matematici e studiosi dell'Università di Cambridge che non sfrutta regole per rilevare e individuare le minacce, ma è finalizzato all'analisi dei comportamenti degli utenti e/o dei dispositivi sulla rete: qualora un'anomalia venisse rilevata, viene inviato un apposito rapporto agli operatori umani addetti alla sicurezza per prendere le contromisure necessarie.

192 Questa possibilità è di fondamentale importanza se si nota che quasi la totalità dei dati sono innocui mentre i pericoli si celano in una serie di frammenti di informazioni, per questa ragione si deve studiare ogni singolo passaggio di dati per ritrovare le minacce *cyber*. Se si volesse utilizzare una metafora: rintracciare un potenziale attacco informatico è come trovare un ago in un pagliaio.

proteggere o ripristinare il sistema. Tuttavia ciò è possibile solo in termini teorici poiché la capacità di operare del programma varia al variare di numerosi fattori quali, l'ampiezza dei dati da analizzare, la complessità dei malware da individuare, la potenza dell'hardware su cui opera etc.

Questa è sicuramente la funzione principale delle IA nel settore ma tali tecniche non si occupano solamente di individuare le minacce e di indagare sulle attività all'interno della rete, ma opera anche attraverso la prevenzione, evitando le intrusioni non autorizzate e proteggendo i dati più sensibili contenuti nei dispositivi.

L'AI agisce memorizzando i comportamenti degli utenti sul web, il modo con cui digitano le password e le informazioni scambiate così da avere un quadro della situazione e attuare le misure necessarie per garantire la sicurezza. Il software risuletrà, a seguito dell'analisi, capace di verificare se chi sta visitando un sito internet è una persona oppure un'altra IA[193]. Grazie a tale modalità di lavoro, si possono in generale riconoscere i visitatori e gli utenti di siti e banche dati non tanto dalle password inserite ma dal comportamento che adottano visitando il sito.

Un'ulteriore innovazione arriva dall'impiego di reti neurali addestrate con tecniche di apprendimento intuitive che permettono di proteggere, in maniera quasi istintiva, le informazioni di valore. Il programma, cioè, è addestrato a riprodurre la capacità decisionale umana dettata dall'istinto, ricercando contromisure veloci ed efficaci per affrontare minacce imminenti o sconosciute.

Chiaramente in questo scenario esiste il rischio che i pirati informatici possano usare gli stessi sistemi di sicurezza per far partire i loro attacchi. Anche i *Big* dell'informatica, con strumenti di difesa sofisticati, collegati a software Intelligenti, sono stati soggiogati da *cracker* e *hacker* ma si è registrato come i loro successi/tentativi siano serviti da stimolo ed esempio per un incremento dell'efficienza dei nuovi sistemi di sicurezza informatica.

3.2. Le nuove sfide della Sicurezza Informatica nel mondo dell'*Internet Of Things*.

Se parte delle azioni dei cyber criminali sono finalizzate a rubare la disponibilità dei dati personali delle persone fisiche, si può osservare come diventino un bersaglio più che ambito quei dispositivi contenenti una immensa mole di dati e connessi alla rete, cioè tutte le apparecchiature rientranti delle tencologie IoT.

Il furto dei dati tuttavia non è l'unico aspetto che rende questi dispositivi delle ottime prede anzi forse è il meno rilevante. I dispositivi IoT sono tutti interconnessi tra loro e la possibilità di violare un singolo dispositivo consente all'attaccante di entrare, monitorare e controllare tutto il sistema che li collega.

In un'analisi rivolta proprio al tema della sicurezza, la società di servizi informatici, Deloitte[194],

193 Si prenda in esame, ad esempio, il modo con cui vengono cliccati i tasti del mouse, la velocità di movimento, la durata dei click e quanto permette di monitorare i visitatori delle pagine web.

194 Deloitte Touche Tohmatsu è un'azienda che fornisce servizi di consulenza e revisione dei sistemi informatici, la prima nel mondo per ricavi e numero di professionisti impiegati.

fornisce l'esempio molto semplice di un telecomando per l'apertura del cancello del garage che consente anche di disattivare da remoto l'allarme: la violazione delle autorizzazioni del telecomando potrebbe consentire un accesso libero ed indisturbato ad eventuali soggetti malintenzionai che apparirebbero al sistema e probabilmente anche ai vicini di casa come accessi autorizzati.

Se infatti la nostra attenzione si focalizza sui dati personali, bisogna comunque rilevare che i dispositivi IoT consentono una forte integrazione tra mondo virtuale e quello reale, tale che mediante sensori un software può controllare una porzione di realtà ed in questo contesto anche gli attacchi informatici possono avere effetti ibridi sul mondo sia virtuale che reale, come per fare degli altri esempi, il controllo di un semaforo o di una macchina a guida automatizzata oppure quello dei sistemi di produzione industriale o ancora l'alterazione delle normali funzionalità di un pacemaker.

Questi strumenti possono definirsi dei bersagli "facili" in quanto le loro attività si svolgono nella rete anche senza il diretto controllo umano: quest'ultimo spesso non è consapevole dell'attività che ha compiuto la macchina e potrebbe scoprire un'eventuale minaccia quando ormai i danni sono troppo estesi.

Da qui emerge un'esigenza fondamentale, non può esistere un progetto IoT che sia disgiunto da forti misure du sicurezza: anche qui le norme del GDPR ed in particolare l'articolo 32, ricostruisce l'equazione in cui tanti più dati, in particolare sensibili, si condividono e tanto maggiore sarà il rischio di attacchi e di conseguenza dovrà aumentare la funzionalita e l'efficienza dell'assetto della sicurezza.

Se l'interconnessione dei dispositivi è la caratteristica principale che si sperava di realizzare mediante i dispositivi IoT, costituisce anche la sua più grande fragilità in quanto frammenta i punti di accesso di un sistema unitario. L'insicurezza di un dispositivo rende egualmente insicuro tutto il complesso poiché sarà quella, la porta utilizzata dall'hacker per intrufolarsi all'interno.

Secondo quanto viene riferito da Itai Kranz, esperto di design tra le fila dei Google da quasi venti anni, "non solo l'IoT connette molte cose prima non connesse all'interno delle imprese, ma porta con sé l'integrazione tra IT[195] e OT[196]. Questo significa che i cybercriminali iniziano a indirizzare i propri sforzi verso il sabotaggio o la presa di controllo dei singoli dispositivi o dei sistemi OT che controllano gli apparati e le infrastrutture critiche", evidenziando che già nel 2016 si fosse segnalato un aumento del 110 per cento di queste nuove tecniche di *cyber* attacchi.

Il Gruppo di lavoro articolo 29 ha analizzato nel 2014, con il parere numero 8, ("*Opinion on Recent Developments on the Internet of Things*"), le problematiche del settore, sottolineandone le fragilità. Sicuramente tale Opinione risulta parecchio datata ma le preoccupazioni espresse dal WP29 rimangono più che attuali[197].

195 "IT" o "*Information Tecnology*", in italiano tecnologia informtiva, concerne quell'insieme di tenciche di trasferimento ed elaborazione di informazione.

196 "OT" o "*Operational Tecnology*", in italiano tecnologia operativa attiene invece alle metodologie che consentono di passare dall'informazione ad un'attività che abbia effetti sul mondo reale rimuovendo il filtro umano tra informazione e azione.

197 Letteralmente*: "Data losses, infection by malware, but also unauthorized access to personal data, intrusive use of wearable devices, or unlawful surveillance are as many risks that stakeholders in the IoT must address to attract prospective end-users of their products or services. [… The IoT raises several security challenges, namely as security and resource constraints force device manufacturers to balance battery efficiency and device security. In particular, it is not yet clear how device manufacturers will balance the implementation of confidentiality, integrity and availability measures at all levels of the*

In particolare, afferma che la vulnerabilità e l'appetibilità dei dispositivi IoT rispetto ad attacchi informatici può comportare numerosissimi rischi ed è divenuta, nel tempo, un'importante sfida per i programmatori poiché le misure di sicurezza in questi casi non devono essere solo adeguati ai rischi ma vanno anche bilanciati alle più limitate capacità computazionali dei dispositivi ed eventualmente con i livelli di consumo della batteria.

Le strategie di sicurezza nell'IoT, in generale, fanno riferimento ad una serie di passaggi irrinunciabili per garantire ambienti di comunicazione protetti. Il primo step sicuramente attiene all''autenticazione dei *devices* IoT, tale che ogni dispositivo che vuole comunicare con il sistema deve essere preventivamente autenticato e autorizzato a farlo. Sulla base di ciò si potrebbe andare anche a segmentare il ventaglio di azioni e di accesso che ogni dispositivo può compiere con il sistema, limitando da un lato le funzioni dell'apparecchio ma dall'altro inibendo le azioni dell'attaccante che si impossessi dello stesso.

Il secondo passaggio invece attiene alle misure di sicurezza "proprie", cioè quelle "misure tecniche e organizzative" che vengono definite dall'articolo 32, come ad esempio la cifratura, le quali consentono di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità" dei dati. Queste sono una necessità sia per i dati contenuti nei singoli dispositivi IoT sia per quelli contenuti del sistema nel suo complesso.

Il tutto deve poi essere supportato da adeguati software finalizzati all'analisi delle possibili minaccie, fornendo delle piattaforme di visualizzazione delle criticità e dei tentativi di sabotaggio all'operatore umano per consenitre un costante monitoraggio di tutto il sistema.

Da ultimo, un buon livello di sicurezza conta necessariamente sull'aggiornamento periodico delle tecniche e dei software impiegati, in quanto anche le tecniche invasive ed i malware si aggiornano ed evolvono giorno dopo giorno: anche qui, se alcune parti non vengono aggiornate puntualmente, si rischia di lasciare un varco aperto agli attaccanti.

3.3. Obbligo di notifica all'autorità di controllo in caso di violazione dei dati personali.

Sempre nella sezione relativa alla sicurezza dei dati, cioè la seconda sezione del IV Capo, sono contenute altre due norme, relative all'obbligo di notifica in capo al titolare in caso di violazione dei dati (cd *Data Breach Notification*)

L'articolo 33, in particolare, prevede che "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità di Controllo [...] senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza."

Il termine breve di 72 ore ha un'importanza fondamentale in quanto, l'Autorità di Controllo deve attivarsi nel minor tempo possibile per limitare, con la collaborazione del titolare, i danni derivanti dalla

processing sequence with the need to optimise the use of computational resources – and energy – by objects and sensors."

violazione. Ciò spiega anche l'onere probatorio posto a carico del titolare dall'ultimo periodo del primo paragrafo dell'articolo 33. secondo cui "qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo."

Tuttavia, come abbiamo osservato nel paragrafo precedente, gli attacchi informatici sono sempre più frequenti e una puntuale comunicazione all'Autorità di controllo di ogni violazione e minaccia determinerebbe una paralisi della sua attività. Proprio per questo motivo viene omesso l'obbligo di notificazione nei casi in cui sia "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche."

Per far sorgere l'obbligo della *Data Breach Notification* quindi si richiede non solo che l'attacco informatico sia andato a buon fine ma il titolare deve anche valutare, sotto la sua diretta responsabilità, se le conseguenze dell'attacco possano ripercutersi direttamente sui diritti fondamentali degli individui dei cui dati si tratta. È evidente che qualora siano violati categorie di dati, diverse da quella dei dati personali, non sussistono rischi per le libertà delle persone fisiche e di conseguenza l'obbligo di notifica non sussiste[198]: questa posizione è esplicitamente confermata dal WP29 nelle *Guidelines.on Personal Data Breach Notification on Personal Data*.

L'obbligo di notificazione all'Autorità di controllo ha due finalità, la prima mira alla tutela delle persone fisiche in quanto si richiede che l'Autorità impartisca al titolare ordini e istruzioni per limitare i danni derivanti ai diritti dell'individuo e chiudere le falle del sistema per il futuro mentre la seconda finalità, di ordine pubblicistico, attiene a verificare l'adeguatezza delle misure di sicurezza poste dal titolare prima dell'attacco così da evidernziarne le eventuali responsabilità.

La soggezione dell'obbligo di notificazione alle sole violazioni che presentino elevati livelli di pericolosità sociale, giustifica anche l'articolato apparato sanzionatorio di cui l'Autorità dispone.

Rispetto al contenuto della notificazione soccorre il paragrafi 3 dell'articolo 33, il quale prevede una serie di informazioni che devono essere obbligatoriamente fornite all'Autorità idonee a "descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione", a "descrivere le probabili conseguenze della violazione", a descrivere inoltre "le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

Il titolare deve altresì comunicare i dati identificativi del *DPO* o di "altro eventuale punto di contatto presso cui ottenere più informazioni" ma viene anche aggiunto, nel quarto paragrafo, che qualora non sia possibile fornire contestualmente tutte o parte delle informazioni, le stesse possono essere recapitate all'Autorità di Controllo nelle fasi successive senza comunque ingiustificato ritardo".

198 Tuttavia, nelle violazioni di sistemi di Intelligenza Artificiale o *Big Data*, risulta particolarmente complicato escludere che non siano stati oggetto di attacco dei dati personali e ciò potrebbe determinare un accumulo di lavoro per le Autorità di Controllo ma sembra il giusto prezzo da pagare per un controllo pubblicistico in questa delicato settore.

Nonostante il GDPR consenta di prorogare il termine di 72 ore qualora non sia possibile al titolare di fornire contestualmente le informazioni necessarie all'Autorità, salvo però che alleghi i motivi del ritardo per evitare di incorrere in responsabilità, risulta difficile che un ritardo possa verificarsi in concreto. Ciò a causa del quinto paragrafo dell'articolo 33 che impone al titolare un puntuale obbligo di documentazione.

Ciò che deve essere documentato dal titolare o dal responsabile, se nominato, attiene ad ogni attività relativa alla "violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio."

Tuttavia la finalità della norma non è fondamentale solo per consentire al titolare l'adempimento degli obblighi di notificazione ma anche e sopratutto per permettere un'eventuale esonero delle sue responsabilità qualora dovesse giustificare il suo operato in contraddittorio con l'Autorità. Questa è la doppia finalità che si evince dall'interpretazione dell'ultimo periodo dello stesso paragrafo 5, articolo 33, secondo cui "Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."

D'altronde questa duplicità di fini deriva proprio dal doppio ruolo che riveste l'Autorità nel caso di una *Data Breach Notification*: da un lato va a supportare tempestivamente l'attività del titolare per trovare soluzioni idonee a limitare le conseguenza che un attacco informatico può avere sulle persone fisiche ma dall'altro deve mettere in luce le eventuali responsabilità del titolare per non aver assicurato un'adeguata protezione alle sue attività di trattamento e quindi infrangendo le norme dettate dal GDPR.

3.4. Obbligo di notifica all'Interessato in caso di violazione dei dati personali.

A norma dell'articolo 34, l'obbligo del titolare di notificare la violazione di dati personale si estende, sotto certe condizioni, anche a favore dell'interessato.

La condizione che fa scattare l'obbligo di informare "senza ritardo" anche gli interessati, è contenuta nel primo paragrafo, il quale richede che la "violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Come nel caso della notifica alle Autorità di Controllo, anche in questa circostanza, la presenza di rischi elevati è valutata direttamente dal titolare sotto la sua responsabilità ma stavolta può accadere che il titolare venga intimato a fornire tale comunicazione.

In particolare il paragrafo 4 prevede cbe qualora "il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali[199], l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che" sia presente una delle circostanze elencate nel paragrafo 3, le quali fanno cadere l'obbligo di

199 Secondo l'interpretazione più coerente della norma, vi rientra sicuramente il caso in cui il titolare non solo non abbia ancora dato la comunicazione ma che non intenda farlo nemmeno in un momento futuro.

comunicazione.

L'Autorità che viene resa edotta della violazione dal parte del titolare, sulla base dell'articolo 33, può o supportare la sua valutazione circa la natura e l'entità del rischio oppure può discostarsene, qualificando il rischio come grave[200] ed imponendo che venga informato dell'evento anche l'interessato.

In riferimento al "rischio elevato" si deve notare che non va ricollegato ad un rischio che grava non solo individualmente sui singoli interessati[201] ma va osservato nel complesso degli stessi con parametri oggettivi come ad esempio la quantità e natura dei dati violati o l'ampiezza geografica dei trattamenti oppure il numero di interessati coinvolti etc.

In merito al contenuto della comunicazione agli interessati, va osservato come il seconda paragrafo dell'articolo 34, effettui un richiamo integrale almeno ai contenuti che devono necessariamente essere presenti alla notificazione alle Autorità di Controllo. In particolare: "La comunicazione all'interessato [...] descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)."

Nonostante le due diverse comunicazioni abbiano un contenuto minimo ed indispensabile comune, hanno effetti totalmente diversi: la notificazione all'Autorità assolve anche ad una funzione pubblicistica come si è visto[202] e può essere omessa solo qualora non risulti un rischio per i dati personali dalla violazione.

Nel caso della notificazione all'interessato, assolvendo esclusivamente la funzione di rendere la violazione nota alle persone fisiche così da permetterle di porre in essere i rimedi necessari[203], la norma permette di omettere l'informativa in una serie di casi.

In particolare il terzo comma dell'articolo 34 prevede che "Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura"[204] oppure nel caso in cui "il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati" e da ultimo qualora "detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia."[205]

200 Ovviamente sulla base di sue ulteriori attività valutative compiute dopo aver svolto accertamenti sull'attacco di cui ha avuto notizia.

201 Sul punto è si espresso molto chiaramente il WP29, il quale, nelle "Linee Guida sulla Notificazione della Violazione dei Dati Personali" prevede che la comunicazione va effettuata anche nel caso in cui dei rischi elevati corrano solo per un signolo interessato.

202 A tal proposito rimando alla lettura del paragrafo prcedente.

203 Ad esempio se oggetto di furto di un attacco informatico sono i dati relativi alle carte di credito degli interessati, questi, resi consapevoli della violazione, possono richiederne il blocco presso la banca che offre il servizio.

204 In questo caso, l'interessato non potrebbe comunque porre in essere azioni ulteriori a tutela della sua posizione: il titolare ha già adeguatamente protetto i suoi dati ed i suoi diritti e libertà non corrono rischi.

205 In questa circostanza invece la finalità della norma è quella di non aggravare eccessivamente gli oneri posti in capo al titolare,

Le ragioni principali su cui si basa l'esonero della comunicazione sono rintracciabili sia nel timore sociale che potrebbe derivare da un attacco che tuttavia non genererà più rischi per diritti e libertà dei soggetti, generando inutile sfiducia nei consocitati ma anche per evitare un danno grave reputazionale che deriverebbe all'imoresa dalla comunicazione pubblica della notizia.

Il legislatore ha inteso quindi trovare un delicato equilibrio tra queste necessità, circoscrivendo le ipotesi della comunicazione agli interessati solo nei casi di gravi rischi per le loro diritti e libertà, derivanti dall'attacco informatico, e solo se il titolare non si sia ancora attivato per porri in essere le misure idonee a scongiurarne gli effetti negativi.

4. Gli strumenti di semplificazione previsti dal GDPR.

Si configura così uno scenario davvero articolato che si complica al complicarsi delle specificità delle attività di trattamento garantendo un equilibrio per tutto il sistema così da lasciare senza oneri eccessivi le "piccole attività" ma allo stesso tempo irrobustendo le tutele e le garanzie necessarie per quei trattamenti che presentino dei rischi, sulla base dei più disparati fattori.

Le competenze richieste per porre il sistema in sicurezza possono arrivare ad essere talmente tecniche da richiedere il supporto di figure ulteriori quali il *DPO* o il responsabile per evitare di violare le norme fissate dal regolamento e cadere così in responsabilità per il suo operato.

Il Regolamento, per evitare una paralisi del sistema, ha previsto anche due strumenti di semplificazione sfruttabili in tutti quei casi in cui il trattamento superi determinate soglie di complessità[206] per garantire in ogni momento l'aderenza dell'attività alle norme del GDPR.

Il modello di semplificazione si concretizza sui principi dell'etica dell'impresa o del software, a seconda del momento in cui le soluzioni in questione vengono integrate nell'attività del titolare.

L'ingresso della dimensione etica nel settore produce come diretta conseguenza un incremento dell'accountability per il titolare in cambio di una minore regolazione della sua attività: l'assunsione di impegtni etici è idonea a garantire una tutela anche oltre la rigida applicazione delle norme del GDPR.

Sulla base dell'analisi fin qui svolta, si notano fin da subito le potenzialità di questi strumenti nella dimensione delle IA e dei dispositivi appartenenti all'IoT in quanto è proprio l'automatismo delle loro attività di trattamento che fa sorgere un impegno maggiore sia per i titolari che per i programmatori dei dispositivi al fine di garantire che il loro comportamento sia basato su algoritmi etici idonei al rispetto della vita[207], dei

consentendo una via più pratica per informare tutti le persone fisiche con un'unica azione.

206 In realtà tali strumenti sono fruibili da ogni titolare e per ogni attività di trattamento ma si noti che nel caso in cui un trattamento sia particolarmente articolato tali strumenti di semplificazione diventano quasi una necessità.

207 L'elaborazione degli algoritmi di comportamento etico fondati sul rispetto della vita umana è uno dei punti più importanti nello sviluppo di un'IA e uno dei più risalenti. Già nel 1942 lo scrittore Isaac Asimov nel suo racconto, *Circolo vizioso*,

diritti e delle libertà fondamentale dell'uomo.

Gli strumenti in questione vengono definiti nella quinta Sezione, relativa alla responsabilità del titolare, del IV Capo del GDPR e sono i Codici di Condotta e le Certificazioni.

Si tratta di strumenti con caratteristiche e funzioni diverse tra loro ma presentano due punti di contatto rispetto ai fini che si pongono di ottenere. Il primo attiene alla flessibilità con cui le imprese e le organizzazioni possono risultare *compliant* (rispettosi) al Regolamento, potendo ritagliare solo le misure idonee e necessarie a garantire gli *standard* adeguati di sicurezza.

Il secondo profilo in comune attiene al profondo rapporto che si va ad instaurare tra impresa/organizzazione e l'Autorità di Controllo finalizzato a garantire preventivamente che le attivitò di trattamento siano lecite e sicure. Tale rapporto non può assimilarsi alla consultazione preventiva *ex* articolo 36[208], con cui sicuramente ne condivide parzialmente le finalità, in quanto tale rapporto si instaura anche a prescindere da una valutazione sui rischi e non si esaurisce in un singolo colloquio ma mira ad integrare un dialogo continuativo tra i due soggetti per tutta la durata delle attività di trattamento.

Visti gli obiettivi comuni di tali strumenti di semplificazione, andiamo ora ad analizzare individualmente le potenzialità che i singoli strumenti possono presentare, sopratutto con riferimento all'epoca di trattamenti di dati complicati dall'intervento di Macchine Intelligenti e dispositivi IoT.

4.1. I Codici di Condotta.

I codici di condotta si concretizzano in una serie di regole di condotta o pratiche uniformi elaborate da organismi di varia natura sia Internazionali, regionali, statali oppure anche privati, particolarmente diffuse e garantiste dei diritti delle persone fisiche. Si tratta comunque di disposizioni non obbligatorie in generale ma devono essere specificatamente accettati per divenire giuridicamente vincolanti anche se l'autorevolezza dell'organismo da cui provengono potrebbe comportare che siano di larga applicazione.

I codici di condotta non costituiscono una vera novità in quanto sono stati previsti in Italia, nel campo della protezione dei dati personali, già dalla legge 675/96[209] in sede di recepimento della Direttiva 95/46/CE.

Il Regolamento Europeo n. 679/2016 continua l'incoraggiamento all'utilizzo dei codici di condotta, mutandone conformazione e finalità per meglio adattarla al nuovo contesto economico, tecnologico e sociale

descrive gli imprevisti cui si potrebbe arrivare se una macchina robotica non sia dotata di particolari regole relazionali che intercorrono tra il suo agire e la vita umana. Asimov racchiude tali regole in tre postulati, divenuti oggi le tre leggi fondamentali della robotica. In particolare: "Un robot non può recare danno a un essere umano, né può permettere che, a causa del proprio mancato intervento, un essere umano riceva un danno". Inotre "Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge." Da ultimo, "Un robot deve proteggere la propria esistenza, purché tale autodifesa non contrasti con la Prima o con la Seconda Legge."

208 Attraverso cui si prevede che "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio."

209 In particolare all'art. 31, comma 1, lett. h), e poi è stato ripreso nel D.lgs. n. 196/2003 dall'art. 12.

intervenuto nel tempo.

Il GDPR sembra accordate a tale strumento un ruolo molto più incisivo rispetto al passato e ciò è riscontrabile già dall'art. 40 il quale sancisce che "gli Stati membri, le Autorità di Controllo[210], il Comitato europeo per la protezione dei dati[211] e la Commissione[212] incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese."

Ma quelli descritti nel primo paragrefo non sono gli unici soggetti legittimati a poter elaborare o modificare dei Codici di Condotto perchè, secondo il quinto paragrefo, sono abilitati anche "le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento" ma con dei limiti.

Infatti, qualora "intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate."

In questa circostanza infatti è necessario un controllo pubblicistico preventivo dell'Autorità che assicuri la coerenza del codice ai principi dettati dal Regolamento Europeo così da evitare che uno strumento di flessibilità possa divenire un mezzo di elusione della legge.

La lettura dell'articolo 40 va poi integrata dal dettame del Considerando 98, il quale specifica chiaramente le finalità dei Codici.

Non solo si precisa che l'incoraggiamento delle istituzioni pubbliche all'adozione dei codici di condotta deve comunque avvenire "nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori" ma si consenta altresì che "tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche."

Ciò che emerge con chiarezza è che il punto su cui dovrà ruotare tutto il Codice di condotta sarà comunque il GDPR: si possono "calibrare" gli obblighi di tutela sulla base delle specificità del trattamento, rafforzando le parti più "fragili" dell'attività ma non si potranno andare ad ignorare gli altri obblighi negli altri settori dell'attività più sicuri.

In termini tecnici, il Codice di Condotta non potrà mai accogliere interpretazioni o applicazioni delle norme del GDPR che modifichino *in peius* l'efficacia di queste ultime, al contrario saranno ammesse quelle che innalzino il livello di effettività delle disposizioni nei settori che richiedono una specifica sorveglianza

210 Come d'altronde risulta chiaramente dalla dizione dell'articolo 57, paragrafo 1, lettera m).
211 In particolare tale potere viene esplicitato nell'articolo 70, paragrafo 1, lettera n).
212 Va sottolineato che gli Stati Membri e la Commissione in materia, siano dotati di poteri maggiori rispetto a quelli stabiliti dal GDPR considerando la posizione che ricoprono.

per consentire una maggiore tutela di diritti e libertà delle persone fisiche.

Questo strumento ponendo come suo centro i concetti di specificità e innalzamento della tutela e data la sua estrema malleabilità, è uno dei ponti che in futuro potrebbe effettivamente consentire l'ingresso all'interno del tessuto sociale di ogni tecnologia che sarà sviluppata: ogni nuova esigenza potra essere adeguatamente affrontata attraverso un Codice e la sua aderenza al Regolamento è garantita dall'Autorità.

4.2. *Segue*: Finalità e limiti all'adozione dei Codici di Condotta.

La possibilità di poter predeterminare il contenuto di questi Codici, non è senza limiti e sicuramente il vincolo più grande attiene al rispetto delle norme e dei principi enunciati dal GDPR

Per garantire tale aderenza, il secondo paragrafo dell'articolo 40 elenca una serie di finalità che devono essere seguite nell'adozione di questi Codici e nello specifico si prescrive che tali codici debbano essere elaborati, modificati o prorogati, "allo scopo di precisare l'applicazione delle disposizioni del Regolamento, ad esempio:

a) il trattamento corretto e trasparente dei dati;

b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

c) la raccolta dei dati personali;

d) la pseudonimizzazione dei dati personali;

e) l'informazione fornita al pubblico e agli interessati;

f) l'esercizio dei diritti degli interessati;

g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;

h) le misure e le procedure di cui agli articoli 24 e 25 del GDPR e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;

i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;

j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;

k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79 del GDPR."

L'ampiezza delle finalità che vanno perseguite dai Codici di condotta ricalca quelle del Regolamento e delinea una serie di garanzie minime che vanno accordate così da permettere che questi strumenti riescano efficacemente a gestire l'attività dei titolari.

Lo scopo specifico della puntualità che caratterizza la norma è appunto quello di consentire una legislazione parallela per ogni specificità di trattamento così da frammentare le modalità con cui perseguire uno stesso fine. Le modalità di scrittura degli algoritmi, le capacità di legare insieme tecniche cognitive di un

elaboratore o anche solo la modalità di legare insieme più fasi o anelli di uno stesso trattamento variano da programmatore a programmatore, a seconda delle sue competenze o semplicemente dal suo modo personale di approcciarsi ai problemi della vita e questi Codici di codotta permettono di tenere conto di questo fattore umano.

Ogni programmatore o titolare, potrà così mantenere il suo "stile" personale nella progettazione di un trattamento, a patto che riesca ad irrobustire, eventualmente con l'aiuto delle Autorità nazionali, tutti i punti speficicati dal secondo paragrafo dell'articolo 40, di modo che la tutela sia almeno pari a quella accordata dal GDPR.

La flessibilità che permette ai titolari di predisporre normative settoriali soecificate e dizzerenziate, risulta così incanalata verso margini invalicabili ben definiti dal secondo paragrafo.

Tutto ciò è possibile anche grazie alle modalità di adozione dei codici a cui sono dedicati molti paragrafi dell'articolo 40. Il quinto paragrafo introduce la disciplina sancendo che "Le associazioni e gli altri organismi che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate."

È l'Autorità[213] quindi l'unico organo competente ad assicurare che il codice di condotta sia *compliant* con il Regolamento e questo deve avvenire prima che lo stesso sia adottato così da prevenire ogni minimo rischio potenziale.

A seguito della proposta e della successiva approvazione da parte dell'Autorità di Controllo l'*iter* del codice si biforca: se il codice dovrà essere applicato a trattamenti che avvengono esclusivamente sul territorio di uno Stato Membro[214] allore l'Autorità registra e pubblica il codice, divenendo così efficace e vincolante per il proponente ed eventualmente per lo abbia sottoscritto o vi abbia aderito.

Nel caso in cui le attività di trattamento avvengano sul territorio di "vari Stati Membri", il settimo paragrafo si preccupa di stabilire che "prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 lo sottopone […] al comitato, il quale formula un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie."

In questo caso, l'obiettivo del legislatore è quello di garantire, ad un livello superiore, la conformità del Codice sia al Regolamento che alle singole normative nazionali degli Stati interessati. Ad analogo fine si sarebbe potuto arrivare trasmettendo la proposta ad ogni singola Autorità di Controllo degli Stati interessati dal trattamento ma si è inteso evitare il rallentamento del sistema o eventuali giochi di forza, centralizzando la procedura a livello Europeo.

213 L'Autorità competente ai sensi dell'articolo 55 è quella dello Stato nel cui territorio è basata la sede legate dell'associazione o dell'organizzazione che presenta il progetto di Codice.

214 Testualmente "se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri."

Il parere del Comitato Europeo per la Protezione dei Dati è vincolante, tuttavia non è finalizzato all'approvazione finale del Codice in quanto questa spetta solo, a norma del paragrafo 8 dell'articolo 40, alla Commissione, cui deve essere trasferito il testo del Codice. Questa, può stabilire, "mediante atti di esecuzione", della validità del codice ad effetto generale all'interno di tutto il territorio dell'Unione e contestualmente ne deve "dare un'adeguata pubblicità dei codici approvati."[215]

Da ultimo, si prevede che i testi approvati dalla Commissione vengano poi ritrasferiti al Comitato Europeo, così che possano essere contenuti "in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati."

Tutto il sistema si chiude poi con il disposto del quarto paragrafo dell'articolo 40 il quale richiede che il codice di condotta di cui al paragrafo 2 contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1[216], di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo."

4.3. Le Certificazioni, i Marchi ed i Sigilli.

Il secondo strumento di semplificazione incoraggiato dalle istituzioni Nazionali ed Europee, "Stati Membri, Autorità di Controllo, Comitato e Commissione", si concretizza nei meccanismi di Certificazione della protezione dei dati, compresi i marchi e sigilli.

Nonostante le profonde analogie con i Codici di Condotta, va notato fin da subito come queste due tecniche siano tenute ben distinte dal GDPR in quanto mirano a raggiungere un medesimo fine, la semplificazione, con tecniche specifiche.

Già a prima lettura dell'articolo 42, primo paragrafo, si può notare come gli strumenti di certificazione, per quanto vadano a tutelare le esigenze anche dalle micro imprese, mirano, ad assumere una dimensione più generale, Europea. La norma infatti pone che "Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese."

Le Certificazioni possono essere rilasciate anche per singole attività di trattamento sia dalle Autorità nazionali che da meccanismi di certificazione abilitati allo scopo mentre appare, dal quinto paragrafo dell'artioco 42, che i sigilli ed i machi possano avere esclusivamente una dimensione Europea e generale

215 Seconto il disposto del decimo paragrafo dell'articolo $0 GDPR.

216 Specificatamente "Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente." Ciò per evitare che sia sempre un affaticamento del ruolo dell'Autorità nella fase di monitoraggio.

anche se la dizione della norma non risulta priva di incertezze sul punto[217].

L'aspetto che differenzia maggiormente i Codici e le Certificazioni è ravvisabile nelle finalità che i due strumenti si pongono: il primo mira ad adattare le norme del trattamento al fine di meglio gestire le specificità dei trattamenti ed innalzare il grado di tutela per diritti e libertà degli interessati mentre le certificazioni, i sigilli ed i marchi mirano esclusivamente a dimostrare la conformità dell'attività di trattamento alle norme del GDPR, senza definire modalità differenziate di applicazione dello stesso.

Lo scopo delle Certificazioni però non è quello di esimere la responsabilità del titolare e del responsabile rispetto le loro attività di trattamento, rimanendo impregiudicati sia i loro doveri che i poteri dell'Autorità di Controllo sugli stessi[218] ma lo scopo ultimo è quello di dare idonea garanzia ad i terzi circa la legittimità dei trattamenti effettuati, garantendo anche che siano adeguate e sicure le tecnologie impiegate o le misure organizzative disposte a difesa di eventuali attacchi informativi o guasti tecnici.

La Certificazione, nonché i marchi ed i sigilli, conferiscono una garanzia verso i terzi che le attività di trattamento cui saranno soggetti siano conformi alle disposizione sulla protezione dei dati personali e allo stesso tempo permettono al titolare o al responsabile di assolvere l'onere probatorio di dimostrare di aver posto in essere tutto ciò che era necessario per garantire un adeguata tutela delle persone fisiche.

Le modalità con cui una Certificazione diviene efficace nei confronti di un titolare inoltre è molto più semplice: non tenendo conto delle specificità del trattamento non è richiesto uno strumento che caso per caso deve essere rielaborato o modificato dal titolare con conseguente controllo di conformità dell'Autorità ma semplicemente si prescrive al terzo paragrafo che “La certificazione è volontaria e accessibile” e per renderla vincolante è succiciente un atto di adesione alla stessa.

Al momento in cui l'adesione viene inoltrata, si prevede inoltre che il titolare del trattamento o il responsabile forniscano al meccanismo di certificazione o, nel caso, all'autorità di controllo competente, “tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.”

Ciò che rileva è che anche in questa circostanza si instaura un rapporto tra il titolare o il responsabile e l'organismo autorizzato al rilascio di meccanismi di certificazione finalizzato principalmente ad un controllo preventivo di aderenza tra la sua attività di trattamento ed i requisiti necessari per ottenere le agevolazioni derivanti dalle Certificazioni, dai marchi o dai sigilli.

Tuttavia non si tratta esclusivamente di un controllo preventivo ma si instaura un vero e proprio rapporto di fiducia continuativo in quanto se da un lato il primo periodo del settimo paragrafo dell'articolo 42

217 La dizione della norma letteralmente prevede che “La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.”

218 A tale proposito il paragrafo quattro dell'articolo 42 dispone che “La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.”

specifica che le Certificazioni sono rilasciate "per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti", il secondo periodo, prontamente specifica tuttavia che "la certificazione è revocata, se del caso, dagli organismi di certificazione o dall'autorità di controllo competente, qualora non siano o non siano più soddisfatti i requisiti per la certificazione."

La garanzia di idonea tutela non è un requisito necessario "*una tantum"* ma deve perdurare finchè perdura il meccanismo di certificazione altrimenti di rischia la revoca dello stesso.

Infine per permettere una massima trasparenza e centralizzazione di tutto il sistema di Certificazione, si prevede al sesto comma che il Comitato Europeo per la Protezione dei Dati, rediga un apposito registro dove siano iscritti, sia tutti i meccanismi di Certificazione rilasciati o approvati a livello Nazionale che i marchi ed i sigilli rilasciati a livello Europeo e destinati ad avere uniforme applicazione su tutto il territorio dell'Unione[219].

4.4. *Segue*: Il ruolo della Commissione rispetto ai meccanismi di Certificazione.

Il ruolo della Commissione all'interno del settore dei meccanismi di Certificazione ha un'importanza ed un 'incisività davvero importante, sopratutto nell'ottica delle IA e dei dispositivi IoT.

I paragrafi 8 e 9 dell'articolo 43 delineano due poteri in capo alla Commissione, rispettivamente "il potere di adottare atti delegati al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati" e il potere di "stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi."

Sembrano poteri di indirizzo molto blandi ma va ricordato che l'impiego dei poteri da parte della Commissione ha, per natura, effetti su tutto il territorio dell'Unione.

Si concentra così ad un livello più alto ed essenzialmente politico, la possibilità di indirizzare le attività degli organismi di certificazione al fine, da un lato di "precisare i requisiti" e quindi di specificare le garanzie che vanno offerte alle persone fisiche per ottenere una Certificazione ma dall'altro deve "stabilire norme tecniche" e quindi deve considerare le criticità che sorgono anche dall'impiego delle nuove tecnologie, prime tra tutte quelle Intelligenti.

Tutto ciò è sempre legato ad una coerenza di fondo di tutto il GDPR ai fini che si pone nel primo articolo, consentendo anche a livello politico[220] e generale la tutela dei diritti e delle libertà delle persone

219 A tale proposito il nono paragrafo dell'articolo 43 prevede che: "La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati."

220 Ovviamente, il livello politico, riveste sempre un ruolo chiave e fondamentale nella scelta dell'impiego delle nuove misure

fisiche e la libera circolazione dei dati personali.

Occorre infatti ricordare ancora una volta, prima di chiudere la trattazione del tema che gli obiettivi del nuovo Regolamento sono ambizioni e richiedono l'intervento di soggetti sia privati che pubblici affinchè possano essere realmente raggiunti ed inoltre serve il maggior grado di collaborazione ad ogni livello, sia esso tecnico, politico o giuridico, per intraprendere una direzione unica e sicura tale da consentire l'ingresso delle nuove tecnologie.

Il GDPR non si pone con timore dinnanzi al futuro ma anzi riconosce che "la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali"[221] ed ha deciso di affrontare tali sfide offrendo un elevato numero di soluzioni che i titolari possono sfuttare, comprese le più "creative", ma sempre entro il limite dei principi fissati nel Regolamento e sotto la stretta osservanza di Autorità specialistiche o politiche sia Europee che Nazionali.

tecnologiche alle attività di trattamento e al tessuto sociale in generale tale che il GDPR ha voluto porre un meccanismo di raccordo tra le attività "innovative" delle Autorità di Controllo specializzate, sia Nazionali che Eutopee e le attività "innovative" dell'organi politico Europeo.

221 Come si rileva nel primo periodo del sesto Considerando.

Conclusioni

I dati personali sono una nuova categoria di beni che negli ultimi tempi sono stati al centro di numerose questioni. Molti scandali recenti si sono generati proprio dall'incorretto uso di questi dati ma allo stesso tempo sono stati il motore del progresso tecnologico.

Dallo scandalo di Cambridge Analytics al bosone di Higgs, sembra proprio che si configuri un contesto dove il progresso non possa avvenire senza perdere una fetta importante dei nostri diritti ed è proprio su questa base che si fonda la sfida legislativa sia a livello Europeo che Nazionale.

La crescita tecnologica e l'incremento della quantità di informazioni che si sono generati nei sistemi informatici, ha tuttavia sottolineato i limiti delle precedenti normative che regolavano il settore. Risultano mutate le esigenze conseguenti alla raccolta e l'impiego di dati divenendo un bene diffusamente commercializzato in modo autonomo e suscettibili di valutazione economica.

La *DG Connect,* l'organo che si occupa di monitorare il mercato europeo delle comunicazioni, ha rilevato che solo nel 2016 il settore dati, ha visto circa 60 miliardi di euro, e nel giro di un triennio potrebbe raggiungere quota 100 miliardi.

L'interesse nel mercato di questo bene, ne ha comportato una raccolta sempre più spietata, con tecniche sempre più raffinate. Il progresso tecnologico infatti ha portato, al giorno d'oggi, un'ulteriore sviluppo nell'uso di Internet e di conseguenza di raccolta dei dati. Non è più solo la nostra attività diretta sul Web a generare informazioni, come ad esempio i *post* su Facebook, le ricerche in Internet o i servizi richiesti *online* ma anche i nostri dispositivi, autonomamente, sono in grado di accedere alla rete per ricercare o comunicare informazioni al sistema sfuggendo, di conseguenza, al nostro diretto controllo.

La vera motivazione che sottende questo florido sviluppo del mercato dei dati personali, è fortemente legato alle nuove tecnologie che si stanno immettendo nel mercato. Le capacità logiche degli elaboratori riescono a lavorare su queste grandi quantità di contenuti, arrivando a stabilire delle informazioni di fondamentale importanza. Si parla spesso sul tema di "*dati dai dati*" proprio per questa capacità di ritrovare le associazioni nascoste che intercorrono tra le grandi quantità di informazioni già in nostro possesso. *Machine Learning*, Reti Neurali e *Big Data* sono solo esempi di queste nuove metodologie informatiche di ricerca ed elaborazione.

Precedentemente la materia era regolata, a livello Europeo, dalla Direttiva 45/96, la quale mirava ad armonizzare le discipline nazionali al fine di tutelare i diritti delle persone e per consentire la libera circolazione dei dati. Tuttavia nel 1996 non si poteva prevedere una rivoluzione informatica di questa portata, infatti la libera circolazione delle informazioni personali assumeva solamente un ruolo ancillare, in quanto la loro circolazione veniva considerata e garantita solo in relazione alle altre libertà fondamentali del mercato interno dell'Unione.

In particolare il Considerando numero 3 prevedeva che "[nel]l'instaurazione e il funzionamento del

mercato interno, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona"

Già da questa unica considerazione si può comprendere il motivo che ha portato la Direttiva a sfumare in un solo ventennio, non era in grado di favorire un vero sviluppo uniforme del mercato interno ed allo stesso tempo non era in grado di gestire le attuali e più complicate tecniche di trattamento.

Le istituzioni Europee hanno risposto a queste nuove esigenze, introducendo uno strumento legislativo in grado, non solo di considerare tutti questi nuovi sviluppi tecnologici e sociali ma anche di predisporre le basi per gestire quelli futuri, tale strumento è il Regolamento 679/2016.

Il Regolamento, come strumento legislativo, ha la capacità di essere direttamente vincolante per tutti gli Stati Membri dell'Unione, creando una disciplina uniforme e fornendo certezza giuridica a tutto il sistema a differenza della Direttiva che consentiva discipline differenziate tra gli Stati seppur armonizzate sotto principi comuni.

Tale esigenza risulta chiaramente nel Considerando n. 8 del GDPR, il quale richiede che "il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri".

Le consapevolezza di questi mutamenti si concretizza nel Considerando 6 del Regolamento, dove si nota che "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuo,ve sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. Le attuali tecnologie consentono tanto alle imprese private quanto alle autorità pubbliche, di utilizzare dati personali come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."

Viene così riconosciuto il ruolo autonomo e centrale dei dati personali all'interno del mercato Europeo, facendo della sua libera circolazione il suo pilastro ma senza mai perdere di vista la tutela dei diritti e delle libertà delle persone fisiche. Tale sintesi tra libertà di circolazione e tutela dei diritti fondamentali, dovrebbe portare, come risultato, all'instaurazione di un clima di fiducia in tutta l'Unione.

Sul punto, il Considerando numero 7 prevede esplicitamente che "Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche."

Tutto il quadro normativo è stato così riformato in questa prospettiva ma è stato necessario, a tal fine,

riordinare i poteri e gli equilibri tra i soggetti principali di un'attività di trattamento. È stata rafforzata la posizione degli interessati ed agevolato l'esercizio dei loro diritti, vengono poi rimarcati ed ampliati gli obblighi del titolare in ordine alle sue attività e infine è stato irrobustito il ruolo di sorveglianza delle Autorità di Controllo Nazionali ed Europee.

Inoltre, la tecnica normativa del Regolamento non mira a definire pedissequamente le attività che intende regolare ma le individua in modo ampio, utilizzando un linguaggio neutrale così da intrappolare tra le maglie della norma il maggior numero di attività.

Il fulcro di tutto il sistema viene ad incentrarsi sulla posizione del Titolare del trattamento, sul quale grava l'obbligo generale del rispetto delle norme in materia, dovendo garantire e dimostrare sotto la sua responsabilità di aver posto in essere un trattamento lecito e sicuro.

La tecnica normativa neutra e la necessità di garantire sempre dei trattamenti leciti comporta la frammentazione delle attività di trattamento in vari livelli, i quali presentano caratteristiche e necessità diverse. In particolare il GDPR non ponendo limiti alle modalità con cui possono svolgersi le attività di trattamento, riconosce che questi possano presentare rischi e pericolosità differenziati a seconda delle strategie utilizzate o delle tecnologie impiegate. Di conseguenza stabilisce che siano adeguatamente considerate e valutate tali specificità dai titolari e che siano messe in sicurezza.

Il livello della sicurezza da predisporre al trattamento cresce progressivamente al crescere dei rischi che lo stesso presenta.

Dispositivi IoT che navigano e comunicano autonomamente nella rete dati personali o algoritmi di Data Analysis, che consentono di scoprire informazioni personali nuove ed ulteriori rispetto a quelle già a disposizione del titolare, possono così iniziare ad entrare nel sistema. Tanto da arrivare in un futuro a regolare l'attività totalmente indipendente di macchine robotiche intelligenti.

Tutto ciò ovviamente è in linea di massima solo prospettabile. La tecnica normativa neutra se da un lato ha il notevole vantaggio di aprire le porte al futuro, dall'altro richiede un'attività di adeguamento interpretativo delle norme che sia costante e coerente.

L'arduo compito di adeguare la tutela accordata dalle norme alle specifiche attività di trattamento, in particolar modo quando comportino gravi rischi per i diritti e libertà delle persone fisiche, è affidata alle Autorità di Controllo. Tali Autorità svolgono funzioni di monitoraggio sia preventivo che successivo alle attività sotto la loro sorveglianza.

Strategie di trattamento o l'impiego di *software* che non sono specificatamente regolati dalla normativa, possono essere comunque impiegati in vario modo dai titolari, se superano il vaglio di conformità al GDPR di tali organi. Il controllo di legittimità può riguardare sia singole attività di trattamento, attraverso le consultazioni preventive, che attività a livello generale, mediante i codici di condotta ed i meccanismi di certificazione.

In materia il meccanismo di coordinamento e coerenza riveste un ruolo di assoluta importanza in quanto deve legare le attività delle singole autorità di controllo nazionali, all'organo di controllo Europeo, il

Comitato per la Protezione dei Dati Personali, così da creare dei contesti normativi uniformi in tutta l'Unione seppure specializzati.

È proprio in questo scenario, che molti studiosi hanno elaborato delle possibili strategie per disciplinare il problema. Una tra queste si potrebbe incardinare nel concetto della responsabilità robotica legata alla personalità giuridica dei dispositivi Intelligenti. Altre vedono la soluzione nell'elaborazione di un etica dei robot attraverso cui si possono implementare algoritmi con regole di comportamento. Ulteriori strategie, invece, individuano nella nomina di un supervisore umano un modo per monitorare i trattamenti compiuti automaticamente dalla macchina.

In ogni caso si tratta di una serie di scenari molto interessanti ma il presente ed il futuro dell'ingresso di questi strumenti all'interno del sistema è ancora incerto, ed è legato al modo in cui le istituzioni Europee e Nazionali, decideranno di gestire e regolare le attività.

In ultima analisi, tutto dipenderà dalla loro prudente valutazione, sia come singole autorità competenti nel loro territorio sia come parte di un sistema centralizzato Europeo, così da permettere uno sviluppo omogeneo e costante in tutto il territorio.

In conclusione, nonostante le criticità rilevate e l'incertezza che caratterizza molte applicazioni pratiche del GDPR nel contesto delle nuove tecnologie, si rileva che le istituzioni europee hanno deciso di varare una riforma estremamente ambiziosa e impegnativa. Ciò è il risultato di un percorso molto travagliato, in cui si è tenuto conto dei successi ottenuti dalla Direttiva 46/95, preservandone e approfondendone i principi di fondo. Al contempo, vengono poi introdotte una serie di nuove norme, al fine di adattare la disciplina alle attuali mutate esigenze di tutela ed anche a quelle future che emergeranno nel contesto delle moderne tecnologie.

Bibliografia.

Asimov, I. (1950). *I, Robot.* Mondadori.

Bisol, B., Carnevale, A., & Lucivero, F. (2014). Diritti umani, valori e nuove tecnologie. Il caso dell'etica della robotica in Europa. *Metodo. International Studies in Phenomenology and Philosophy*, *2*(1).

Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*.

Bugliesi, M., Calzavara, S., Focardi, R., & Khan, W. (2015). CookiExt: Patching the browser against session hijacking attacks. *Journal of Computer Security*, *23*(4), 509-537.

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(2), 257-268.

Calzavara, S., Focardi, R., Squarcina, M., & Tempesta, M. (2017). Surviving the Web: A Journey into Web Session Security. *ACM Computing Surveys (CSUR)*, *50*(1), 13.

Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D. *Identity in the Information Society*, *3*(2), 247-251.

Chanana, A., Singh, S., & Paliwal, K. K. (2017, May). Malware detection using GA optimized K-means and HMM. In *Computing, Communication and Automation (ICCCA), 2017 International Conference on* (pp. 355-362). IEEE.

Chollet, F. (2017). *Deep learning with python*. Manning Publications Co..

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer law & security review*, *25*(2), 123-135.

Corradini, I. (Ed.). (2017). *Internet delle cose: Dati, sicurezza e reputazione*. FrancoAngeli.

Crockett, K., Goltz, S., & Garratt, M. (2018). "GDPR impact on computational intelligence research."

D'Acquisto, G., & Naldi, M. (2017). *Big Data e Privacy by design*(Vol. 5). G Giappichelli Editore.

D'Acquisto, G., Naldi, M., Bifulco, R., Pollicino, O., & Marco, B. (2018). *Intelligenza artificiale, protezione dei dati personali e regolazione* (Vol. 6). G Giappichelli Editore.

Daśko, N. (2018). General data protection regulation (GDPR) – revolution coming to european data protection laws in 2018. What's new for ordinary citizens? *Comparative Law Review, 23.*

Davenport, T. H. (2015). *Big data @l lavoro. Sfatare i miti, scoprire le opportunità: Sfatare i miti, scoprire le opportunità*. FrancoAngeli.

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, *65*(3), 122-135.

Dennett, D. C. (1993). *Consciousness explained*. Penguin uk.

Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a Human Right. *Human Rights Law Review*, *14*(3), 441-458.

Finocchiaro, G. (2017). *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli.

Gaggi, M (2018). *Homo Premium – come la tecnologia ci divide.* Laterza.

Gagliardi, F. (2014). La naturalizzazione dei concetti: aspetti computazionali e cognitivi. Sistemi Intelligenti. Anno XXVI, Numero 2. Pp. pp. 283-298

Géron, A. (2017). *Hands-on machine learning with Scikit-Learn and TensorFlow: concepts, tools, and techniques to build intelligent systems*. " O'Reilly Media, Inc.".

Goodfellow, I. (2016). YoshuaBengio, and Aaron Courville," Deep Learning, MIT Press.

Gstrein, O. J., & Ritsema van Eck, G. J. (2017). Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows'. *International Data Privacy Law*.

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, *23*(1), 259-289.

Hecht-Nielsen, R. (1992). Theory of the backpropagation neural network. In *Neural networks for perception* (pp. 65-93).

Hildebrandt, M. (2009). Who is profiling who? Invisible visibility. In *Reinventing Data Protection?* (pp. 239-252). Springer, Dordrecht.

Hintze, M. (2017). Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*, *8*(1), 86-101.

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). *An introduction to statistical learning* (Vol. 112). New York: springer.

Jefferson, G. (1949). The mind of mechanical man. *British Medical Journal*, *1*(4616), 1105.

Kranenborg, H. (2016). O. Lynskey, The Foundations of EU Data Protection Law. *International Data Privacy Law*, *6*(4), 324-326.

Krausova, A. (2018). Online Behavior Recognition: Can We Consider It Biometric Data under GDPR. *Masaryk UJL & Tech.*, *12*, 161.

Kurzweil, R. C., Albrecht, P., & Gibson, L. (2012). *U.S. Patent No. 8,204,580*. Washington, DC: U.S. Patent and Trademark Office.

Lambrinoudakis, C. (2018). The general data protection regulation (GDPR) era: Ten steps for compliance of data processors and data controllers.

Lynskey, O. "The Link between Data Protection and Privacy in the EU Legal Order", in EADEM, The Foundations of EU Data Protection Law, Oxford, Oxford University Press, 2015

Machinery, C. (1950). Computing machinery and intelligence-AM Turing. *Mind*, *59*(236), 433.

Marini L., Aprea I., (2015) "*Le guidelines on regulating robotics: una sfida per il diritto dell'Unione"*, in Ordine internazionale e diritti umani, n. 5.

Marini, P. (2018). *GDPR: il nuovo regolamento europeo sulla Privacy*, IPSOA.

Moore, G. E. (1965). *Cramming more components onto integrated circuits*. *Proceedings of the IEEE*, *86*(1), 82-85.

Nemitz, P. (2018). "Constitutional democracy and technology in the age of artificial intelligence." *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences 376.*

Nieuwesteeg, B., & Faure, M. (2018). *"An analysis of the effectiveness of the EU data breach notification obligation."* Computer Law & Security Review, 34(6), 1232-1246.

Niger, S. (2006). *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*. Cedam.

Pizzetti, F. (2016). La protezione dei dati personali dalla direttiva al nuovo regolamento. Una sfida per le Autorità di controllo e una difesa per la libertà dei moderni. Aracne.

Pizzetti, F. (2016). *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamente europeo*. G Giappichelli Editore.

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). *Backups and the right to be forgotten in the GDPR: An uneasy relationship.* Computer Law & Security Review: The International Journal of Technology Law and Practice,34(6).

Riccio G. M., Scorza G., Belisario E. (2018). *GDPR e normativa privacy. Commentario*, Ipsoa.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,.

Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language* (Vol. 626). Cambridge University Press.

Searle, J. R. (1980). *Minds, brains, and programs. Behavioral and brain sciences*, *3*(3), 417-424.

Sirur, S., Nurse, J. R. C., & Webb, H. (2018). "Are we there yet? understanding the challenges faced in complying with the general data protection regulation (GDPR). "

Stark, J. R., & Fontaine, D. R. (2015). *Cyber Insurance: A Pragmatic Approach to a Growing Necessity*.

Tamò-Larrieux, (2018). *A. Designing for Privacy and its Legal Framework Data Protection by Design and Default for the Internet of Things.* Springer.

Temme, M. (2017). Algorithms and Transparency in View of the New General Data Protection Regulation. *Eur. Data Prot. L. Rev.*, *3*, 473.

Treacy, B. (2012) "*Formalising the role of the DPO - the practical consequences*", Privacy & Data Protection, Vol. 12, N. 3.

Tzanou, M. (2013). *"Data protection as a fundamental right next to privacy? Reconstructing'a not so new right."* International Data Privacy Law, 3(2), 88-99.

Vestoso, M. (2018). The GDPR beyond Privacy: Data-Driven Challenges for Social Scientists, Legislators and Policy-Makers. *Future Internet*, *10*(7), 62.

Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(3), 436-449.

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology*, *10*(2), 266-294.

Walker-Osborn, C., & McFarlane, G. (2018). GDPR Four Months On. *ITNOW*. *60*(4), 48-49.

Warren, S. D., & Brandeis, L. D. (1890). "*The right to privacy*." Harvard law review, 193-220

Wolters, P. T. J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility?. *International Data Privacy Law*.

Wright, D. (2012). *"The state of the art in privacy impact assessment." Computer law & security review, 28*(1), 54-61.

Sitografia.

Crea G., “Macchine Intelligenti e protezione dei dati in una prospettiva di Ethics by design” in www.altalex.com URL consultato il 22 dicembre 2018 ;

Agenzia per l'Italia Digitale “Misure di Sicurezza” in https://www.agid.gov.it/ URL consultato il 17 novembre 2018 ;

Aiello L. C., Dapor M., “Intelligenza Artificiale: i primi 50 anni.” in http://lacam.di.uniba.it/people/courses/icse/icse0910/AielloDapor.pdf URL consultato il 9 novembre 2018;

Autorità Garante per la Protezione dei Dati Personali in https://www.garanteprivacy.it/web/guest URL consultato il 6 novembre 2018 ;

Avast, “Malware” in https://www.avast.com/c-malware URL consultato il 10 gennaio 2019 ;

Calvi A., “Innovazione della rete Internet” in https://www.telecomitalia.com/tit/it/innovazione/rete/internet-day.html URL consultato il 28 novembre 2018 ;

Dutcher J. “What is Big Data.” sul sito dell'Università di Berkeley https://datascience.berkeley.edu/what-is-big-data/ URL consultato il 15 ottobrere 2018 ;

Fiorillo M., “GDPR, IoT e intelligenze artificiali: nuove sfide per la privacy?” in https://www.insidemarketing.it/gdpr-internet-of-things-ai-privacy/ URL consultato il 14 dicembre 2019 ;

Hayes B. “Six ways to define Big Data.” Pubblicato sul “Business Broadway” ; http://businessoverbroadway.com/2014/09/09/six-ways-to-define-big-data/ URL consultato il 15 ottobre 2018 ;

Iaselli M., “Certificazione nel GDPR” in https://www.altalex.com/documents/altalexpedia/2018/03/13/certificazione-nel-gdpr URL consultato il 10 gennaio 2019 ;

Iaselli M., “Il concetto di sicurezza informatica nell’ottica del GDPR” in

https://www.altalex.com/documents/news/2017/12/07/il-concetto-di-sicurezza-informatica-gdpr URL consultato il 29 novembre 2018 ;

IASELLI M., I compiti del Data Protection Officer: chiariamo tutti i dubbi, in www.agendadigitale.eu. URL consultato il 4 dicembre 2018 ;

Karspersky, "IT threat evolution Q1 2018. Statistics" https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/ URL consultato il 23 novembre 2018 ;

La Commission nationale de l'informatique et des libertés, https://www.cnil.fr/fr/la-cnil-delivre-plus-de-50-labels-0. URL consultato il 10 dicembre 2018 ;

Mantelero A., "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment" in www.sciencedirect.com URL consultato il 20 novembre 2018 ;

Miladinova V., drewewr D., "The canary in the data mine" in www.sciencedirect.com URL consultato il 17 novembre 2018 ;

Mondini - Rusconi (studio legale), "Big data: privacy, gestione, tutele. Acquisizione e protezione dati, linee guida GDPR, concorrenza e..." in www.altalex.it URL consultato il 7 gennaio 2019 ;

Ng A., "Machine Learning". https://www.coursera.org/learn/machine-learning URL consultato il 24 novembre 2018 ;

Steel E., "Companies scramble for consumer data" in www.ig-legacy.ft.com URL consultato il 30 novembre 2018 ;

Windows – Microsoft, su www.microsoft.com. URL consultato il 4 dicembre 2018 ;

Zanotti L., "Tag etichetta RFID: cos'è, come funziona ed esempi dell'identificazione a radiofrequenze" in https://www.internet4things.it/iot-library/rfid-cosa-e-come-funziona-esempi-applicativi/ URL consultato il 16 novembre 2018;