Profili di diritto civile della sanità e dell'assistenza: consenso informato e autonomia negoziale etico-algoritmica

Fabio Carchidi*

CIVIL LAW PROFILES OF HEALTH AND CARE: INFORMED CONSENT AND ETHICAL BARGAINING AUTONOMY

ABSTRACT: In the light of disquisitions concerning the doctrinal and jurisprudential formant, the present work proposes to analyse the civil law qualification of informed consent from a philosophical point of view with the aid of an ordering criterion such as the logos of legal science: axiology, which is not merely the logical interpretation of a balancing of principles but rather the systematic interpretation of the legal system regardless of the sharing of the *modus cogitandi* since science deploys its efficacy through the search for a synthesis between thesis and antithesis.

KEYWORDS: Civil law; health and care; artificial intelligence; international law; bargaining autonomy

ABSTRACT: In virtù di disquisizioni concernenti il formante dottrinale e quello giurisprudenziale, il presente lavoro si propone di analizzare la qualificazione civilistica del consenso informato in chiave filosofica tramite l'ausilio di un criterio ordinatore quale *logos* della scienza giuridica: l'assiologia, che non è mera interpretazione logica di un bilanciamento tra principi bensì interpretazione sistematica dell'ordinamento giuridico a prescindere dalla condivisione del *modus cogitandi* poiché la scienza dispiega la sua efficacia tramite la ricerca di una *sintesi* tra tesi e antitesi.

PAROLE CHIAVE: Diritto civile; sanità e assistenza; intelligenza artificiale; diritto internazionale; autonomia negoziale

**Fabio Carchidi: Professore curricolare di diritto, relazioni internazionali ed economia politica presso le scuole secondarie di secondo grado (MIUR). Già tutor presso la Scuola di Specializzazione per le Professioni Legali dell'Università della Calabria. Mail: fabio.carchidi@salvemini.bo.it. Contributo sottoposto a doppio referaggio anonimo.*

Autonomia negoziale assistita, meccanismi di certificazione e ISO/IEC 27001 in ambito sanitario – 4. Un prologo necessario: il dibattito sull'autonomia negoziale e l'assiologia dell'Artificial Intelligence.

1. Analisi diacronico-normativa dell'*argumentum*

L'evoluzione del concetto di *riservatezza*, al giorno d'oggi, coniuga le esigenze storico-interpretative con la necessità di tutela degli aspetti relativi alla vita privata e al dato personale. In siffatto contesto, il legislatore sovranazionale ha affrontato la questione dell'impatto degli sviluppi della società dell'informazione sulla protezione dei dati personali con graduali implementazioni. La Commissione Europea che, com'è noto, partecipa al processo legislativo tramite azioni propulsive ha perseguito la finalità principale di migliorare il funzionamento del mercato comune, non precludendo le necessità di protezione dei dati personali dei singoli[1].

Storicamente, l'evoluzione normativa sovranazionale e *de relato* nazionale tramite recepimento interno, ha subito trasformazioni non indifferenti alla letteratura giuridica, questo avviene soprattutto con la direttiva 2002/58/CE, relativa alla vita privata, familiare e alle comunicazioni elettroniche contenente una disciplina innovativa adeguata, per quei tempi, ai notevoli sviluppi avutisi nel settore dell'*information technology*.

Essa stabilisce norme per garantire la sicurezza nel trattamento dei dati personali, la notifica delle violazioni dei dati personali e la riservatezza delle comunicazioni; vieta anche le comunicazioni indesiderate qualora l'utente non abbia fornito il proprio consenso[2].

L'istituto poc'anzi analizzato acquisirà maggiore rilevanza giuridica tramite il Regolamento generale sulla protezione dei dati (REG UE 2016/679) in quanto strettamente connesso alla presenza di dati sensibili *rectius* particolari ex art. 9.

In pendenza degli ulteriori progressi all'interno delle tecnologie dell'informazione e della comunicazione si propone un miglioramento per il trattamento e lo scambio di dati di qualsiasi natura, per lo stato della protezione delle persone relativamente a tali attività nella Comunità che, ancora, registra notevoli difformità negli Stati membri[3].

[1] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, Milano, 2019, 3-17, nel quale gli autori si soffermano sulla protezione dei dati personali quale indice di democraticità di uno Stato posto al di fuori dei totalitarismi; si v. G. CHIAPPETTA, *Lezioni di diritto civile*, Rende-Napoli, 2018, 8 ss. nel quale si discorre di una tutela armonizzata *de minimis*, nel contesto dell'articolo 8 della CEDU *rectius* della protezione della riservatezza, attraverso cui la persona troverebbe la realizzazione del sé; inoltre, per un riferimento normativo comunitario v. Regolamento (ue) 2016/679 del parlamento europeo e del consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[2] direttiva 2002/58/ce del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), viene valutata innovativa dalla *scientia iuris* soprattutto per le disposizioni volte a garantire la sicurezza tecnica nel trattamento dei dati personali, la notifica cadenzata dai sistemi di gestione della sicurezza delle informazioni.

[3] E. CATERINI, *Lineamenti di diritto civile italoeuropeo. Dal mercato alla persona*, Rende, 2009, 49-52.

1.1. Il Regolamento UE 2016/679 e le norme principio a sostegno della c.d. *ethics by design.* I *dati particolari* scaturenti dal trattamento dei dati in ambito sanitario.

Il Regolamento UE 2016/679, pur rappresentando un progresso fondamentale degli ultimi anni, non è noto per l'introduzione di particolari mutamenti all'impianto – perlomeno complessivo – del sistema della cybersicurezza; presentando due caratteristiche prodromiche a difficoltà applicative e interpretative: le proposizioni prescrittive più stringenti, infatti, a causa di meccanismi richiedenti la ridefinizione delle procedure interne e la riformulazione dei rapporti con gli *stakeholders,* o meglio, dipendenti, collaboratori, fornitori, clienti o utenti, impongono una rivoluzione copernicana nell'approccio alla gestione dell'informazione, con l'azione-coazione di un monitoraggio costante delle misure di sicurezza tecnologiche ed organizzative, con oneri di spesa anche ingenti[4].

In siffatto contesto la normativa è satura di oneri *rectius* costi espliciti ed impliciti legati all'adozione dei provvedimenti di sicurezza *ad hoc*, specie nel panorama post covid-19 ovvero bellico del conflitto Russia-Ucraina nel quale imporre adeguamenti normativi comporta rischi notevoli quali riduzione qualificata nel conto economico del bilancio dei margini di profitto e dunque impiego di risorse per il succitato adeguamento con un bilanciamento a danno della privacy che, *ictu oculi,* porta alla diffusione di un sempre più ampio stato di illegalità. Per converso, ai destinatari della normativa è stato concesso un lasso di tempo più o meno ampio per ammortizzare e dilazionare i costi da sostenere.

La contropartita, però riguarda altri rischi, il RGPD *rectius* REG (UE) 2016/679 se da un lato presenta, in *nuce,* vantaggi con l'ormai lapalissiano merito di costituire punto focale della disciplina sulla privacy informativa, dall'altro rende, *de facto,* obbligatoria la creazione del c.d. «*ecosistem*» normativo nel quale possano trovare soddisfazione i multiformi interessi economici coinvolti nella loro raccolta, elaborazione, utilizzo e condivisione[5].

A suffragio di ciò, la novità della normativa europea direttamente applicabile nel territorio nazionale è quella di fungere da norma di chiusura in grado di incorporare il rispetto del diritto nelle piattaforme digitali e nei processi organizzativi cosicché l'attività produttiva integri le cautele inerenti al trattamento dei dati personali.

Ad avallare il *modus cogitandi* sinora espresso nel contesto del trattamento dei dati governato da una tecnologia più sofisticata ed invasiva, si è cercata una soluzione al problema della protezione dei dati che non fosse meramente formale e che risultasse efficace e idonea a trattare un flusso di informazioni in costante crescita per disponibilità matematica e statistica.

L'ottemperanza ai principi del RGPD permette una sofisticazione dei dati personali che sia in primo luogo lecita e trasparente, ma soprattutto richiede, in forma espressa, il consenso al trattamento dei dati personali che appartengono alle categorie dei *dati particolari*: l'art. 9 del RGPD afferma che è fatto

[4] E.A. ROSSI, *Qualche problema in materia di competenza e giurisdizione nel Regolamento Generale sui Dati Personali,* in *Studi Vrbinati di scienze giuridiche, politiche ed economiche, LXXXV -2018,* nuova serie A, 69, 3- 4, 256 ss. cfr. V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *op. cit.,* 23 ss.

[5] F. BARRA CARACCIOLO, *La tutela della personalità in internet*, in *Diritto dell'informazione e dell'informatica*, 2, 2018, 206 nel quale si sottolineano i pregi del Regolamento a contatto con il complesso sistema tecnologico; v. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, Napoli, 2020, 60-65, in particolare quando specifica, in virtù della manualistica per la quale la funzione delinea la forma, che il sistema socio-culturale è un aspetto strutturale conformativo e come tale non può che determinare il contenuto dello ius – ciò detto per spiegare quanto privacy e crisi da covid-19 siano collegati.

divieto trattare dati relativi alla salute se non tramite apposite basi di legittimità, tra le quali il consenso è considerata la principale.

L'etica, la bioetica e la conformità ai principi dettati da una norma comunitaria si trovano più che mai prossimi[6].

Il rispetto dei principi del RGPD per gli specifici progetti che prevedono l'impiego di algoritmi *machine learning based*, comporteranno, al di là di ogni ragionevole dubbio, una particolare attenzione ai temi del diritto civile della sanità e dell'assistenza.

[6] REG (UE) 2016/679 art. 9: «Trattamento di categorie particolari di dati personali. 1. 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. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. 4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute» inoltre, ai fini di una disquisizione lineare e relativa al contesto affrontato si v. P. PERLINGIERI, *Manuale di diritto civile*, Napoli, 2021, 77-82.

L'aderenza ai principi generali di protezione dei dati personali, a titolo meramente esemplificativo: *liceità, limitazione delle finalità, trasparenza, equità, accuratezza e minimizzazione dei dati, sicurezza, protezione dei dati in base alla progettazione e by default* consentono di adeguare i database rimpinguati su piattaforme di vario genere alle finalità espresse. A tal proposito le trasgressioni ai precetti contenuti all'interno delle disposizioni *rectius* discriminazioni e processi decisori non trasparenti o non sottoposti a consenso saranno assenti o fortemente mitigati; ciò detto seguendo il criterio in base al quale il trattamento è lecito esclusivamente se le informazioni sono state trasmesse agli interessati e se il consenso – preventivo al trattamento dei dati – consente di escludere, per ovvi motivi, il trattamento di particolari categorie di dati personali.

Altro *thema* nell'intervento di algoritmi di *Artificial Intelligence* in ambito sanitario è quello dell'anonimizzazione dei dati sulle informazioni personali raccolte ed elaborate, per quanto possibile, e in relazione alle finalità del trattamento, tenendo conto di ogni ulteriore probabile effetto/impatto/rischio implicito nel progetto, in termini di responsabilità civile e bioetica[7].

Nel caso S. & Marper vs UK, del 4 dicembre 2008, due cittadini britannici, uno dei quali minorenne, ricorrono alla Corte Europea dei Diritti dell'Uomo (n.d.r. Corte di Strasburgo) lamentando la violazione degli artt. 8 e 14 della Convenzione Europea per la Salvaguardia dell'Uomo e delle Libertà fondamentali per via della conservazione presso le banche dati della Polizia di dati sanitari, impronte digitali, campioni biologici e profili di DNA dopo la conclusione delle azioni penali nei loro confronti; la Corte di Strasburgo ha constatato, tramite interpretazione evolutiva, l'importanza particolare dei diritti lesi tale da ridurre il margine di apprezzamento statale desunto dalle circostanze del caso, dal contesto locale e dalle legislazioni degli Stati membri in materia[8].

1.2. Consenso informato ex L.219/2017 nelle fasi di *ricerca e sviluppo* ed elaborazione del *machine learning semantico*

Per generare algoritmi di AI rispettosi dell'ordinamento nazionale e internazionale quali indizi di pragmatismo applicato *ab initio,* cioè nella fase iniziale nella quale il progetto viene pensato ovvero le prime fondamenta vengono interposte come basi dell'elaborazione degli algoritmi, è facoltà degli esperti in materia far riferimento ai principi del RGPD poiché consentiranno di limitare fortemente l'uso contro funzionale dei *dataset* tramite i quali tali algoritmi sono "preparati", limitando i rischi che le applicazioni comportano a seguito del loro rilascio.

[7] In relazione all'argomento del *machine learning* v. I. CORRADINI; E. ARDELLI, T. AHRAM, *Advances in Human Factors in Cybersecurity AHFE 2020 Virtual Conference on Human Factors in Cybersecurity*, July, 16-20, 2020, USA; per ciò che concerne bioetica e diritto civile nella legalità costituzionale v. G.PERLINGIERI, G.CAPAREZZA FIGLIA, *L'«interpretazione secondo Costituzione nella giurisprudenza» crestomazia di decisioni giuridiche*, Napoli, 2021, IX-XIV «la trasfigurazione in senso sociale di categorie e figure di matrice patrimoniale […] l'attenzione verso il profilo dell'interesse negli istituti e nelle situazioni soggettive ha permesso una rivalutazione del profilo oggettivo e funzionale rispetto a quello formale e strutturale ed ha contribuito a una giurisprudenza valutativa la quale, nell'abbandonare il metodo meramente deduttivo della sussunzione sillogistica, recupera la giuridicità del fatto nell'operazione di qualificazione normativa e accoglie finalmente una concezione unitaria e sistematica dell'ordinamento giuridico».

[8] G. CHIAPPETTA, *op. cit.,* 24 ss.; Corte Europea dei Diritti dell'Uomo, S. & Marper c. Regno Unito del 4 Dicembre 2008 «the Court will first consider whether the retention by the authorities of the applicants' fingerprints, DNA profiles and cellular samples constitutes an interference in their private life» (§59), https://hudoc.echr.coe.int

Pertanto, specie nel caso dello sviluppo mediante *machine learning semantico* che abbia come scopo, ad esempio, l'assistenza qualificata in una realtà ospedaliera o assistenziale, è obbligatorio normativamente e deontologicamente, che il progetto prodromico all'implementazione garantisca il rispetto dei dati personali[9].

Tale rispetto potrà essere raggiunto, in virtù della normativa comunitaria del 2016 in combinato disposto con la normativa sul *consenso informato* varata dal legislatore italiano il 22 dicembre 2017, in specifico, la L. n. 219, se i dati saranno: trattati in modo lecito, equo e trasparente nei confronti degli interessati («liceità, correttezza e trasparenza»); raccolti per finalità determinate, esplicite e legittime e non ulteriormente trattati in modo incompatibile con tali finalità; l'ulteriore trattamento a fini di archiviazione nell'interesse del pubblico, di ricerca scientifica o storica o statistica non sarà considerato incompatibile con le finalità iniziali («limitazione delle finalità»); adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trattati («minimizzazione dei dati»); accurati e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per garantire che i dati personali imprecisi, in considerazione degli scopi per i quali sono stati acquisiti, siano cancellati o rettificati senza indugio («accuratezza»); conservati in una forma che consenta l'identificazione delle persone interessate per un periodo di tempo non superiore a quello necessario per gli scopi per i quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi, nella misura in cui i dati personali saranno trattati esclusivamente a fini di archiviazione nell'interesse del pubblico, per scopi di ricerca scientifica o storica o per scopi statistici, previa attuazione di adeguate misure tecniche e organizzative per salvaguardare i diritti e le libertà delle persone interessate («limitazione della conservazione»); trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danneggiamento accidentale, utilizzando adeguate misure tecniche o organizzative («integrità e riservatezza»)[10].

Tutto ciò detto conduce all'esecuzione di un *assessment* d'impatto sull'etica e sulla protezione dei dati, ai sensi dell'articolo 35 del GDPR[11], che si soffermi non già esclusivamente sull'identificazione degli

[9] P.B. HELZEL, *La bioetica come ponte tra società e innovazione,* Rende, 2016, 145 ss.; cfr. M. KEARNS, A. ROTH, *The ethical algoritm,* New York, 17 ss. per quanto concerne l'anonimizzazione dei dati quale metodologia fondante per il rispetto delle normative sulla protezione dei dati personali.

[10] Regolamento ue 2016/679, artt. 5-9; sul requisito dello scopo; si v. L. FEILER, N. FORGÒ, M. WEIGL, *The EU General Data Protection Regulation (GDPR): A commentary,* UK, 56: «*Il requisito della definizione dello scopo (derivante dall'obbligo di determinazione della finalità) costituisce un aspetto materiale del principio di "limitazione delle finalità". Le finalità devono essere specificate in modo sufficientemente preciso in modo che: (i) si possa valutare quali tipologie di trattamento rientrano; e (ii) è possibile valutare la liceità delle finalità nonché la liceità del trattamento in generale. Finalità del trattamento quali "finalità di marketing" o "finalità di sicurezza informatica" non sono, in linea di principio, sufficienti (si veda l'esplicita dichiarazione del Gruppo di lavoro Art. 29, Parere 03/2012 sulla limitazione delle finalità WP 203 (2013*)»

[11] Su tale articolo, baluardo della cybersicurezza nazionale è opportuno v. L. FEILER, N. FORGÒ, M. WEIGL, *The EU General Data Protection Regulation (GDPR): A commentary,* UK, 130 ss. «*che la valutazione d'impatto sulla protezione dei dati debba essere effettuata "prima" del trattamento significa che il trattamento non può iniziare prima che la valutazione d'impatto sulla protezione dei dati sia stata completata (e, se necessario, prima dell'avvio della consultazione con l'autorità di controllo ai sensi all'articolo 36). Secondo l'art. 29, l'esecuzione di una valutazione d'impatto sulla protezione dei dati "è un processo continuo, non un esercizio una tantum" e dovrebbe essere "iniziato il prima possibile nella progettazione del trattamento" (cfr. Gruppo di lavoro art. 29, Linee guida*

elevati rischi per i diritti e le libertà fondamentali delle persone fisiche in una realtà sanitaria bensì che evidenzi tutte le lacune che devono essere mitigate con una serie di soluzioni proporzionate al fine di garantire una tutela armonizzata *de minimis*.

Il progetto dell'algoritmo di *machine learning semantico* in una realtà sanitaria e dunque tramite l'azienda che lo attua, *prima facie*, deve riconoscere che lo strumento e il progetto stesso potrebbero sollevare una composizione etico-giuridica rilevante. A tale scopo, l'algoritmo di machine learning semantico (e.g. in un contesto ospedaliero) avrebbe l'obbligo di dedicare la fase prodromica all'indagine sugli aspetti etici e legali della ricerca; la Carta dei diritti fondamentali dell'Unione europea o, volgarmente, la Carta di Nizza, è il principale strumento giuridico a livello comunitario che riconosce e garantisce i diritti personali, politici, economici, civili e sociali dei cittadini e dei residenti dell'Unione Europea. È per tale *ratio essendi* che si dovrebbe prendere in particolare considerazione l'impatto potenziale delle attività di ricerca sui diritti tutelati dalla Carta, tra cui dignità, libertà, uguaglianza, solidarietà, giustizia[12].

I diritti sinora esposti devono essere tutelati tramite progettazione dell'algoritmo a monte, *in primis* dalle attività di R&S del progetto (soprattutto le ricerche aventi ad oggetto persone e/o la raccolta di dati personali con finalità precise); *in secundis* attraverso l'impiego del machine learning semantico.

Il Considerando 84 del RGPD sottolinea quanto sia indispensabile, al fine di migliorare la conformità alle norme ordinamentali, laddove «*le operazioni di trattamento possano comportare un rischio elevato per i diritti e le libertà delle persone fisiche*» effettuare una valutazione d'impatto sulla protezione dei dati per valutare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.

I diritti della personalità coinvolti in un progetto di implementazione di un algoritmo di tale caratura sono quei diritti riguardanti la sfera soggettiva *rectius* il diritto soggettivo dalla prospettiva assoluta riferito, dunque, agli operatori che utilizzeranno lo strumento e, ovviamente, i pazienti[13].

Adunque, è fondamentale valutare la totalità dei possibili rischi nell'ambito di una valutazione preventiva del rischio, considerando che l'impatto sui diritti di tali persone ha una conseguenza mediata ovvero immediata su tutte le attività che seguiranno.

A titolo esemplificativo e non esaustivo, le tecnologie per la sistematizzazione, la raccolta nonché l'elaborazione di immagini e, infine, l'estrazione di video e testi, possono essere potenzialmente intrusive dei diritti alla riservatezza garantiti dalla Carta dei diritti fondamentali dell'Unione Europea, in specifico, dalla prospettiva della responsabilità civile ex articolo 79 del RGPD che aggrega una tutela giurisdizionale «diretta» nei confronti dell'interessato, permettendo l'accesso alla giurisdizione – com'è

sulla valutazione dell'impatto sulla protezione dei dati (DPIA) e determinare se il trattamento è "probabile che comporti un rischio elevato" ai fini del regolamento 2016/679", WP 248 (2017)»

[12] V. Autorizzazione n. 2 del 2016 che cita e fa salvi i principi della Carta di Nizza e autorizza al trattamento dei dati idonei a rivelare lo stato di salute del 15 dicembre 2016, valida sino al 24 maggio 2018, ma poi fatta salva dal decreto di adeguamento della normativa nazionale per un periodo transitorio prevedendo un successivo riesame.

[13] Dalla prospettiva civilistica è impossibile non citare il caposaldo della letteratura giuridica sul tema T. A. AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978, 34-51; v. anche R. BORRUSO, *Computer e diritto*, Milano, 1991, 301-307; cfr. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, Napoli, 2006, 906 ss.; v. G. CHIAPPETTA, *Persona e informazioni aziendali riservate*, Napoli, 2010, 8-10

noto, esclusiva del giudice ordinario – nel caso di violazione dei diritti – contemplati e rilevati dal Regolamento – a seguito di un trattamento dei dati personali[14].

A questo proposito, al fine di espletare una corretta analisi valutativa, bisogna bipartire le diverse fasi in cui si articola la produzione di un algoritmo di AI per una realtà sanitaria.

In pendenza della prima fase, ovverosia la fase di ricerca, gli strumenti di implementazione di un algoritmo di machine learning semantico, nonostante siano già all'interno della struttura, vengono utilizzati per scopi sanitari e pertanto si applica al trattamento dei dati personali il REG (UE) 2016/679 senza alcun dubbio sulla legge applicabile, tuttavia sorge spontaneo un dubbio gnoseologico, la portata delle disposizioni del GDPR applicate al trattamento dei dati personali durante la fase di ricerca.

Essendo che la funzione dà forma al negozio giuridico ergo alla struttura degli effetti essenziali, l'algoritmo funge da raccoglitore di dati resi disponibili dal pubblico, dal web, dalle aziende farmaceutiche, da realtà universitarie e dalla stessa struttura.

La sofisticazione di informazioni da tali fonti potrebbe implicare anche la raccolta di *personal data*[15].

Il «dato personale» è *qualsiasi informazione relativa a una persona fisica identificata o identificabile* (la c.d. «persona interessata»); la persona fisica identificabile è una persona che può essere individuata, direttamente o indirettamente, in particolare con riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica[16].

L'eventualità che un dato possa essere considerato «personale» secondo il RGPD è, per l'appunto, molto probabile che si realizzi, in quanto l'identificabilità potrebbe derivare non solo dall'identificatore in via diretta cancellabile o non raccolto (c.d. «K-anonimia») ma anche attraverso la combinazione di svariati elementi (c.d. «L-diversità»). Le informazioni vengono raccolte attraverso fonti diverse

[14] A tal proposito v. R. MONTINARO, *Tutela della riservatezza e risarcimento del danno nel nuovo codice in materia di protezione dei dati personali*, in *Giust. Civ., II,* 2004, II, 248; Sul danno non patrimoniale v. Cass., 24 giugno 2016, n. 13161, in *De Jure*;

[15] P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, cit., 60-65, in particolare quando specifica, in virtù della manualistica per la quale la funzione delinea la forma, che il sistema socioculturale è un aspetto strutturale conformativo e come tale non può che determinare il contenuto dello ius.

[16] RGPD, art. 4; Si rammenta, in siffatto contesto, il Considerando n. (26): «I *principi di protezione dei dati dovrebbero applicarsi a qualsiasi informazione riguardante una persona fisica identificata o identificabile. I dati personali che sono stati oggetto di pseudonimizzazione, che potrebbero essere attribuiti a una persona fisica mediante l'uso di informazioni aggiuntive, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per determinare se una persona fisica è identificabile, dovrebbero essere presi in considerazione tutti i mezzi che ragionevolmente possono essere utilizzati, come l'individuazione, dal responsabile del trattamento o da un'altra persona per identificare la persona fisica direttamente o indirettamente. Per accertare se è ragionevolmente probabile che i mezzi vengano utilizzati per identificare la persona fisica, si dovrebbe tener conto di tutti i fattori oggettivi, come i costi e il tempo necessario per l'identificazione, tenendo conto della tecnologia disponibile al momento dell'identificazione elaborazione e sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi alle informazioni anonime, vale a dire le informazioni che non si riferiscono a una persona fisica identificata o identificabile o ai dati personali resi anonimi in modo tale che l'interessato non sia o non sia più identificabile. Il presente Regolamento non riguarda quindi il trattamento di tali informazioni anonime, anche per fini statistici o di ricerca*».

dall'interessato *ergo* i dati non vengono ottenuti direttamente dall'interessato stesso, ma dalle suddette fonti.
In questi casi, si deve – presumibilmente- pensare che i dati dei pazienti siano stati sottoposti preventivamente alla richiesta di un consenso qualificato per il trattamento ed al *consenso informato* ex L. 219/2017 per la conduzione del *project*.
Qualora la fattispecie concreta preveda la presenza di terzi interessati, ai quali un *cluster* specifico di *data* potrebbe fare riferimento, e.g. storia genetica e familiare del paziente, che sono diversi dai pazienti stessi; è ragionevole presumere che tali informazioni non siano state ottenute dallo stesso interessato, bensì da altre fonti. Il punto focale della *quaestio* è che i loro dati non sarebbero resi noti al pubblico volontariamente e manifestamente e non sarebbero stati sottoposti a *consensus;* generando così il paradossale effetto che, per lo stesso campione genetico o meglio etnico, un algoritmo di machine learning semantico potrebbe prendere le stesse decisioni anche se i soggetti non appartengono alla stessa famiglia e quindi, tendenzialmente, non condividono quelle componenti umane che sono in grado di influenzare la capacità di autodeterminazione; aspetto profondamente rilevante per un approccio bioetico[17].

1.2.1. Consenso e «autonomia negoziale algoritmica». Analisi in combinato disposto degli artt. 1376 c.c. e art. 7 RGPD

Il principio consensualistico, contemplato nell'articolo 1376 Cod. civ., porta al più tradizionale esercizio delle situazioni soggettive e rende, *de facto,* possibile il loro inserimento nella circolazione giuridica e, in tal caso, algoritmica.
L'autonomia negoziale del singolo nel cyberspazio – tutt'altro che tradizionale – dal punto di vista della preselezione degli interessi da introdurre nella regola tecnica, porta a descrivere, l'autonomia privata, prevista dall'art. 41 Cost., che definisce degli scopi-valori riguardanti non soltanto ogni creazione legislativa bensì anche i rapporti *interprivati*.
L'item dell'era tecnologico-digitale che il formante dottrinale ha analizzato e categorizzato è proprio fulcro umano dell'algoritmo, il consenso.
Una prima classificazione ha inserito i dati personali tra i diritti della personalità con la conseguente risultanza che l'attività di raccolta e trattamento si qualifica come antinomica senza la manifestazione di volontà del soggetto; il consenso, in tal senso, diviene atto autorizzativo di diritto privato al quale collegare una natura non negoziale; tale *modus cogitandi*, però, non troverebbe congruenza nell'articolo 6 del RGPD – nel quale si legge il consenso con funzione scriminante – bensì nell'articolo 9 par. 2 lett a) che in realtà, andando oltre l'interpretazione letterale, avrebbe una di bilanciamento tra interessi diversi: la garanzia di quello pubblico al trattamento dei dati e di quello privato alla loro circolazione.

[17]U. DRAETTA, *Documenti precontrattuali nei negozi relativi a mergers e acquisitions. Rassegna della prassi internazionale,* in *Compravendite internazionali di partecipazioni sociali*, Milano, 1990, 110 ss.; G. CHIAPPETTA, *L'incidenza della dottrina sulla giurisprudenza delle Alte Corti nel diritto di famiglia e dei minori*, Rende-Napoli, 2014, 22 ss.; C. GALLI, *Il diritto d'autore e la tutela della proprietà industriale sulla rete Internet,* in *Internet e diritto civile*, Napoli, 2015, 139 ss.

Una ulteriore qualificazione si sofferma sulla volontà come manifestazione per autorizzare l'ingresso di un secondo soggetto nella situazione giuridica del primo con la generazione del c.d. sinallagma, tuttavia, tale modus operandi è aderente a un retaggio precedente, basti pensare alla disposizione presente nell'articolo 11 della legge n. 675/1996 oggi ampiamente superata dall'articolo 7 del RGPD che si limita a collocare, in capo al titolare del trattamento, la situazione soggettiva passiva di onere per dimostrare che il requisito consensuale sia stato manifestato.
Un'interpretazione sistematica tra le normative citate porta a dichiarare che il consenso, la cui prova dell'esistenza è onere documentale del titolare del trattamento, può essere parafrasato come un «*comportamento concludente attraverso il quale l'interessato manifesta la propria disponibilità affinché altri raccolgano ed elaborino le proprie informazioni*»[18]

2. Il nesso di causalità adeguata al c.d. *Ethics and Data Protection Impact Assessment* (EDPIA)

Quanto finora detto porta alla logica riflessione riguardante la società che sviluppa un algoritmo di machine learning semantico in una realtà sanitaria quale titolare del trattamento; questa deve esaminare preventivamente la necessità di effettuare una EDPIA (*ethics and data protection impact assessment*), analizzando, pragmaticamente, se il trattamento del dato effettuato nell'ambito della fase di R&S potrebbe rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Con tale ratio, si specifica che la EDPIA, ai sensi dell'articolo 35 e ss. del RGPD, non è facoltativa solo per i trattamenti che, come appena detto, possono rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche[19];
Procedimentalizzando il ragionamento, è necessario applicare la fonte primigenia in materia; il RGPD identifica alcune operazioni di trattamento che presentano rischi intrinseci elevati: a) valutazione di aspetti personali basati su trattamento automatizzato, incluso il *profiling*, e su cui si basano processi decisionali che producono efficacia giuridica sulla persona fisica o che influenzano in modo significativo la stessa persona fisica; b) trattamento su larga scala di categorie particolari di dati di cui all'articolo 9 comma 1 del RGPD, o di dati personali relativi a condanne penali e reati di cui all'articolo 10 del RGPD; o c) monitoraggio sistematico di un'area accessibile al pubblico su larga scala.[20]

[18] V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *op. cit.,* 249-260; cfr. C. ROGGERO, *Il diritto di immagine su Internet* (Italian Edition), 2018, 38-39; per un'ulteriore disamina consultare P. PERLINGIERI, *Manuale di diritto civile*, cit., 529-535. Cfr G. CHIAPPETTA*, Il rapporto da comunicazione commerciale ed il principio di autodeterminazione,* in *Rassegna di diritto civile*, 3, 2008, 640-645: «*Parte della dottrina ha reputato l'articolo 41 della Costituzione una norma programmatica in quanto dopo aver enunciato la libertà di iniziativa economica privata, affiderebbe al legislatore il compito di disciplinare la materia […] la sentenza della Corte Costituzionale del 14 giugno 1956 n. 1 mette in luce che lo stesso concetto di norma programmatica non era uniforme essendo usato per individuare caratteri eterogenei di norme giuridiche*». Cfr. P. LAGHI, *Cyberspazio e sussidiarietà*, Napoli, 2015, 236-240.
[19] P.B. HELZEL, *La bioetica come ponte tra società e innovazione,* Rende, 2016, 120 ss.; cfr. M.KEARNS, A. ROTH, *The ethical algoritm,* New York, 12 ss. nei quali si sottolinea l'importanza dei dati sensibili *rectius* dati particolari dai quali desumere i principi dell'articolo 8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali.
[20] Al fine di rendere la disquisizione più chiara si consiglia la lettura di C. GALLOTTI, *Sicurezza delle informazioni–Edizione 2022: Gestione del rischio-I sistemi di gestione-La ISO/IEC 27001:2022-I controlli della ISO/IEC*

Tale elenco non è da considerarsi esaustivo, vista l'impossibilità di enucleare la totalità dei casi concreti, invero, il Gruppo di lavoro dell'articolo 29 (attualmente «*European Data Protection Board*» anche "WP29") nelle sue Linee guida (WP 248 rev.01) sulla c.d. valutazione d'impatto sulla protezione dei dati (DPIA) ha descritto ulteriori criteri su come localizzare i tipi di trattamento ad alto rischio, integrando la normativa ordinamentale:

1) Valutazione, compresi *profiling* e la *prediction*, partendo da «*aspetti riguardanti la prestazione dell'interessato sul lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, il luogo o i movimenti*» (considerando 71 e 91 del RGPD);
2) Procedimenti automatizzati con effetti giuridici et similia: elaborazioni finalizzate a decidere su soggetti che generano «*effetti giuridici riguardanti la persona fisica*» o che «*incidono in modo analogo e significativo sulla persona fisica*» (articolo 35, paragrafo 3, lettera a), del RGPD). A titolo esemplificativo si veda il trattamento che può portare all'esclusione o alla discriminazione delle persone;[21]
3) Monitoraggio sistematico: tipologia di trattamento utilizzata per osservare e/o controllare il soggetto interessato, inclusi i dati raccolti attraverso «*un monitoraggio sistematico di un'area accessibile al pubblico*» (articolo 35(3)(c) del RGPD). Questa tipologia di monitoraggio è qualificabile quale criterio per orizzontarsi in quanto i dati personali possono essere raccolti in situazioni nelle quali gli interessati possono non essere consci di chi sta raccogliendo i loro dati e soprattutto di come saranno utilizzati. In *surplus*, può essere categoricamente difficile per le persone fisiche evitare di essere oggetto di tale trattamento in spazi pubblici ovvero accessibili al pubblico;
4) Dati particolari: si tratta di categorie speciali di dati così come definite dall'articolo 9 del RGPD (e.g. informazioni *ex ante* sulle opinioni politiche degli individui), nonché di dati personali relativi a procedimenti penali in pendenza o in giudicato. Un esempio pratico potrebbe essere un'azienda ospedaliera generale che conserva la cartella clinica dei pazienti ovvero un agente investigativo privato che conserva i dati dei soggetti socialmente pericolosi. Tale criterio, inoltre, *per relationem,* comprende dati che possono essere considerati come indice di aumento del rischio per i diritti e le libertà degli individui, si pensi ai dati relativi alle comunicazioni elettroniche, ai dati relativi all'ubicazione, ai dati finanziari (che potrebbero essere utilizzati per frodi nei pagamenti). In siffatto contesto, può essere rilevante il fatto che i dati sono già stati resi disponibili al pubblico dall'interessato o da terzi. Rilevanti sono anche le informazioni generate da una persona fisica nell'ambito di attività puramente personali (e.g. service di cloud computing per la gestione di documenti personali, servizi di posta elettronica, agende, e-reader, e altre applicazioni per la registrazione di dati personali che possono contenere informazioni particolarmente personali), la cui pubblicizzazione per scopi diversi dalle attività domestiche può essere percepita come lesiva del diritto alla riservatezza della vita privata e familiare;
5) Dati elaborati su larga scala: il RGPD non definisce cosa si intenda per larga scala; bisogna tener conto del *numero di soggetti interessati*, sia come numero specifico sia come percentuale della

27002:2022, Roma, 2022, 176 ss.; nella giurisprudenza recente del Consiglio di Stato si v. Cons. Stato, Sez. III, 31/12/2020, n. 8543, AIFA – Agenzia Italiana del Farmaco c. P.S.I. S.r.l. e altri.

[21] Ulteriori esplicazioni su questi concetti sono fornite nelle Linee guida WP29 sulla profilazione (WP 251 rev.01)

popolazione interessata; il *volume* dei dati e/o la *gamma* dei diversi dati trattati; la *durata*, o la *permanenza*, dell'attività di trattamento dei dati nonché l'estensione *geografica* dell'attività;

6) Aggregazione di dati abbinati o combinati, e.g. a partire da due o più operazioni di *processing* di dati effettuate per scopi diversi e/o da diversi responsabili del trattamento;
7) Dati relativi a persone vulnerabili[22]: il trattamento di questa tipologia di dati può rendere necessaria una DPIA per via del *gap* di potere tra l'interessato e il responsabile del trattamento, invero, l'individuo può non essere in grado di acconsentire o di opporsi al trattamento dei suoi dati. Nel pratico, i dipendenti aziendali o di altro genere trovano spesso difficile opporsi al trattamento effettuato dal loro datore di lavoro, quando questo è strettamente legato alla gestione delle risorse umane. Inoltre, anche i figli potrebbero non essere in grado di opporsi o di dare il proprio consenso al trattamento dei propri dati in modo consapevole e ponderato *rectius* informato. Ciò riguarda anche le persone fisiche più vulnerabili della popolazione aventi una capacità di agire limitata e dunque necessita di un tutore, curatore o amministratore di sostegno, come, ad esempio, gli interdetti, gli inabilitati, i richiedenti asilo, gli anziani, i pazienti, o con un *gap* qualificato;
8) Utilizzo innovativo o applicazione progressiva di organizzazione tecnologica, come l'uso combinato dell'impronta digitale e del riconoscimento del volto per un migliore controllo dell'accesso fisico, etc. Il RGPD, infatti, chiarisce all'articolo 35, paragrafo 1 e considerando 89 e 91, che lo sfruttamento di una innovativa tecnologia può far sorgere la necessità di effettuare un'ulteriore DPIA. La motivazione è semplice, l'uso di tale tecnologia può creare nuove forme di raccolta e utilizzo dei dati, con un elevato rischio per i diritti e le libertà degli individui. Si pensi ad alcune applicazioni di "*IoT*" potrebbero avere un impatto significativo sulla vita quotidiana e sulla privacy degli individui e dei pazienti[23];
9) Proiezione e trasferimento transfrontaliero di dati *ergo* al di fuori dell'Unione Europea[24], tenendo conto, tra le altre cose, del Paese o più Paesi di destinazione, della possibilità di ulteriori

[22] RGPD, Considerando 75: «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*»

[23] F. CARCHIDI, *Persona e commercio di dati particolari nell'ottica dei flows of personal data,* in *Diritto, Economia e Tecnologie della Privacy*, 3, 2020;

[24] RGPD, Considerando 116: «*Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati*

trasferimenti o della possibilità di trasferimenti basati su deroghe per situazioni specifiche previste dal RGPD[25];

10) In virtù dell'articolo 22 del RGPD, se il trattamento «*impedisce agli interessati di esercitare un diritto o di usufruire di un servizio o di un contratto*»[26].

Questo ingloba il trattamento che ha lo *scope* di consentire, modificare o rifiutare l'accesso degli interessati a un servizio o l'entrata in un contratto, a titolo di esempio, il caso in cui un intermediario finanziario analizza i propri clienti in base a un database di riferimento per decidere se offrire loro un prestito. L'EDPB, infatti, fa riferimento all'obbligo di eseguire un DPIA per valutare analiticamente la congruenza nell'operazione di trattamento, subordinatamente alla valutazione di almeno una diade dei suddetti criteri; al contrario, è obbligatorio documentare le ragioni per l'omissione di un DPIA.
In ogni caso, i criteri succitati non rappresentano una norma di chiusura, poiché in molti casi il trattamento che riguarda solo uno di questi criteri può richiedere una DPIA; è obbligatorio, quindi, valutare con attenzione questo aspetto e, in casi ambigui, eseguire la DPIA a titolo di precauzione[27].

2.1. (segue) Facoltatività, *autonomia negoziale algoritmica* e DPIA

Le fattispecie da enucleare riguardano la sfera dell'autonomia del soggetto nella *libertà contrattuale* di cui il diritto civile italiano, dalla tradizione romanistica, contempla.
La DPIA non risulta obbligatoria nei seguenti casi:

1) Nel caso di trattamento non «*suscettibile di comportare un rischio elevato per i diritti e le libertà naturali dei figli*» ai sensi dell'articolo 35 comma 1 del RGPD;
2) Nel caso in cui la natura, la portata, il contesto nonché lo scopo del trattamento presentano strette analogie a un trattamento per il quale è già stata esperita una DPIA. In tali casi, i risultati della DPIA per l'analoga operazione di *processing* possono essere riutilizzati;

---

dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto, vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento».

[25] F. CARCHIDI, *Aspetti problematici di inquadramento della giurisdizione e dell'autorità di controllo competente nei trattamenti di dati transfrontalieri*, in *Rivista Ambiente Diritto*, inserita nell'area 12 delle Riviste Scientifiche Giuridiche Classe A.

[26] RGPD, Considerando 91: «*Ciò dovrebbe applicarsi in particolare 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, 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*».

[27] v. AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI E CONSIGLIO D'EUROPA, C. GIAKOUMOPOULOS, G. BUTTARELLI, M. O'FLAHERTY, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, 2018, 277 ss; cfr. V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *op. cit.,* 450 ss.

3) Nel caso in cui il trattamento ai sensi dell'articolo 6.1 c) ed e) del RGPD ha una base giuridica nel diritto comunitario o nel diritto dello Stato membro dell'Unione Europea al quale il responsabile del trattamento è vincolato; tale normativa disciplina la specifica attività ovvero l'insieme di operazioni di *processing* in questione;
4) Qualora il trattamento sia incluso nell'elenco predisposto dall'autorità di controllo per le operazioni di trattamento per le quali non è richiesta la DPIA, ai sensi dell'articolo 35 comma 5 del RGPD;
5) Qualora le operazioni di trattamento siano già in pendenza al 25 maggio 2018, salvo il verificarsi di cambiamenti tecnologici significativi o altri cambiamenti significativi delle condizioni.

Si nota come l'implementazione di un algoritmo di *machine learning semantico* in una azienda ospedaliera sostanzialmente tocchi tutti gli aspetti finora affrontati *ergo* la necessità di svolgere una valutazione d'impatto risulta quantomeno difficile da ignorare.

Tale valutazione, seguendo i nessi logici finora redatti, altro non è che un consulto di natura giuridica concertata da un'attenta analisi dei rischi a fronte di presidi di sicurezza tecnici e organizzativi che consentono lo svolgimento "sicuro" del trattamento dei dati personali e in ultima, non di certo per importanza visto il percorso per giungervi, dell'erogazione del servizio[28].

L'analisi di tipo bioetico, quindi, si sposta dal letto del paziente fino alla macchina e da questa al software che la regolamenta, per giungere al dataset che l'ha programmato e alla società che ha scelto quel set, fino al creatore del software che ha deciso di condurlo. Questo risalire alla fonte, quale causalità adeguata, è necessario per capire dove si innestano le necessarie valutazioni poiché, una volta giunti al letto dell'azienda ospedaliera.

L'anamnesi scientifica verso la radice del problema, al fine di applicare la *riflessione bioetica*, permette di comprendere che la EDPIA deve essere compiuta da una società che sia essa stessa rispettosa dei principi del RGPD e che quindi sia implementato il c.d. *modello organizzativo per la sicurezza delle informazioni* compliant ai principali standards internazionali e che garantisca lo svolgimento di analisi dei rischi con cadenze specifiche[29].

3. Governance, risk and compliance. *Autonomia negoziale assistita*, meccanismi di certificazione e ISO/IEC 27001 in ambito sanitario.

Preliminarmente, la *European Network and Information Security Agency (ENISA)* è sorta il 14 marzo del 2004, ma soltanto nel 2005 l'Unione Europea la riconosce come entità sovranazionale per rafforzare la coordinazione europea in materia di sicurezza delle informazioni, invero, tutt'ora lo *scope* è quello

[28] E. CATERINI, *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, Napoli, 2020; L. BOLOGNINI, E. PELINO, *Codice privacy: tutte le novità del d.lgs. 101/2018*, Varese, 2018, 11 ss.; Sul tema del modello consenso-centrico si veda a mero titolo esemplificativo Garante concorr. e mercato, 29/11/2018, n. 27432, in *De Jure* «Integra una fattispecie di pratica commerciale aggressiva, in violazione degli artt. 24 e 25 del codice del consumo (d.lgs. n. 206/2005), l'automatica attivazione della funzione di Facebook c.d. "Piattaforma attiva", con il conseguente scambio reciproco dei dati dell'utente tra il social network e siti web/app di terzi, in assenza di un consenso espresso da parte dell'utente stesso, al quale viene impedito di esercitare una scelta libera e consapevole in merito, essendogli riconosciuta una mera facoltà di opt-out»

[29] In tal senso v. C. GALLOTTI, *op. cit.,* 356 ss.

di raggiungere un alto livello di information and network security nella comunità europea assistendo la Commissione, i Paesi membri e di conseguenza gli operatori economici favorendo un'efficacia conoscitiva degli assunti in materia di cyber sicurezza[30].

La precedente normativa ha costruito un sistema di fonti di regolazione del trattamento dati capace di garantire flessibilità coinvolgendo, *de facto*, destinatari delle norme nella parte redazionale di legislazione integrativa nella quale un ruolo maggioritario spettava alle autorità indipendenti; in siffatto contesto, i codici di condotta per il trattamento dei dati personali, già agli albori, nel 1995 non erano solo una manifestazione dell'autonomia negoziale, bensì un progresso nella modalità di disciplina dei settori altamente tecnici e così da premere su una collaborazione sempre più orizzontale tra realtà pubblica e privata. Si tratta di un passo c.d. neutrale nelle forme di autoregolamentazione libera poiché condizionate dai procedimenti istruttori dell'attività pubblica, il Garante per la protezione dei dati dà l'immagine di questo istituto tramite una definizione, ovverosia, «*autonomia assistita*»[31].

Allo stesso modo, i *meccanismi di certificazione* sono categorie di attestazione su base volontaria della compliance del trattamento dei dati effettuati dal titolare – o dai titolari solidalmente – del trattamento ovvero dal responsabile – ovvero dai sostituti del responsabile – nella disciplina europea, rilasciate con cadenza triennale, rinnovabile e su richiesta, non solo dalle autorità nazionali di vigilanza bensì anche da appositi organismi di certificazione privati accreditati in base al Regolamento CE n. 765/2008 (per l'Italia, Accredia) su requisiti di *indipendenza, competenza, efficace gestione delle funzioni e imparzialità*.

In sintesi, il Regolamento UE 2016/679 in combinato disposto al Regolamento UE 881/19 permette alla certificazione dei prodotti (nel caso di specie affrontato anche dei servizi e dei processi nelle realtà sanitarie) ICT il ruolo valoriale di aumentare la titolarità organica nei confronti dei destinatari, siano essi entità nazionali o persone fisiche, tramite la definizione di un *quadro europeo di certificazione della cybersicurezza* finalizzato a costituire meccanismi di certificazione per vidimare servizi, prodotti e processi ICT; così come recita l'articolo 46, par. 2 del Regolamento UE 881/19: «*valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita*»[32].

Nel contesto sanitario sinora affrontato, la normativa ISO/IEC 27001, intesa quale standard di certificazione inerente al meccanismo di cui sopra, suddivide le c.d. *best practices* in 14 *controlli*.

[30] Per ulteriori approfondimenti v. E.M. BRUNNER, M. SUTER, *International CIIP Handbook 2008/2009: an inventory of 25 national and 7 international critical information infrastructure protection policies*, 2009, London, 472 ss.

[31] RGPD, Considerando n. 100: «*Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi*».

[32] Una visione critica è riscontrabile in B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali,* in *Federalismi,* 14, 2020*,* 16-19; cfr. L. BROTHERSTON, A. BERLIN, *La sicurezza dei dati e delle reti aziendali, Defensive Security Handbook*; Milano, 68-71. La c.d. "triade CIA" che, attualmente, riveste un ruolo strategico nella cybersicurezza aziendale.

Il primo controllo è la *politica di sicurezza delle informazioni* riguardante la modalità in cui le politiche devono essere redatte nel sistema di gestione della sicurezza delle informazioni e sottoposte a verifica di conformità.

Le politiche di sicurezza generali possono riguardare sia il *core* dell'azienda che la visione globale in una serie di migliori pratiche per condurre i dipendenti al rispetto di alcuni principi rilevanti per l'azienda stessa. È d'uopo sottolineare che all'interno di queste politiche necessarie per un'azienda che si prepara all'implementazione di un algoritmo di *IA bioethics by design*, i valori del RGPD per i dati personali dovranno essere declinati per impedire trattamenti non compliant alla legge, che risultino in procedimenti trasparenti e che conducano gli utenti, nel caso di specie, i pazienti a conoscere le implicazioni delle decisioni degli algoritmi.

Il secondo controllo è *l'organizzazione della sicurezza delle informazioni,* questo analizza i compiti e le azioni che le parti dovrebbero eseguire, sarà obbligo dell'azienda attribuire ruoli e responsabilità in relazione all'implementazione dei principi succitati, in maniera tale che all'interno dell'organizzazione ci sia una sufficiente conoscenza dei ruoli che riguardano le scelte dei dati e quindi l'implementazione finale che dovrà essere eseguita sul consenso informato del paziente.

Il terzo controllo è la *sicurezza delle risorse umane*, concernente il modus con cui i dipendenti devono essere informati sui valori aziendali, sulla sicurezza dei dipendenti e, successivamente, sulla sicurezza del paziente nonché sull'esercizio del libero arbitrio di quest'ultimo senza condizionamenti esterni.

Il quarto controllo è l'*asset management*, si occupa dei processi riguardanti la gestione del patrimonio informativo e su come le unità elementari devono essere protette; l'organizzazione dovrà conservare *hardware, software e database* nonché tutti gli strumenti o i metodi comuni utilizzati per garantire l'integrità dei dati e l'anonimizzazione delle informazioni dei pazienti. Il *virtual landscape* in cui saranno conservate le informazioni dei pazienti, tramite i quali l'algoritmo viene programmato, logicamente, dovranno essere noti e protetti.

Il quinto controllo ha la nomenclatura: *controllo degli accessi*, questo fornisce una guida su come l'accesso dei contrattualizzati dovrebbe essere limitato a diverse tipologie di dati, riveste cruciale importanza poiché un accesso indiscriminato ai dataset che alimenta l'algoritmo potrebbe condurre un cracker ad alterare i processi decisionali delle strumentazioni sanitarie, ledendo non solo la qualità del prodotto ma non consentendo ai pazienti di esercitare i loro diritti e, *ictu oculi*, privandoli della necessaria trasparenza sulle logiche dell'algoritmo.

Il sesto controllo è basato sulla *crittografia,* fondamentale per la protezione dei dati in maniera tale che questi non siano utilizzati da esterni, proteggendo quindi i pazienti da danni risarcibili.

Il settimo controllo riguarda la *sicurezza fisica e ambientale,* analizza quindi i processi per la messa in sicurezza degli edifici e delle attrezzature interne. L'azienda, nel caso concreto sanitaria, dovrà controllare la presenza di eventuali vulnerabilità sul sito fisico, comprese le modalità di accesso agli uffici e ai centri dati, in maniera da neutralizzare i rischi di compromissione dei database e degli algoritmi che potrebbero avere conseguenze altamente negative sull'interazione tra il paziente e la strumentazione.

L'ottavo controllo è denominato *sicurezza operativa* poiché dà indicazioni su come raccogliere e susseguentemente conservare i dati in modo protetto, un processo che assurge a una nuova urgenza grazie al RGPD poiché implica un approccio bioetico nei confronti del singolo dato e, soprattutto, sull'acquisizione di questo.

Il nono controllo si basa sulla *sicurezza delle comunicazioni* e dunque la sicurezza di tutte le trasmissioni all'interno della rete di un'organizzazione. Il processo comunicativo, da Jakobson in poi è fondamentale in quanto sia dati che algoritmo saranno proiettati al di fuori dell'azienda per arrivare sino al letto del paziente. In tali proiezioni, criminali o il mero caso potrebbero ledere il processo qualitativo e non consentire al paziente la garanzia di operare delle scelte basate sulla ragionevolezza.
Il decimo controllo si occupa *dell'acquisizione, dello sviluppo e della manutenzione dei sistemi* in quanto descrive dettagliatamente i processi di gestione dei sistemi in un ambiente sicuro. Il c.d. *sviluppo sicuro* riveste uno dei fondamentali nodi per l'implementazione di un algoritmo di machine learning semantico in tale ambito, precisamente, è tramite lo sviluppo che i primi semi dei processi decisionali vengono piantati dall'organizzazione. Lo sviluppo, quindi, dev'essere controllato adeguatamente e deve consentire al contrattualizzato di codificare le logiche dell'algoritmo suesposte al fine di evitare attacchi che potrebbero inficiarne le logiche concorrendo all'eventualità di conseguenze anche fatali per i pazienti.
L'undicesimo controllo, relativo ai c.d. *stakeholders* riguarda infatti i *rapporti con i fornitori* cioè il modo in cui un'organizzazione deve interagire con terzi garantendo al contempo il rispetto delle normative. Per quanto possa sembrare irrilevante, in realtà, la *supply chain* di un'organizzazione è spesso una delle principali minacce per l'integrità del dataset e dell'algoritmo.
Il dodicesimo controllo risulta essere *l'information security incident management* si occupa della modalità con la quale il sistema risponde agli incidenti sul luogo di lavoro.
Il tredicesimo, strettamente connesso al controllo già indicato, riguarda gli a*spetti di sicurezza informatica della gestione della continuità operativa,* cioè la modalità in cui devono essere gestiti i disagi e i cambiamenti più importanti. Risulta fondamentale redigere delle politiche e delle procedure volte alla valutazione della struttura ospedaliera in virtù di cosa possa aver bisogno per l'assistenza dei pazienti in concerto con i cambiamenti nel software o nei processi decisionali.
L'ultimo controllo, invece, parla di *conformità*, identifica quali sono le normative ordinamentali e/o di settore applicabili per l'organizzazione, concedendo di conoscerne e quindi rispettarne i principi, che assumo piena importanza nell'implementazione di un algoritmo *bioethics by design.*
Il rispetto delle normative succitate, dal RGPD ai meccanismi di certificazione permettono a un algoritmo di AI semantico di riconoscere ciò che il paziente espone e comunica con esso, e di proteggerlo mitigando tutti i possibili rischi.
Occorre, quindi, avallare l'importanza del consenso al trattamento dei dati personali, del consenso informato nel caso di partecipazione a specifici progetti che ne richiedano l'espressione nonché la trasparenza e l'informazione in relazione alle logiche che agiscono «dietro» la macchina[33].

[33] C. GALLOTTI, *op. cit.,* 243 ss.; cfr. C. GALLOTTI, *Vera easy risk assessment.* Versione 7, Milano, 2022.; IEC/TR 80002-1:2009, *Medical decise software, part 1: Guidance on the application of ISO 14971 to medical device software,* Svizzera, 2009; ISO/IEC 270001:2013 *Information technology. Security techinques, code of practice for information security management systems: Requirement*, Svizzera, 2013.

ISSN 2284-4503

4. Un prologo necessario: il dibattito sull'autonomia negoziale e l'assiologia dell'*Artificial Intelligence*

Il contesto socioculturale nel quale si chiede la definizione riqualificata della missione del contratto in base a un novello quadro di valori dimostra l'acuirsi del dibattito sul ruolo dell'autonomia negoziale.
L'Artificial Intelligence dovrebbe, quindi, assurgere a un carattere *sostenibile* quale clausola e/o criterio interpretativo in grado di concretizzare i valori umani e dunque adeguare, caso per caso, gli strumenti antropomorfici di cui l'uomo è detentore nelle attività quotidiane.
Com'è noto, la natura di qualsivoglia istituto è conforme alla sua funzione – che ha prevalenza sulla struttura – e influenza la costruzione degli elementi essenziali degli atti negoziali; ciò che rileva *hic et nunc*, è la ricerca di una fonte costituzionale – e non su base volontaria come le certificazioni internazionali suesposte – di matrice europea nella fattispecie concreta volta a regolare scelte *macrogiuridiche* nelle quali esiste certezza giuridica nella sistemazione delle questioni tecniche di microdiritto[34].

[34] P. PERLINGIERI, *Il «diritto privato» nell'unità del sistema ordinamentale,* in *Rassegna di diritto civile*, 2, 2019, Napoli, 414- 416; dalla prospettiva giurisprudenziale si v. *Cass. Sez. un.,* 17 settembre 2015, n. 18214, in *Riv. Giur. Edil.,* 2015; E. CATERINI, *Lineamenti di diritto civile italoeuropeo. Dal mercato alla persona,* Rende, 2009, 49-52.

ISSN 2284-4503