LUISS

Dipartimento di Giurisprudenza

Cattedra di Diritto Amministrativo I

Diritto di accesso agli atti nell'era digitale

Chiar.mo Prof. Aristide Police

RELATORE

Chiar.mo Prof. Bernardo Giorgio Mattarella

CORRELATORE

Maria Lucrezia Perla matr. 167 923

CANDIDATO

Anno Accademico 2024/2025

Sommario

Introduzione

Già nel 1908, Filippo Turati esprimeva il concetto di "casa di vetro"[1] per l'amministrazione, una metafora che incarna l'aspirazione a un'azione pubblica chiara e trasparente. Tale principio si riflette nella nostra Costituzione, in particolare negli articoli 97, che sanciscono il buon andamento e l'imparzialità, e 98, che stabilisce che i dipendenti pubblici sono al servizio esclusivo della Nazione. A oltre un secolo di distanza, come evidenziato dalla Commissione speciale del Consiglio di Stato, il nostro sistema giuridico si sta orientando verso una completa accessibilità delle informazioni, ove l'obiettivo di potenziare la trasparenza si lega strettamente anche alla necessità di controllare e monitorare la spesa pubblica.

Le recenti riforme volte ad una progressiva informatizzazione dell'attività ammnistrativa potrebbero rappresentare un momento cruciale nell'evoluzione del rapporto fra cittadino e pubblica amministrazione, valorizzando i principi e gli istituti posti in essere dalla l. 241 del 1990.

Tra i detti principi si rinviene quello di trasparenza che, nella sua evoluzione storica e giuridica, da sempre rappresenta la pietra angolare di un ordinamento democratico che aspira a garantire un rapporto equilibrato tra potere pubblico e cittadinanza.

In questo contesto, il diritto di accesso agli atti amministrativi ha segnato un punto di svolta epocale, sancendo il passaggio da un'amministrazione tradizionalmente concepita come autoreferenziale e riservata a un'entità permeabile, orientata al servizio e al controllo diffuso. Questo principio, la cui essenza trova il proprio fondamento in valori costituzionalmente garantiti quali l'imparzialità, il buon andamento e la partecipazione, è stato formalmente codificato nell'ordinamento italiano propri attraverso la Legge n. 241 del 7 agosto 1990. Tale provvedimento ha per la prima volta riconosciuto in capo al privato il potere di interloquire e di conoscere l'agire amministrativo, superando la storica

[1] F. Turati, Atti del Parlamento Italiano, Camera dei Deputati, sessione 1904-1908, 17 giugno 1908

dicotomia tra amministrazione e cittadino e instaurando un rapporto di maggiore apertura e dialogo.
Tuttavia, nel testo originario di questa normativa le potenzialità del diritto di accesso sono rimaste parzialmente inespresse, principalmente per la non intellegibilità della disciplina, che in particolare non precisava qual dovesse essere la situazione giuridica soggettiva del soggetto legittimato all'accesso. Questo dall'altro lato, ha favorito la persistenza da parte della pubblica amministrazione di un atteggiamento autorevole e complessivamente restio ad un'apertura verso l'esterno, impedendo la piena attuazione e degli intenti legislativi.

Il diritto di accesso, nonostante le disposizioni di legge, ha continuato a operare in un quadro di incertezza, caratterizzato da un'ambiguità normativa che ha alimentato un dibattito prolungato e irrisolto tra studiosi e tribunali per circa quindici anni.
Questa mancanza di chiarezza sui caratteri essenziali del diritto di accesso ha reso di fatto impossibile l'automazione delle procedure e l'uso di strumenti informatici o telematici per il suo esercizio. La digitalizzazione, infatti, richiede la "normalizzazione" della disciplina, ovvero la sua traduzione in algoritmi. Un algoritmo è una sequenza finita di passaggi logici e consequenziali, una regola generale e astratta che un computer può applicare a problemi con caratteristiche simili. È evidente che una disciplina ambigua non può essere la base di un processo di questo tipo, in quanto la programmazione informatica necessita di enunciati univoci e chiari per poter elaborare regole astratte e ripetibili.
L'evoluzione normativa di quest'istituto non si è esaurita con la legge 241 del 1990. Difatti, la novella introdotta con la legge n. 15 del 11 febbraio 2005, sembra aprire nuove prospettive al diritto di accesso. Quest'ultima ha segnato un'evoluzione cruciale per il diritto di accesso, conferendogli la dignità di un vero e proprio diritto soggettivo. Questo cambiamento è stato possibile grazie all'influenza delle posizioni dominanti della dottrina e della giurisprudenza, che hanno avuto un impatto sia a livello sostanziale che processuale. Dal punto di vista processuale, un'ulteriore novità è stata introdotta dalla Legge n. 80 del 14 maggio 2005, la quale ha esplicitamente assegnato la giurisdizione esclusiva su questa materia al giudice amministrativo.
La Legge n. 15 del 11 febbraio 2005 ha ulteriormente consolidato la natura del diritto di accesso, elevandolo a "livello essenziale delle prestazioni concernenti i diritti civili e

sociali", rafforzandone così il rango giuridico e la sua centralità nell'architettura del diritto amministrativo.

Un ulteriore, fondamentale passo in avanti è stato compiuto con il Decreto legislativo n. 33 del 14 marzo 2013, che ha introdotto il concetto di "accesso civico", ampliando la sfera di conoscibilità dell'operato della pubblica amministrazione e promuovendo una cultura della trasparenza come strumento di prevenzione della corruzione.

Oggi il cittadino ha un diritto e specularmente la pubblica amministrazione un obbligo di ostensione, ossia un preciso dovere di esporre i documenti richiesti, rendendo le prospettive per l'informatizzazione del processo di accesso molto più concrete. In sostanza, questa chiarezza normativa rende più realistico l'obbiettivo di un esercizio automatizzato del diritto.

La piena concretizzazione di questo potenziale può generare molteplici vantaggi. L'azione amministrativa acquisisce maggiore trasparenza, poiché la conoscibilità degli atti condiziona e spinge l'amministrazione ad agire con maggiore correttezza e diligenza, abbandonando la tradizionale riservatezza. Si favorisce inoltre una partecipazione più efficace da parte dei privati, che, avendo accesso alle informazioni detenute dall'amministrazione, possono contribuire in modo più utile e informato al processo decisionale. Infine, si garantisce una maggiore imparzialità della funzione e della decisione amministrativa, grazie a un'istruttoria più completa che beneficia degli elementi conoscitivi, come fatti e interessi, forniti dai partecipanti.

Dall'altro lato bisogna tenere conto che non mancano di profilarsi anche taluni aspetti problematici. Il più importante fra tutti è rappresentato dalla considerazione che l'automazione, anche non necessariamente in ambito ammnistrativo, determina di per sé una perdita della creatività dell'attività, essendone presupposto essenziale la costante identità degli elementi e dei passaggi dei procedimenti, motivo per cui l'automazione può essere concepita solo con riguardo ad attività per loro natura ripetitive.

Contemporaneamente a questa complessa evoluzione della disciplina normativa, è stata imposta una profonda riconsiderazione delle modalità di esercizio e delle finalità del diritto di accesso, dovuto principalmente all'avvento dell'era digitale. Difatti, la digitalizzazione non viene più concepita come uno strumento operativo, ma costituisce un elemento strutturale che incide in modo determinate sulla configurazione dello stesso potere pubblico, come chiarito dal Codice dell'Amministrazione Digitale (CAD). Si tratta

di uno scenario inedito che ha sollevato la necessità di conciliare la trasparenza con le nuove sfide poste dalla gestione massiva dei dati, dalla sicurezza informatica e, soprattutto, dalla protezione dei dati personali.

Inoltre, merita di essere menzionata anche l'entrata in vigore del Regolamento (UE) 2016/679 (GDPR) che concorrendo a ridefinire il quadro normativo in materia, ha imposto un delicato bilanciamento tra il diritto alla conoscenza e il diritto alla riservatezza, il quale ormai assurge a diritto fondamentale.

Premesso ciò, il presente elaborato si propone di analizzare criticamente questo intricato percorso, partendo dall'analisi del fondamento costituzionale del diritto di accesso per poi ripercorrerne le tappe normative essenziali. Il primo capitolo sarà dedicato all'esame dei principi cardine che ne sono alla base: trasparenza, pubblicità e partecipazione. Successivamente, verrà affrontata l'influenza della transizione digitale sulla disciplina dell'accesso, focalizzandosi sull'impatto della digitalizzazione sui procedimenti amministrativi e sul ruolo del CAD. Infine, il lavoro si concentrerà sull'ambito più sensibile e complesso: il diritto di accesso ai dati sanitari. L'analisi di questo settore specifico consentirà di esaminare la difficile armonia tra il diritto di accesso, la tutela della salute pubblica e la privacy, evidenziando le sfide e le soluzioni normative necessarie per garantire un'applicazione consapevole e ponderata delle norme vigenti, nel pieno rispetto della dignità della persona e dei valori fondamentali dell'ordinamento.

Capitolo I

Fondamento del diritto di accesso agli atti amministrativi

1.1 Trasparenza, pubblicità, partecipazione: i pilastri del diritto di accesso

Sul piano logico-sistematico, l'analisi della natura del diritto di accesso impone una preliminare e approfondita riflessione sul suo fondamento costituzionale. A partire dall'interpretazione del dato letterale della Costituzione, dottrina e giurisprudenza hanno enucleato una vasta gamma di connessioni significative tra questo istituto e i precetti della Carta costituzionale. Tale correlazione deriva dalle ampie potenzialità intrinseche del diritto di accesso, le quali gli consentono di soddisfare tanto interessi superindividuali di rilevante importanza, quanto esigenze strettamente personali.

La presente trattazione intende ripercorrere, seppur con un approccio non esaustivo, la problematica in esame, prendendo avvio dall'assunto normativo che qualifica l'accesso come mezzo imprescindibile per garantire la partecipazione, la quale conduce alla trasparenza e, per tale via, all'imparzialità dell'agire amministrativo.
La trasparenza è generalmente intesa come criterio applicativo della pubblicità, che a sua volta si configura come principio costituzionale implicito, frutto di una ricostruzione ermeneutica basata su precetti costituzionali espressi, quali il principio democratico, di sovranità popolare, di informazione, di difesa, di imparzialità e di buon andamento dell'amministrazione, e da altri principi da essi deducibili, come lo Stato di diritto e lo Stato sociale.
Inoltre il principio di trasparenza è un principio generale del diritto amministrativo, la cui rilevanza non si esaurisce nell'ambito del procedimento amministrativo. Proprio sulla base della riconosciuta natura poliedrica del principio di trasparenza, la cui realizzazione non si esaurisce nell'ambito del procedimento, essa garantisce ai cittadini la possibilità di

accedere a informazioni sull'assetto organizzativo e sulle operazioni delle pubbliche amministrazioni anche in contesti non strettamente legati a contesti specifici.

Ciò spiega perché, in Italia come in altri ordinamenti, vi sono diverse declinazioni della trasparenza amministrativa espressione di due modelli fondamentali: quello del diritto di accesso ai documenti da parte degli interessati e quello dell'informazione ai cittadini. Tale principio si sostanzia in un complesso di attività ed operazioni finalizzate a garantire, o quantomeno a favorire, la conoscenza di specifici fatti giuridici, la cui importanza è riconosciuta dall'ordinamento. Gli atti e i fatti oggetto di conoscenza acquisiscono la qualifica di pubblici, intendendo con ciò la loro natura di non riservati e non segreti, ovvero conoscibili. Sebbene l'incisiva rilevanza della pubblicità nel determinare la correttezza dell'agire amministrativo fosse stata già affermata ben prima dell'entrata in vigore della costituzione, è nel contesto dell'evoluzione democratica del nostro ordinamento che si registra una più intensa elaborazione concettuale in merito. La pubblicità dei poteri pubblici si presenta come un aspetto strutturale e imprescindibile della fisionomia democratica dello Stato. Senonchè l'affermarsi di questo principio nei rapporti fra cittadini e pubblica amministrazione non è stato, e non è tuttora, agevole. Difatti, l'ordinamento democratico ha ereditato una pubblica amministrazione, la cui originaria configurazione era propria di un sistema autoritario, rendendola pressoché insensibile alle istanze di democratizzazione, che al contrario hanno permeato gli altri poteri statali. Ciò spiega la rigorosa disciplina previgente sul segreto di ufficio, come si evince dall'art. 15 del T.U. sugli impiegati civili dello stato[2]. Inoltre La segretezza era intrinsecamente favorita dall'organizzazione fortemente gerarchizzata dell'amministrazione, impedendo di fatto la circolazione delle informazioni anche al suo interno. Ciò si poneva in aperto contrapposto con la configurazione dell'amministrazione definita dalla norme costituzionali , in particolare negli artt. 2,5,97,98, delle quali tuttavia è stata data un'interpretazione restrittiva, ritenendole generiche e pertanto non immediatamente precettive, permettendo in questo modo alla pubblica amministrazione di mantenere un'organizzazione anacronistica, inadatta all'evoluzione dell'ordinamento.

[2] Tale disposto prevedeva che: "L'impiegato deve mantenere il segreto d'ufficio e non può dare a chi non ne abbia diritto, anche se non si tratti di segreti, informazioni o comunicazioni relative a procedimenti ed operazioni amministrative di qualsiasi natura, e notizie delle quali sia venuto a conoscenza a causa del suo ufficio, quando possa derivarne un danno per l'Amministrazione o per terzi. Nell'ambito delle proprie attribuzioni l'impiegato preposto ad un ufficio rilascia, a chi ne abbia interesse, copie ed estratti di atti e documenti d'ufficio, nei casi non vietati dalla legge, dai regolamenti o dal capo di servizio".

La legge 241 del 1990, e ancor prima la normativa sugli enti locali rappresentano un evidente manifestazione della volontà di includere, pur se tardivamente, l'amministrazione nelle trasformazioni democratiche che hanno interessato il nostro ordinamento. Per questo motivo, la Legge n. 241 del 1990 è da alcuni considerata una rivoluzione copernicana[3] per il nostro ordinamento. D' altro canto, non manca chi sostiene che tale normativa e normativa sia stata attribuita un'importanza eccessiva rispetto alla sua effettiva portata, dato che, innanzitutto, essa è una legge di rango ordinario e, secondariamente, si limita a riprodurre principi e regole già impliciti o desumibili dal dettato costituzionale. É importante sottolineare come la l. 241 del 1990 abbia avuto un ruolo fondamentale nel rendere la trasparenza carattere fondamentale e imprescindibile dell'azione amministrativa, verso la cui concreta attuazione la legge stessa è costantemente orientata, imponendo in tal senso precisi vincoli all'amministrazione stessa. Essa si configura come una modalità intrinseca di essere e di operare dell'amministrazione, manifestandosi attraverso una pluralità di istituti e comportamenti volti a renderne conoscibile l'attività. A ben vedere questa concezione non si discosta significativamente da quella di pubblicità appena esposta, anche dal punto di vista semantico le due espressioni presentano infatti significati affini e contigui. La pubblicità si manifesta attraverso l'intrinseca accessibilità, la piena conoscibilità, la libera frequentabilità e l'universale utilizzabilità del suo oggetto da parte di chiunque essendone la proprietà condivisa con la generalità. La pubblicità si presenta come un concetto dinamico, più precisamente come un processo dinamico, la cui funzione è quella di portare alla luce un oggetto rendendolo comprensibile e alla portata di tutti. Per conto, la trasparenza rappresenta una qualità statica e inerente, un attributo che l'oggetto assume come risultato di tale processo. Tali concetti dunque si pongono, almeno al livello teorico, in un rapporto di genere a specie, ma in pratica tale relazione risulta essere sempre più sfumato, lasciando sempre più spazio alla prospettazione di integrazione e complementarietà reciproca, come sostenuto dalla dottrina maggioritaria.

L'articolo 22 della l. 241 del 1990 sancisce una connessione indissolubile tra la trasparenza dell'azione amministrativa e il principio di imparzialità. Tale disposizione cristallizza il nesso causale tra la piena accessibilità ai documenti e la garanzia di

[3] F. Pubusa, Diritto di Accesso e automazione, Giappichelli, Torino, 2006

un’attività amministrativa non discriminatoria e obiettiva. La conoscibilità dell’attività amministrativa ha trasformato radicalmente il suo operato. Difatti, l’amministrazione è tenuta a svolgere le prove funzioni in piena pubblicità, agendo cioè “alla luce del sole”, il che si traduce in un abbandono della tradizionale riservatezza a favore di un esercizio trasparente e apertamente accessibile. Dal punto di vista dei cittadini, questa evoluzione si traduce in un potere di vigilanza e controllo continuo sulle attività amministrative in corso, determinando il sorgere in capo all’amministrazione da un lato, dello stimolo di operare con maggiore diligenza; dall'altro, impone la necessità di agire sempre in maniera corretta, controllata ed equa, sapendo di essere sotto gli occhi della collettività. La crescente attenzione dell’amministrazione alla sfera giuridica dei soggetti coinvolti dovrebbe condurre ad un trattamento non discriminatorio, in base al quale situazioni uguali sono trattate nello stesso modo e situazioni diverse in modo differente. Conseguentemente gli interessi coinvolti nell’azione amministrativa dovranno essere ponderati in modo congruo, consentendo di perseguire l’interesse pubblico senza sacrificare eccessivamente gli interessi individuali. Ed è in ciò che si sostanzia l’imparzialità, la cui realizzazione passa necessariamente attraverso il rispetto del principio di uguaglianza tanto nella sua accezione formale quanto sostanziale.

Ulteriore implicazione sottesa all’esercizio di un’attività amministrativa corretta leale ed equa consiste nell’osservanza del principio di buon andamento tradizionalmente inteso.

Tuttavia la trasparenza non è un concetto limitato al rapporto tra pubblica amministrazione e cittadino, ma ha un importante risvolto interno all’apparato amministrativo stesso, assicurando una diffusa conoscibilità non solo tra i diversi organi e uffici di un determinato apparato, ma anche fra diverse amministrazioni. In questo modo non solo si facilita lo scambio di informazioni tra le varie entità amministrative, ma si previene l’inutile spiego di risorse, dal momento che la collaborazione agevola notevolmente la condivisione del carico di lavoro. Da ciò si può facilmente dedurre che ulteriore implicazione della trasparenza dell’azione amministrativa è la sua semplificazione, la quale a sua volta assicura un esercizio adeguato e corretto del potere pubblico, che si traduce in un miglioramento dell’efficienza, efficacia ed economicità dell’attività amministrativa complessivamente considerata.

É palese, dunque, che la trasparenza trova il proprio fondamento costituzionale primariamente nell'art. 97 Cost. e, per questa via, anche nell'art. 3. Ma la trasparenza, intesa come strumento volto a rendere conoscibili l'agire amministrativo, concorre in maniera decisiva anche all'attuazione di un ulteriore precetto costituzionale, così come enunciato all'art. 21 Cost., nel quale trova espressione la libertà di manifestazione del pensiero, ma anche la libertà di informazione. Quest'ultima non si configura tanto come libertà volta a cercare ed acquisire determinate notizie, quanto piuttosto come la possibilità di apprendere conoscenze di carattere generale e di utilizzare diverse fonti di informazione, a prescindere dal contenuto particolare delle notizie in esse veicolate.

Pertanto è fondamentale interpretare in maniera ampia e sistematica non solo l'art. 21, ma anche tutte le altre norme costituzionali relative alle questione dell'informazione, al fine di far si che che la libertà di informazione sia riconosciuta come diritto autonomo e distinto dalla semplice libertà di espressione del pensiero. Sulla scorta di questa interpretazione il precetto dell'art. 21 cost. dovrebbe essere letto come se riconoscesse che "tutti hanno diritto di usare ogni fonte di informazione disponibile per diffondere il proprio pensiero". La libertà di informazione si manifesta concretamente attraverso il diritto a ricercare informazioni e il diritto ad avere accesso a fonti informative. Questi due aspetti sono indissolubilmente legati, perché l'uno non può esistere pienamente senza l'altro, e perderebbe significato in assenza del suo complementare. Pertanto l'interpretazione ampia e sistematica dell'art. 21 e delle altre norme costituzionali relative alla problematica dell'informazione contribuiscono alla configurazione di un sistema dove la libertà di informazione e la libertà di manifestazione del pensiero si valorizzano e si rafforzano reciprocamente.

Questa impostazione è perfettamente in linea con la realtà attuale, caratterizzata sia dall'influenza dominante dei media, sia dall'enorme volume di dati e notizie, sia dalla loro rapidissima, quasi immediate, diffusione. Nella società odierna, propriamente definita "società dell'informazione" la possibilità di informarsi e di accedere alle fonti funge da essenziale contrappeso ai poteri derivanti dalla libertà di espressione di coloro che gestiscono la diffusione delle notizie.

Come ben si sa anche gli artt. 24 e 113 cost. Costituiscono un fondamento costituzionale della trasparenza. Il primo di essi, l'articolo 24, riconosce il diritto di agire in giudizio

per difendere i propri diritti ed interessi legittimi. Il secondo, ancor più specificatamente, garantisce la possibilità di ricorrere in sede giurisdizionale contro gli atti della pubblica amministrazione. Per potersi difendere efficacemente, è necessario avere piena conoscenza degli atti e dei fatti che li riguardano, il che implica la conoscibilità dell'azione amministrativa come presupposto per garantire l'effettività del diritto di difesa, concorrendo altresì a ridurre il ricorso al giudice.

In definitiva, il principio di trasparenza, può ben essere ritenuto un precetto costituzionale implicito desumibile dal principio di uguaglianza, dalla libertà di manifestazione del pensiero, dal principio di difesa in giudizio, o ancora, dei principi di legalità, imparzialità, buon andamento.

Inoltre non possiamo trascurare il principio democratico e di sovranità popolare, enunciati nell'art.1 cost. La capacità dei cittadini di **c**onoscere l'attività amministrativa e, più in generale, l'operato dei poteri pubblici, è sia una diretta espressione sia un'applicazione pratica del principio di democraticità del nostro sistema. Questo significa che il potere pubblico non deve solo ottenere la sua legittimazione dal popolo (dal "basso"), ma deve anche essere esercitato "in pubblico", in modo tale da garantire ai cittadini la possibilità concreta di controllare come viene gestita la cosa pubblica[4]. La trasparenza, quindi, diventa il mezzo attraverso cui il cittadino, titolare della sovranità, può effettivamente esercitare un controllo sull'azione detiene il potere.

In quanto strumento teso ad assicurare la trasparenza e l'imparzialità dell'attività amministrativa, il diritto di accesso ha un inconfutabile fondamento nella Carta costituzionale: consiste in tutti i principi e i diritti costituzionali che la trasparenza concorre a rendere effettivi.

Segnatamente, il diritto di visionare ed ottenere copia dei documenti che la pubblica amministrazione possiede al fine di rendere le sue attività conoscibili al pubblico, cioè trasparenti. Il che implica per i cittadini la possibilità di controllare se l'amministrazione stia agendo in modo corretto, equo e legittimo nel corso dello stesso esercizio del potere

[4] Clemente di San Luca G., Diritto di accesso e interesse pubblico, Jovene Editore Napoli, 2006. Sul punto si veda anche ABISINNI F. G., Germania, in MATTARELLA B. G., L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto, Napoli, Editoriale Scientifica, 2018.

pubblico. Questo consente ai cittadini ai cittadini di tutelare immediatamente i propri diritti mentre l'azione amministrativa è in corso, senza adire direttamente il giudice. Difatti, il diritto di accesso consente di influenzare ed anche correggere l'orientante dell'amministrazione, rendendo la partecipazione dei privati più utile al processo decisionale. Tale partecipazione si rivela di particolare importanza anche quando il procedimento si sia concluso ed il privato decide di contestare una decisione. Le argomentazioni difensive potranno essere scritte avendo una conoscenza più completa degli elementi di fatto e di diritto su cui si basa la decisione amministrativa, facendo si che I i ricorsi non vengano più presentati "al buio", ma su basi solide e informate.

Quanto all'amministrazione, è evidente che la costante conoscibilità della sua attività ne condiziona il modo di operare, e anzi la stimola ad essere più corretta, legittima, equa nel suo agire.

In sintesi, il diritto di accesso ai documenti amministrativi è di cruciale importanza perché garantisce il diritto alla difesa e la possibilità di contestare decisioni della pubblica amministrazione, come previsto dagli articoli 24 e 113 della carta costituzionale. Inoltre assicura che l'amministrazione agisca in modo imparziale, efficiente e nel rispetto della legge, come stabilito dall'articolo 97 della Costituzione. Proprio per queste ragioni il diritto di accesso garantisce anche il principio di uguaglianza: se tutti hanno la possibilità per controllare l'operato della pubblica amministrazione, si crea il presupposto per assicurare che i principi sopraindicati siano rispettati.

Inoltre, la conoscibilità di cui stiamo parlando, permette di concretizzare anche i diritti d informarsi e ad essere informati, i quali sono fondamentali per la formazione del proprio pensiero, la cui libertà d'espressione è sancita nell'art. 21 della nostra costituzione;
quindi, indirettamente il diritto di accesso concorre a rendere effetti anche altri precetti costituzionali, quali gli artt. 1,2,3,32,33,41,48 cost.
Oltre a ciò che la dottrina e la giurisprudenza hanno stabilito, bisogna aggiungere un'importante previsione normativa: l'articolo 22 che è stato modificato e aggiornato. Il dettato normativo di quest'ultimo sottolinea le grandi finalità di interesse pubblico che stanno dietro al diritto di accesso, le quali sono così importanti da elevare il diritto di accesso a principio fondamentale dell'agire amministrativo. D'altronde il suo scopo è chiaro e consiste nel favorire a partecipazione dei cittadini e garantire che

l'amministrazione sia trasparente e imparziale. L'articolo stabilisce che l'accesso *"attiene ai livelli essenziali dei diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale ai sensi dell'art. 117, secondo comma, lettera m, della costituzione".* Questa norma dimostra che il legislatore non si è limitato a ribadire lo scopo del diritto di accesso, già chiaro nella versione precedente dell'articolo 22, ma l'ha arricchito con riferimento alla partecipazione. Si tratta di un richiamo importante sotto molteplici aspetti, specialmente perché evidenzia la stretta connessione che esiste fra i due istituti, dove il primo rappresenta un naturale presupposto del secondo.

In conclusione, possiamo dire che l'accesso ha dunque di un ampio fondamento costituzionale: le sue funzioni e le sue caratteristiche lo rendono un strumento cruciale per mettere in pratica molteplici precetti stabiliti nella nostra carta costituzionale.

1.2 Quadro normativo di riferimento

Il percorso per raggiungere la trasparenza normativa in Italia è stato un viaggio lungo e complesso , caratterizzato da diverse tappe normative ed ancora oggi in continua evoluzione. Tale percorso inizia con la legge 816/1985[5], il cui articolo 25 riconosceva a «tutti i cittadini» il «diritto di prendere visione di tutti i provvedimenti adottati dai comuni, dalle province, dai consigli circoscrizionali, dalle aziende speciali di enti territoriali, dalle unità sanitarie locali, alle comunità montane», prevedendo altresì il dovere per le amministrazioni di disciplinare in via regolamentare «l'esercizio di tale diritto». Successivamente alla legge 816/1985, seguì la legge 349/1986, la quale prevedeva il dovere per il ministro di garantire la più ampia divulgazione delle informazioni sullo stato dell'ambiente e riconosceva in capo a "qualsiasi cittadino il diritto di accesso alle informazioni sullo stato dell'ambiente disponibili, in conformità delle leggi vigenti, presso gli uffici della pubblica amministrazione"[6] e di ottenerne copia.

[5] Si veda la Legge 27 Dicembre 1985 n. 816 recante "Aspettative, permessi e indennità degli amministratori locali".

[6] art, 14, comma 3 della legge 349/1986 recante "Istituzione del Ministero dell'ambiente e norme in materia di danno ambientale"

La legge 349/1986 costituiva, in parte, il recepimento nell'ordinamento italiano della direttiva europea 85/337/CEE, relativa alla valutazione dell'impatto ambientale (anche detta VIA) di specifici progetti pubblici e privati. Quest'ultima imponeva agli Stati membri di rendere disponibili al pubblico le richieste di autorizzazione e le informazioni raccolte durante l'istruttoria della valutazione d'impatto ambientale. Altresì richiedeva di definire e specificare le modalità e i luoghi per la consultazione e l'informazione, oltre a stabilire i criteri per la pubblicazione della procedura, al fine di facilitare l'esercizio del diritto di accesso alle informazioni ambientali. Dopo l'introduzione di ulteriori norme, che regolavano l'accesso agli atti amministrativi in settori specifici, il principio della trasparenza amministrativa venne affermato in maniera definitiva, come è noto, con l'entrata in vigore della legge 241 del 1990 sul procedimento amministrativo.

Prima dell'avvento della legge 241 del 1990, la situazione italiana si contraddistingueva per una smisurata discrezionalità nella gestione del procedimento amministrativo da parte dell'amministrazione procedente e per il mancato riconoscimento in capo ai cittadini del diritto di partecipare al procedimento. Tuttavia, il clima culturale stava progressivamente mutando, sulla base di un forte desiderio, diffuso sia fra i cittadini che fra gli esperti del settore, di avere un'amministrazione più dialogante e attenta ai loro diritti e interessi. Proprio per tali ragioni era giunto il momento propizio per accogliere quella che sarebbe stata la più importante legge sul procedimento amministrativo. Finalmente il 7 agosto 1990 si giunse all'approvazione della legge 241, intitolata "*nuove norme in materia di procedimento amministrativo e di diritti di accesso ai documenti amministrativi".* Quest'ultima ha definito una serie di principi fondamentale dell'agire della pubblica amministrazione e introduce nuovi e importanti istituti, stabilendo regole generali sia per la partecipazione dei cittadini al processo decisionale dell'amministrazione, che per la semplificazione delle procedure burocratiche, ma ha anche regolato l'istituzione della figura del responsabile del procedimento, una persona di riferimento per ogni pratica.

A conferma di ciò l'articolo 1, primo comma della legge 241/90, afferma che:

«l'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di pubblicità e trasparenza secondo le modalità previste dalla l. 241/90 e dalle disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario».

Pertanto la legge 241 del 1990 rappresenta il primo vero e proprio punto di svolta verso una pubblica amministrazione più trasparente nei confronti dei cittadini, dal momento in cui segna il passaggio da un sistema in cui l'amministrazione operava in segreto, a uno basato sulla trasparenza e sulla pubblicità. Questi nuovi principi non sono fini a sé stessi, ma sono una diretta conseguenza di valori fondamentali come la legalità, l'imparzialità e il buon andamento dell'amministrazione, tutti garantiti dall'articolo 97 della Costituzione. Dunque con l'avvento di tale legge si è incominciato a parlare in maniera concreta di trasparenza amministrativa, con il chiaro obbiettivo di trasformare radicalmente il sistema amministrativo spesso incomprensibile e chiusa in una realtà aperta e accessibile, soprattutto attraverso i suoi atti. Ciò è sostenuto dall'articolo 22 della suddetta legge, il quale stabilisce che del diritto di accesso inteso «diritto di prendere visione ed estrarre copia dei documenti amministrativi», possono avvalersi «tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso». Difatti, il Consiglio di stato ha dichiarato il proprio orientamento interpretativo, sostenendo che « l'interesse che legittima la richiesta di accesso, oltre ad essere serio e non emulativo, deve essere personale e concreto, ossia ricollegabile alla persona dell'istante da uno specifico nesso: in concreto occorre che il richiedente intenda difendere una situazione di cui è portatore, qualificata dall'ordinamento come meritevole di tutela, non essendo sufficiente il generico e indistinto interesse di ogni cittadino alla legalità o al buon andamento della attività amministrativa » . Quindi, l'accesso ai documenti può essere richiesto solo da chi possiede un interesse specifico e concreto relativamente ad essi e deve riguardare atti e documenti ben precisi[7]. Conseguentemente deve ritenersi inammissibile la richiesta di accesso a documenti della pubblica amministrazione che risulti essere eccessivamente generica poiché l'eventuale soddisfazione di tale richiesta avrebbe implicato una complessa attività di ricerca e catalogazione, non facente parte dei doveri posti in capo all'amministrazione. In sintesi possiamo affermare che il diritto di accesso ai documenti

[7] sul punto si veda anche T.A.R. , Roma , sez. II , 02/10/2023 , n. 14553, secondo cui "Ai sensi dell' art. 22, comma 2, l. n. 241/1990 , l'accesso attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza, e ai sensi dell'art. 24, comma 7, deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi, la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici.

amministrativi subisce limitazioni sia soggettive, quindi relative a chi può richiederlo, che oggettive, relative an quali documenti si possono richiedere, ma anche funzionali, che circoscrivono lo scopo per cui l'accesso può essere richiesto. Questo implica che non è possibile utilizzare l'accesso per controllare genericamente tutto quello che fa la pubblica amministrazione. Non essendo inteso come uno strumento per la società civile ideato al fine di esercitare un controllo democratico sul processo decisionale dell'amministrazione.
Molto importante è il significato giuridico del novellato articolo 22, secondo comma , il quale stabilisce che l'accesso ai documenti amministrativi si eleva a principio fondamentale dell'agire amministrativo ed è ritenuto di cruciale importanza sia per tutelare i diritti di partecipazione dei cittadini, sia per assicurare l'imparzialità e la trasparenza dell'attività amministrativa, che sono concetti strettamente connessi con la partecipazione. L'accesso è talmente importante da essere equiparato ai livelli essenziali delle prestazioni che riguardano i diritti civili e sociali. Questi ultimi, come ben sappiamo, sono costituzionalmente tutelati e dal 2001 la loro regolamentazione è stata assegnata in via esclusiva allo stato, com e indicato dall'articolo 117, comma 2, lettera m, della costituzione.
La genericità della definizione consente dunque di rendere accessibile tutti gli atti e documenti, anche in formato digitale, posseduti dai pubblici uffici e quindi tanto atti intra-procedurali che tanto atti esterni al procedimento, anche relativi ad altri procedimenti amministrativi. Il privato non sarà tenuto ad indicare l'eventuale numero di protocollo dell'atto che intende visionare, in quanto è sufficiente fornire i documenti o i dettagli che ne definiscono il contenuto.
Il diritto di accesso non è di per sé illimitato, in quanto è subordinato alla dimostrazione da parte dell'istante di un interesse concreto, diretto, attuale e meritevole di tutela. In pratica il richiedente deve rendere note le motivazioni che lo inducono a farlo, indicando non solo il legame tra sé stesso e l'interesse che vuole proteggere, ma anche provare che questa necessità è attuale, cioè esiste nel presente. [8]
Inoltre va detto, che il diritto di accedere ai documenti non è concesso solo alle pubbliche amministrazioni, ma riguarda anche riguarda anche enti pubblici economici, aziende autonome gestori di servizi pubblici che, pur essendo privati, si occupano di attività e servizi di interesse pubblico.

[8] In tal senso si veda anche TAR Roma, sez. II, 2 ottobre 2023, n. 14553, op. cit.

L’articolo 24 elenca i casi in cui il diritto di accesso è escluso, ponendo vari limiti, alcuni dei quali di carattere assoluto. Specificatamente questi limiti riguardano documenti coperti dal segreto di stato, procedimenti relativi a sequestri di persona e alla protezione dei testimoni di giustizia, documenti che sono già protetti da un segreto o un divieto di divulgazione, documenti esclusi per mezzo di regolamenti specifici del governo e sono posti al fine di tutelare interessi pubblici fondamentali che vengono considerati più importanti di quelli dei singoli cittadini.

Con l’avvento della legge 241 del 1990 sono stati chiaramente delineati quali documenti l'amministrazione non può rifiutarsi di fornire in copia e le condizioni e i limiti entro cui si può esercitare il diritto di accesso.

Inoltre la legge ha definiti i tempi massimi entro cui l’amministrazione è chiamata a decidere e ha precisato cosa accada quando l’amministrazione non risponde, come nel caso del cosiddetto silenzio-assenso o silenzio rigetto. Viene anche definito il responsabili del procedimento che rappresenta il soggetto cui bisogna rivolgersi per superare le difficoltà burocratica e per velocizzare il procedimento.

Il punto di forza di questa legge consiste nell’aver fornito regole precise a cui l’amministrazione si deve attenere per tutelare i diritti e gli interessi dei cittadini.

Il contributo più significativo della legge sul procedimento amministrativo è stato il miglioramento del rapporto tra i cittadini e la Pubblica Amministrazione, in particolare stabilendo come l’amministrazione deve svolgere la propria attività al fine di rispettare i principi dettati, limitando la discrezionalità di cui essa godeva.

Tale legge, posta in essere sulla scorta di uno spirito di rinnovamento generale dei rapporti tra cittadini e potere pubblico, ha subito nel corso del tempo molteplici modifiche volte a integrarne il contenuto.

Negli anni successivi, La legge 241 del 1990 ha subito numerose e significative modifiche. Queste sono state introdotte principalmente dalla Legge 15/2005, intitolata "Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa”. In seguito, il decreto legge 35 del 2005, conosciuto anche come decreto-legge sulla competività ha apportato successive modifiche a diversi aspetti della stessa normativa. La legge n. 15 del 2005 ha radicalmente innovato la legge sul procedimento amministrativo e ha definito una regolamentazione più organica e completa in materia di accesso ai documenti, disciplinata dagli arti. 22 e seguenti.

Pur mantenendo inalterata la struttura originale delle legge, i due provvedimenti sopracitati ne hanno modificato e integrato il contenuto. Lo scopo era rendere le pubbliche amministrazioni più efficienti e migliorare il loro rapporto con i cittadini, oltre che adeguare il contenuto della legge ai cambiamenti avvenuti nel frattempo nel sistema costituzionale e normativo.

Le novità introdotte dalla suddetta normativa possono essere ricondotte prevalentemente a cinque ambiti, rendendola più semplice da consultare. Il primo ambito concerne l'introduzione di nuovi principi che regolano l'agire della pubblica amministrazione. Difatti, la trasparenza è ormai una regola generale ed esplicita che guida l'attività della pubblica amministrazione, il cui operato può essere costantemente controllato e valutato. Inoltre l'amministrazione nell'esercizio delle sue funzioni è sempre tenuta a conformarsi e a rispettare i principi dell'ordinamento comunitario. Un ulteriore principio generale è sancito al comma 1 bis dell'articolo 1 della legge sul procedimento amministrativo, secondo il quale "la pubblica amministrazione agisce secondo il diritto privato, salvo che la legge disponga diversamente, nell'adozione di atti di natura non autoritaria". Ciò implica che l'amministrazione deve agire secondo le stesse regole dei privati quando non esercita poteri autoritativi, salvo che ci sia una legge che stabilisca diversamente.

Uno dei principi più rilevanti in materia di diritto di accesso agli atti della pubblica amministrazione è quello introdotto con l'articolo 3 bis della legge 15/2005, ossia l'uso della telematica al fine di migliorare i rapporti tra amministrazione e cittadini. Tale principio è stato ripreso e sviluppato in maniera più esaustiva nel Codice dell'amministrazione digitale, approvato con d.lgs.82/2005.

Il secondo ambito delle novità introdotte concerne lo svolgimento dell'intero procedimento amministrativo. Per esempio le modifiche stabiliscono che nella comunicazione con cui si da notizia dell'avvio del procedimento, l'amministrazione è tenuta ad indicare anche la data entro cui si concluderà. Inoltre è tenuta a specificare le conseguenze in caso di inerzia della stessa amministrazione e gli eventuali rimedi esperibili dal cittadino Per i procedimenti avviati dai privati, deve essere specificata anche la data di presentazione della loro richiesta (come previsto dall'articolo 8, comma 2, lettera c).

Un ulteriore novità è stabilita nell'articolo 10 bis nel quale si afferma che dove l'amministrazione decida di non accogliere una richiesta deve avvisare gli interessati,

prima della formale conclusione del procedimento mediante adozione del provvedimento negativo, al fine di permettere agli interessati stessi di presentare eventuali osservazioni o documenti, dei quali l'amministrazione dovrà tenere conto nell'adozione della decisone finale. Infine, se l'amministrazione dovesse conferire il rifiuto dovrà indicare chiaramente, nelle motivazioni, perché non ha ritenuto valide le obiezioni o gli elementi aggiuntivi forniti dalla controparte.

Il terzo ambito riguarda la disciplina in tema di silenzio. Gli articoli 19 e 20 della legge 241 del 1990 sono stati integralmente riscritti dal Decreto Legge 35/2005[9] . Quest'ultimo ha portato all'introduzione degli istituti della denuncia di inizio attività, che viene rinominata Dichiarazione di inizio attività (DIA) e del silenzio assenso.

Il quarto ambito che è stato riformato è quello relativo al provvedimento finale, mediante la legge 15/2005 è stato aggiunto all'articolo 21 un intero Capo (il IV-bis) che introduce le norme relative a efficacia, esecutorietà, esecutività, revoca, recesso, nullità, annullabilità, annullamento d'ufficio e convalida.

Il quinto e ultimo ambito che riguarda direttamente il tema dell'accesso, si distingue per una completa rivisitazione della stessa normativa. In particolare l'articolo 22 è stato integralmente riscritto, preoccupandosi ora di definire espressamente il diritto di accesso, a differenza della normativa precedente, indicandolo come la facoltà per le persone interessate di visionare e ottenere copie dei documenti amministrativi. É importante tener distinto questo specifico diritto di accesso, conosciuto come "accesso conoscitivo" o "informativo" , dal cosiddetto accesso "partecipativo" regolato dal precedente articolo 10.

Le radici del cosiddetto diritto di accesso conoscitivo si rinvengono negli articoli 97 e 98 della costituzione, che enunciano il principio del buon andamento dei pubblici uffici.

É importante notare che prima della legge 241 del 1990 era stata affermata nella dottrina la regola della riservatezza e la segretezza delle istruttorie amministrative. Con l'introduzione di questa legge la riservatezza è diventata un'eccezione, e i casi in cui l'accesso è escluso sono stati specificamente elencati dal legislatore. In seguito, la legge 15 del 2005 ha ribadito questo concetto, innovando l'articolo 22 della legge 241 del 1990, e ha consentito di elevare il diritto di accesso a principio fondamentale dell'attività

[9] Decreto legge 14 marzo 2005, n. 35 recante "Disposizioni urgenti nell'ambito del Piano di azione per lo sviluppo economico, sociale e territoriale" convertito poi nelle legge 85 del 2005

amministrativa attraverso un articolata evoluzione giurisprudenziale e normativa. La sua elevazione a principio cardine ha conferito al cittadino uno strumento imprescindibile per la tutela dei propri interessi e per l'esercizio di un controllo democratico sull'operato della pubblica autorità, culminando poi nella sua qualificazione quale livello essenziale delle prestazioni concernenti i diritti civili e sociali, assurgendo così a rango costituzionalmente garantito.

Il diritto di accesso riguarda i documenti amministrativi, così come definiti all'articolo 22 lettera d, ieri tecnici o nulla osta così come modificato dalla legge 15 del 2005, secondo il quale per documento amministrativo si intende "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti relativi ad un determinato procedimento detenuti dalla Pubblica Amministrazione". La norma ha risolto, in modo esplicito e affermativo, la questione se la portata del diritto di accesso si possa estendere anche agli atti interni, ovvero quei documenti endoprocedimentali, che pur non avendo un impatto diretto e immediato sul cittadino costituiscono fasi preparatorie del provvedimento finale, come ad esempio pareri tecnici o nulla osta[10]. Inoltre, la norma ha risolto anche l'ulteriore questione se il diritto di accesso possa riguardare anche gli atti di diritto privato emanati dalla P.A. Secondo la nuova disciplina, che sul punto ha recepito le decisioni della giurisprudenza più recente, ciò che rileva ai fini del diritto di accesso non è la natura pubblica o privata dell'attività posta in essere, ma il fatto che l'attività di diritto privato della pubblica amministrazione sia finalizzata alla tutela del pubblico interesse e sia comunque soggetta al principio di imparzialità.

Il nuovo articolo 22, novellato dalla legge 15/2005, definisce due punti fondamentali. Innanzitutto, alla lettera a), precisa che il diritto di accesso consiste nella possibilità per gli interessati di visionare e ottenere copie dei documenti amministrativi.

[10] Sul punto si vede T.A.R. , Potenza , sez. I , 05/10/2023 , n. 565 secondo cui "Ai sensi dell'art. 22, comma 1, lett. d), l. n. 241 del 1990, il diritto di accesso può essere esercitato anche nei confronti degli atti amministrativi interni e/o endoprocedimentali, anche se provengono da altre Amministrazioni o da soggetti privati, se vengono acquisiti nell'ambito di un procedimento amministrativo; l'ostensione dei documenti amministrativi va riconosciuta a prescindere dall'utilità che il richiedente ne potrà trarre, in quanto il diritto di accesso ai documenti amministrativi risulta finalizzato a soddisfare il mero bisogno di conoscenza non solo dei soggetti interessati, titolari di un diritto soggettivo o di un interesse legittimo, ma anche dei soggetti portatori di interessi diffusi e/o collettivi (art. 4, d.P.R. n. 184 del 2006), e comunque risulta strumentale ad assicurare l'imparzialità e la trasparenza dell'azione amministrativa. (art. 22, comma 2, l. n. 241 del 1990)".

Successivamente, alla lettera b), chiarisce chi sono i soggetti legittimati a esercitare questo diritto, affermando che l'interesse a cui si collega la richiesta di accesso deve essere diretto, concreto, attuale, e deve corrispondere a una situazione giuridicamente protetta e chiaramente collegata al documento che si intende consultare.

Un'altra questione problematica che è stata esplicitamente affrontata dalla legge 15 del 2005 riguarda le associazioni e i comitati che rappresentano interessi diffusi. La legge 15 del 2005 ha espressamente qualificato come potenziali titolari del diritto di accesso anche questi soggetti privati, in quanto portatori di interessi diffusi.

Prima dell'entrata in vigore di questa nuova legge la giurisprudenza si limitava a verificare la sussistenza di un nesso tra l'oggetto della richiesta di accesso e i fini statutari dell'ente, tenendo conto anche di quanto l'associazione fosse rappresentativa. Diversamente, l'accesso non era consentito quando riguardava informazioni estranee agli interessi legali dell'associazione, oppure quando lo scopo statutario dell'ente era un generico interesse a controllare la trasparenza e la legittimità dell'operato amministrativo, circostanza quest'ultima ritenuta di per sé insufficiente per legittimare l'esercizio del diritto di accesso. Questo approccio è stato ribadito dall'articolo 24, come modificato dalla legge 15 del 2005, il quale sostanzialmente afferma l'inammissibilità delle richieste di accesso documentali finalizzate ad un mero e indiscriminato controllo sull'attività delle amministrazioni.

Un altro punto fortemente innovato dalla legge del 2005 concerne i vari livelli di limitazioni al diritto di accesso, disciplinati in maniera più dettagliata ed esaustiva rispetto alla normativa precedente all'articolo 24. Quest'ultimo originariamente già escludeva l'accesso per tutti quei documenti per tutti i documenti coperti dal segreto di Stato ai sensi delle vigenti disposizioni di legge e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge o dal regolamento governativo di attuazione. Con l'avvento della legge 15 del 2005 sono state aggiunte ulteriori materie onere l'esercizio del diritto di accesso è stato precluso. Innanzitutto nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano. Successivamente nei confronti delle attività delle pubbliche amministrazioni dirette all'emanazione di atti normativi, atti

amministrativi generali, di programmazione e pianificazione, poiché anch'esse restano soggette alla loro disciplina particolare. Ulteriormente nei procedimenti selettivi, quando vengono in evidenza documenti contenenti informazioni di natura psico-attitudinale relativi a terzi, come ad esempio le valutazioni psicologiche o attitudinali fatte su un candidato a un concorso. Quando ci sono materie così delicate, le singole amministrazioni, come i Ministeri o altri enti devono creare dei regolamenti interni, che hanno il compito di definire esattamente quali tipi di documenti che sono in loro possesso non possono essere accessibili, proprio per proteggere gli interessi quali la privacy dei canditati. Al di fuori delle ipotesi più specifiche appena esaminate, il nuovo comma 6 dell'articolo 24 elenca una serie di interessi che, se messi a rischio, possono portare all'esclusione del diritto di accesso. In primo luogo possiamo ricordare la sicurezza nazionale, difesa e relazioni internazionali, che rappresentano documenti la cui diffusione potrebbe compromettere la sicurezza dello Stato. A seguire, interessi relativi alla politica monetaria e valutaria, ossia informazioni che, se rivelate, potrebbero destabilizzare l'economia. O ancora relativi a ordine pubblico e lotta alla criminalità, o attinenti alla vita privata, come dati personali (epistolari, sanitari, finanziari) o informazioni sensibili di aziende (la cui divulgazione violerebbe la privacy. Infine, non mancano di essere menzionati interessi relativi alla contrattazione collettiva nazionale di lavoro, quindi atti legati alle trattative sindacali e ai mandati interni di chi le conduce, al fine di tutelare la segretezza del processo negoziale. Sostanzialmente si potrebbe dire che la normativa cerca di bilanciare il diritto del cittadino all'accesso con la necessità di proteggere interessi pubblici e privati superiori, delineando chiaramente i casi in cui il diritto di accesso può essere escluso.

La legge del 2005 è intervenuta modificando anche l'originario articolo 27 della legge 241 portando all'istituzione della "Commissione per l'accesso ai documenti amministrativi", cui sono affidati i compiti di vigilare sulla piena attuazione del principio di conoscibilità degli atti amministrativi, di redigere annualmente una relazione sulla trasparenza dell'attività amministrativa e di proporre al governo eventuali modifiche di leggi o regolamenti per tutelare pienamente il diritto di accesso.

Il ruolo principale della commissione non è tanto quello di perseguire gli interessi pubblici tradizionali, quanto piuttosto garantire l'interesse dei cittadini da una posizione

di indipendenza rispetto al governo e conseguentemente dall'indirizzo politico. Questa autonomia le permette di esercitare una funzione che, nella sostanza, è molto simile a quella giurisdizionale, ovvero una funzione di "giudizio" o di risoluzione delle controversie, agendo come un organo terzo e imparziale. Proprio per tali ragioni viene qualificata dalla più recente dottrina come un'autorità amministrativa indipendente.

Merita di essere menzionata un'altra innovazione importante in materia, prevista dal comma 4 dell'articolo 25, come modificato dalla legge 15 del 2005, il quale ha delineato una specifica mansione del difensore civico nella tematica dell'accesso ai documenti. Quest'ultimo fu sconosciuto al nostro ordinamento fino all'introduzione delle regioni. In particolare, quando l'interessato si vede negare la propria richiesta di accesso ai documenti da parte della pubblica amministrazione ha la possibilità di rivolgersi al difensore civico competente entro 30 giorni per chiedere che la decisione dell'amministrazione venga riesaminata. Se il Difensore Civico ritiene che il rifiuto dell'accesso sia illegittimo, lo comunica alla stessa Amministrazione che aveva negato il documento. Entro questo periodo di trenta giorni l'amministrazione è tenuta a rispondere, confermando il diniego precedente con una motivazione dettagliata, in alternativa ritirando il diniego e concedendo conseguentemente l'accesso ai documenti, o non rispondendo affatto, circostanza quest'ultima in cui si applica il silenzio assenso-legittimante e dunque l'accesso si dovrà considerare automaticamente concesso.

In sostanza, il percorso normativo della trasparenza nel nostro ordinamento, avviato da leggi settoriali negli anni '80 e culminato con la legge 241 del 1990, ha segnato il passaggio da un sistema amministrativo opaco a una basato sulla pubblicità e accesso. Le modifiche successive, in particolare la Legge 15/2005, hanno maggiormente consolidato il diritto di accesso, elevandolo a principio fondamentale e livello essenziale delle prestazioni, pur definendo con maggior esattezza limiti e bilanciamenti con interessi come la riservatezza. L'introduzione di nuove figure come la Commissione per l'accesso e il ruolo rafforzato del difensore civico testimoniano l'impegno a garantire ai cittadini strumenti concreti per un controllo democratico e una partecipazione effettiva all'operato della pubblica amministrazione.

1.2.1 La legge n. 33 del 2013 e l'accesso civico generalizzato

Un'altra disposizione che ha rappresentato un'importante innovazione in tale ambito è il D.Lgs 33/2013 "Riordino della disciplina riguardante gli obblighi di pubblicità trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni", in attuazione della delega contenuta nella legge 190 del 2012, conosciuto anche come "decreto trasparenza"[11]. Tale disposizione segna un punto di svolta dal momento in cui introduce nel nostro ordinamento la nozione di accesso civico. Quest'ultimo istituto, di cruciale importanza, viene disciplinato dall'articolo 5 del relativo decreto, il quale ha istituito nel sistema amministrativo un obbligo di pubblicazione in capo alla pubblica amministrazioni riguardo specifici documenti, dati e informazioni: questo dovere viene assolto mediante la pubblicazione sui siti web istituzionali, essendo attualmente questa la metodologia più rapida per assicurare la trasparenza amministrativa e un capillare controllo da parte dei cittadini. In questo modo, i principi di accessibilità e pubblicità assurgono quasi a diritto costituzionale, poiché concretizzano i valori democratici di uguaglianza, buon andamento, efficacia ed efficienza dell'azione amministrativa.

Inoltre, di fronte a questo obbligo di pubblicazione il legislatore ha previsto un diritto sinallagmatico in capo ai cittadini, in base al quale chiunque può accedere ai siti internet delle amministrazioni in modo diretto, immediato e libero, senza necessità di registrarsi sul sito internet o di presentare una specifica domanda, al fine di consultare questi documenti.

Ai sensi dell'art. 5 del suddetto decreto l'oggetto dell'obbligo di pubblicazione riguarda tutta la documentazione pertinente l'attività e l'organizzazione dell'amministrazione, includendo, a titolo esemplificativo, i nomi dei funzionari preposti ai vari uffici, i dettagli relativi alla formazione e all'aggiornamento del personale amministrativo, nonché tutte le informazioni che descrivono il rapporto e le interazioni tra l'ente e i cittadini. Ma, come esaminato in precedenza, la trasparenza e la pubblicità sono concetti distinti: la trasparenza è da un lato compatibile con la secretazione di atti che devono rimanere

[11] Nel seguito del testo, per semplicità e brevità, il decreto legislativo 14 marzo 2013, n. 33 (Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni) sarà indicato, a seconda del contesto, come "decreto legislativo 33/2013" o "decreto trasparenza".

inaccessibili, e dall'altro lato non può dirsi pienamente raggiunta se la pubblicità non si risolve in comprensibilità delle informazioni da parte dei cittadini.[12] Difatti, il decreto trasparenza impone che queste informazioni debbano essere esaustive, rispettare la privacy dei cittadini, rispettare il segreto d'ufficio, e soprattutto, essere sempre aggiornate.

L'obbiettivo primario di queste innovazioni è quello di promuovere un controllo diffuso sull'operato pubblico ribadendo il principio fondamentale di sovranità popolare attraverso una maggiore partecipazione democratica. Queste innovazioni normative segnano un'evoluzione normativa verso una trasparenza mirata a coinvolgere attivamente i cittadini nelle decisioni amministrative. La trasparenza amministrativa "totale" consente a chiunque di accedere alle informazioni delle amministrazioni pubbliche, sia statali che locali. Ciò implica l'abbandono delle precedenti restrizioni sull'accesso, sulla scia del percorso iniziato con il d.lgs 150/2009, che già introduceva l'obbligo di pubblicare dati sui siti istituzionali.[13]

Diversamente dalla domanda di accesso procedimentale, questa tipologia di accesso non richiede alcune motivazione da parte del richiedente ed è gratuita e la relativa domanda deve essere inviata al Responsabile dell'ufficio Prevenzione della Corruzione e Trasparenza. Quest'ultimo una volta ricevuta l'istanza la registra ufficialmente e provvede a valutarne il contenuto. Entro trenta giorni dalla presentazione della domanda è poi tenuto a prendere una decisione, che deve essere comunicata mediante provvedimento esplicito e motivato, e divulgare online l'informazione o il documento richiesto. Contestualmente alla pubblicazione sul sito ufficiale dell'amministrazione, il dato o l'atto viene inviato direttamente all'interessato, insieme al link per accedere al formato digitale. Nel caso in cui l'amministrazione neghi, anche solo parzialmente l'accesso all'atto, ciascun privato ha la facoltà di presentare domanda di riesame allo stesso Responsabile, il quale sarà tenuto ad emettere un nuovo provvedimento di accoglimento o di rigetto, rigorosamente motivato, entro e non oltre venti giorni. Tuttavia, qualora la richiesta di accesso riguardi altri individui, in particolare i loro dati personali,

[12] SANTISE M., Coordinate ermeneutiche di diritto amministrativo, cit., p. 395

[13] emanato in attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni.

come previsto dall'articolo 5-bis, comma 2, lettera a) il Responsabile dovrà rivolgersi all'Autorità Garante per la protezione dei dati personali per ottenere il parere preventivo di quest'ultima. Il garante a sua volta dovrà esprimersi entro dieci giorni dalla ricezione della richiesta del Responsabile. Inoltre, secondo quanto previsto dal D.lgs 104/2010 (anche noto come Codice del processo amministrativo), il cittadino può, in ultima istanza, proporre ricorso contro la decisione del Garante o contro il provvedimento del Responsabile dinanzi al Tribunale Amministrativo Regionale competente.

Pertanto si potrebbe affermare che notevoli sono le differenze tra l'accesso procedimentale tradizionale e il più recente accesso civico. Innanzitutto l'accesso classico svolge un ruolo difensivo, poiché è finalizzato a tutelerà la posizione giuridica di un cittadino all'interno del procedimento giurisdizionale. Al contrario l'accesso civico semplice mira ad un controllo generalizzato e diffuso da parte di ogni cittadino sull'operato della pubblica amministrazione. Inoltre, mentre l'accesso tradizionale consente di consultare soltanto i documenti amministrativi, la nuova tipologia di accesso civico comprende sia i documenti, sia gli atti sia le informazioni di cui la P.A. è in possesso. Ulteriore differenza risiede nel fatto che la legge 241 del 1990 richiedeva un nesso diretto fra interesse giuridico da tutelare e l'atto a cui si voleva accedere, condizione quest'ultima che non è stata posta per l'esercizio dell'accesso civico semplice. Ulteriormente, come accennato in precedenza, l'istituto dell'accesso civico rimane ad istanza di parte, ma a differenza dell'accesso tradizionale, non necessità di alcuna motivazione, il che implica che nessuna richiesta potrà essere respinta per assenza o inadeguatezza della motivazione. Vi è poi un ulteriore distinzione, anch'essa già accennata in precedenza, relativa al costo dell'accesso. Difatti, l'accesso civico semplice risulta essere gratuito, mentre l'accesso ai sensi della Legge 241/90 risulta a pagamento, con un costo che serve a coprire le spese di riproduzione del documento.

La novità definitiva giunse con l'avvento dell'articolo 7 della Legge 7 agosto 2015, cosiddetta legge Madia, e con l'approvazione del conseguente decreto legislativo 25 maggio 2016 n. 97. Con tale decreto il governo si apprestava a dare attuazione alla previsione della lettera h) dell'art. 7 della Legge Madia che delinea tra i criteri da realizzare «riconoscimento della libertà di informazione attraverso il diritto di accesso, anche per via telematica, di chiunque, indipendentemente dalla titolarità di situazioni

giuridicamente rilevanti, ai dati e ai documenti detenuti dalle pubbliche amministrazioni, salvi i casi di segreto o di divieto di divulgazione previsti dall'ordinamento e nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati, al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche»[14].

Si potrebbe affermare che la libertà di informazione, espressamente menzionata nella norma citata, costituisce un elemento essenziale libertà di espressione, condizione indispensabile per la democraticità dello stato. Da ciò si deduce che gli amministrati devono essere posti nella condizione di acquisire informazione sui meccanismi di gestione del potere, in virtù del fatto che l'informazione costituisce "l'architrave dello Stato democratico".[15]

Il sopracitato d.lgs 97/2016 ha novellato il d.lgs 33 /2013 introducendo una nuova tipologia di accesso, ossia accesso civico generalizzato, destinata ad affiancarsi e non a sostituire le altre due preesistenti. Il legislatore con questa previsione ha tratto ispirazione dal "Freedom of Information Act" (FOIA) statunitense, traducibile letteralmente in "Atto per la libertà di informazione", promulgato il 4 luglio 1966. Questa legge ha influenzato oltre novanta Paesi nel mondo, portandoli ad adottare un sistema di trasparenza pubblica che assicura la conoscibilità di tutti i documenti, atti, informazioni e dati detenuti o comunque in possesso di un'entità pubblica, con la previsione di eccezioni ben definite e limitate nell'ambito di più ampie politiche di open government. Tali politiche ridefiniscono il rapporto tra pubblica amministrazione e cittadino, spostando l'aspetto centrale di questa relazione da un approccio basta sull'erogazione di servizi, dove il cittadino è solo fruitore, ad uno basta sulla leale e reciproca collaborazione, in cui il cittadino viene attivamente coinvolto nelle scelte di governo.

L'accesso civico generalizzato trae origine dal precedente istituto dell'accesso agli atti, previsto dall'articolo 22 della legge 241 del 1990, trasformandone radicalmente requisiti,

[14] La legge delega (legge n. 124 del 2015, cd. Madia) infatti autorizza il Governo ad intervenire adottando «entro sei mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni integrative e correttive del decreto legislativo 14 marzo 2013, n. 33, in materia di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni» (art. 7)

[15] Barra, F. 2024. Il diritto d'accesso civico generalizzato (c.d. FOIA): paradigmi, modelli e percorsi applicativi. *Rivista italiana di informatica e diritto*. 6, 1 (Jun. 2024), 191–216.

legittimazione e limiti. Non è più un semplice strumento per risolvere controversie, ma diventa un vero e proprio strumento di trasparenza. La differenza fondamentale risiede nel fatto che i cittadini non devono in alcun modo specificare le motivazioni poste a fondamento della richiesta. Con l'istituto dell'accesso civico generalizzato si pone dunque in capo alla pubblica amministrazione di pubblicare e rendere accessibili ai cittadini gli atti, i documenti e i dati, inclusi quelli non rientranti nell'obbligo di pubblicazione previsti per l'accesso civico semplice.

Si tratta dunque di un accesso libero che riguarda sia i documenti amministrativi sia i dati amministrativi, che garantisce ai cittadini la facoltà di controllare l'operato della pubblica amministrazione.

Si assiste dunque alla nascita di un istituto che condivide alcune caratteristiche sia con l'accesso procedimentale della legge 241 del 1990, sia con l'accesso civico semplice del Dlgs 33/2013. Questo risultato è stato reso possibile dalle significative innovazioni introdotte dal Trattato di Lisbona del 2009, il quale ha sancito il principio generale di trasparenza e il diritto di accedere liberamente ai documenti in possesso delle autorità pubbliche, senza necessità per il richiedente di dimostrare un interesse specifico o preventivo. In questo modo la collaborazione tra pubblica amministrazioni e cittadini viene ulteriormente rafforzata, i quali vengono resi maggiormente partecipi nelle attività pubbliche e possono sollecitare la PA ad agire in linea con i principi di imparzialità, buona amministrazione e trasparenza.

L'accesso civico generalizzato riconosce un vero e proprio diritto "a titolarità diffusa", dal momento che chiunque è legittimato a richiederlo, senza alcuna limitazione in ordine ai soggetti legittimati e senza la necessità di fornire una specifica motivazione[16].

Come analizzato in precedenza l'accesso civico generalizzato è esercitabile relativamente «ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione»[17]. Secondo le Linee guida dell'Autorità Nazionale Anticorruzione (d'ora in poi ANAC) n. 1309 del 2016 chiarisce che il "dato"

[16] Sul punto si veda anche T.A.R. , Roma , sez. III , 08/04/2022 , n. 4182 e T.A.R. , Napoli , sez. VI , 05/04/2022 , n. 2333
[17] Barra, F. 2024. Il diritto d'accesso civico generalizzato, op. cit.

ricomprende un concetto molto esteso da riferire "al dato conoscitivo come tale, indipendentemente dal supporto fisico sui cui è incorporato e a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione". [18]Di conseguenza, la distinzione tra "documenti" e "dati" implica che l'amministrazione deve considerare valide anche le richieste che specificano solo i dati desiderati, senza necessariamente indicare i documenti precisi in cui essi sono contenuti. Le richieste esplorative, meramente indirizzate a conoscere le informazioni in possesso della PA, non sono comunque ritenute ammissibili. Inoltre, le richieste non devono essere generiche, ma devono consentire di Le richieste inoltre non possono essere generiche, ma devono permettere di identificare il dato, il documento o l'informazione desiderata, indicandone almeno la natura o l'oggetto.[19]

Quando si parla di accesso civico generalizzato e lo si confronta con le altre forma di accesso previste nel nostro ordinamento vi sono alcune differenze. Nel caso di accesso civico generalizzato la richiesta può essere negata se la divulgazione dei dati o dei documenti richiesti potrebbe causare un pregiudizio per determinati interessi pubblici considerati prevalenti.[20]Oltre gli interessi pubblici da tutelare rimangono fermi i casi di esclusione previsti all'articolo 5-bis comma 3 del dlgs 33/2013. [21] Diversamente dall'accesso civico semplice il cui scopo consiste nel rimediare alla mancata pubblicazione da parte della Pubblica Amministrazione dei documenti e degli atti che è obbligata a rendere pubblici, l'accesso civico generalizzato può essere utilizzato esclusivamente per fini conoscitivi o di controllo sull'operato dell'amministrazione.

A differenza dell'accesso procedimentale, la richiesta per l'accesso civico generalizzato non deve per forza riguardare uno specifico documento già indicato dal richiedente, ma come abbiamo analizzato in precedenza, trattandosi di un tipo di accesso più ampio ed esteso, può riguardare anche informazioni e dati e non solo documenti. La relativa

[18] ANAC 2016, p. 4.2
[19] Consiglio di Stato, sez. VI, sentenza, 22 giugno 2020 n. 3891
[20] Questi interessi sono elencati nell'articolo 5-bis, comma 1, del D.Lgs. 33/2013 e includono, ad esempio:La sicurezza pubblica e l'ordine pubblico, la sicurezza nazionale, le relazioni internazionali, la politica e la stabilità finanziaria ed economica dello Stato
[21]Il testo recita così:Il diritto di cui all'articolo 5, comma 2, è escluso nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990.

procedura prevista dal d.lgs 97/2016 stabilisce che la richiesta deve essere presentata alla pubblica amministrazione che detiene l'informazione. Se questa informazione contiene dati personali relativi ad un terzo, chiamato controinteressato, l'istante dovrà avvisare quest'ultimo della propria richiesta, concedendogli dieci giorni di tempo per presentare opposizione motivata, anche per via telematica. Una volta scaduto tale termine la pubblica amministrazione è tenuta a rispondere alla domanda di accesso con provvedimento scritto e motivato. Dopodiché se la pubblica amministrazione decide di accogliere parzialmente la richiesta deve spiegare le motivazioni del diniego parziale, quale esclusione prevista all'articolo 5-bis comma 3 del dlgs 33/2013 opera[22]. Se, invece la PA accoglie la richiesta pienamente deve fornire l'informazione richiesta entro quindici giorni dalla data in cui il controinteressato ha proposto opposizione. Infine, se la PA nega in toto l'accesso o rifiuta di pronunciarsi, si applica le stessa disciplina prevista in materia di accesso civico semplice.

In conclusione l'accesso civico è un istituto che rafforza la democraticità del nostro sistema. Il suo esercizio non è solo un diritto, ma un dovere civico mediante il quale il cittadino contribuisce a creare istituzioni più efficienti e trasparenti promuovendo l'integrità e contrastando comportamenti illeciti e negligenze all'interno della Pubblica Amministrazione.

1.3 Il Principio di Minimizzazione dei Dati: Fondamento per la Tutela della Riservatezza nell'Era Digitale

Trasparenza, pubblicità e accesso hanno ad oggetto documenti, atti, informazioni e dati in possesso delle pubbliche amministrazioni. Da ciò discende l'immediata necessità di bilanciare accuratamente la loro diffusione specialmente quando si tratta di dati di terzi e della loro riservatezza.

La trasparenza, infatti, può incontrare un limite significativo nel necessario bilanciamento con la privacy, in particolare se l'oggetto della richiesta di accesso riguarda dati personali idonei a delineare un profilo del soggetto rivelandone personalità e comportamento, comprimendo così le libertà individuali. Proprio per tali motivi, ai fini di assicurare l'accesso al richiedente ma anche di proteggere il soggetto cui tali dati si riferiscono, si è

[22] ibidem

affermato a livello sovranazionale il principio di minimizzazione dei dati, in base al quale l'accesso a dati altrui deve essere permesso solo per quanto strettamente necessario e per il tempo dovuto.

La presenza sul fronte europeo di disposizioni eterogenee e frammentarie costituiva un ostacolo per la libera circolazione delle informazioni. E fu così che si giunse all'approvazione della Convenzione 108 del 1981, che rappresenta la prima disciplina unitaria in materia. Questa Convenzione ha introdotto regole specifiche a garanzia del trattamento "automatizzato" dei dati, tra cui spiccano l'obbligo di ottenere il consenso degli interessati al trattamento dei propri dati e il divieto di tali dati verso paesi o sistemi che non assicurino una protezione adeguata delle informazioni personali. Pertanto, si potrebbe affermare che la Convenzione è stata posta in essere con l'obiettivo di assicurare un livello minimo di garanzie, stabilendo una serie di principi a cui avrebbero dovuto attenersi i singoli stati membri in modo da assicurare il rispetto del diritto alla privacy degli individui nei confronti di ogni elaborazione automatizzata dei dati concernenti individui identificati o identificabili.[23] Tuttavia, la dottrina maggioritaria non ha mancato di individuare alcune lacune presenti nella Convenzione, essenzialmente date dal fatto che quest'ultima si dedica solo a informazioni oggetto di trattamento automatizzato, mentre ignora i dati trattati con procedure manuali.

All'indomani della Convenzione, le istituzione europee sentirono la necessità di armonizzare le diverse legislazione esistenti sulla privacy nei vari Stati membri, con il duplice scopo di colmare le lacune presistenti e fornire una copertura giuridica in tutti quegli stati dove il diritto alla protezione dei dati personali non era ancora regolamento.

La preoccupazione principale era creare una disciplina unitaria che tutelasse anche gli archivi manuali, al pari di quelli informatici, dato che presentavano gli stessi rischi per la privacy ma erano rimasti esclusi dalla protezione della Convenzione di Strasburgo del 1981.

Fu soltanto nel 1995 che L'Unione Europea emanò la direttiva 95/46/CE, conosciuta come "direttiva madre", in materia di protezione dei dati personali. Tale direttiva fu

[23] Alongi, Pompei, Diritto della privacy e della protezione dei dati personali, Tab edizioni, 2021, p. 31

approvata con lo scopo di armonizzare le legislazioni degli stati membri e di assicurare una tutela equivalente della persona nell'ambito del trattamento dei dati personali. Difatti, la direttiva madre, come il Regolamento GDPR che la sostituisce, mira a bilanciare il rispetto del diritto alla vita privata da un lato, e la libera circolazione dei dati tra i vari stati dall'altro.

Nel frattempo, siamo nel 2002, quando l'Unione Europea introdusse un nuovo strumento normativa di importanza fondamentale per la protezione dei dati personali: una legislazione specifica sul trattamento dei dati personali e la tutela della vita privata in materia nel campo delle comunicazioni elettroniche. Nasceva così la direttiva 2002/58/CE50, nota come "ePrivacy", successivamente modificata dalla direttiva 2009/136/C[24]. Conseguentemente, il legislatore nazionale dovette riconsiderare le norme sulla protezione dei dati. Per recepire la nuova direttiva, fu così emanato il Decreto Legislativo n. 196/2003, meglio conosciuto come il "Codice privacy" (il cui nome ufficiale è Codice in materia di protezione dei dati personali). Con l'introduzione del Codice in materia di protezione dei dati personali, tutta la normativa sulla protezione dei dati, che prima era frammentata in vari interventi integrativi e modificativi della legge 675/1996[25], è stata riunita in un unico testo di legge. Si tratta della prima vera e propria esperienza di codificazione e coordinamento di tutte le normative in materia di protezione dei dati personali. Ma non solo: è stato anche il risultato di un lavoro di armonizzazione e adattamento ai principi sviluppati nel tempo in dottrina, plasmando le norme più significative secondo le interpretazioni consolidate della giurisprudenza e le decisioni del Garante per la protezione dei dati personali. Il dlgs 196/2003, tutt'ora in vigore nel nostro ordinamento, sebbene notevolmente ridimensionato dall'arrivo del GDPR, ha introdotto notevoli novità.

Successivamente, il 27 aprile 2016, si è giunti all'approvazione da parte del Parlamento Europeo e del Consiglio, del Regolamento generale per la protezione dei dati personali n.

[24] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

[25] Decreto legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali

2016/679[26], superando di fatto le precedente direttiva madre. Le istituzioni europee furono spinte dalla duplice esigenza di ridurre le disparità causate dalle diverse modalità applicative della disciplina e superare l' evidente disarmonia tra le varie legislazioni nazionali degli stati membri.

Il Regolamento, come ben si sa, è direttamente applicabile in tutti i paesi dell'Unione. Proprio per questo motivo, sono stati concessi agli stati membri due anni per adattare le proprie leggi nazionali, con la possibilità di inserire norme integrative o anche in deroga rispetto al testo approvato a Bruxelles, purché lo stesso Regolamento lo consentisse. Esso accoglie una nuova impostazione che prendendo le distanze da una visione "proprietaria" del dato, in base al quale non lo si può trattare senza consenso, favorisce una visione di "controllo" dello stesso, garantendo in tal modo la libera circolazione dello stesso e una maggior tutela dei diritti dell'interessato[27].

Tra le principali novità introdotte nel GDPR meritano di essere ricordati alcuni principi, che rappresentando il fondamento su cui poggia l'intera normativa, mirano a garantire che il trattamento dei dati personali avvenga sempre nel rispetto dei diritti e delle libertà degli individui, delineando allo stesso tempo un quadro normativo e più solido e coerente in materia di privacy. E, come già analizzato in precedenza, il diritto di accesso agli atti amministrativi, sebbene sia uno strumento fondamentale per il controllo sull'operato della pubblica amministrazione, necessità un adeguato bilanciamento con la tutela della privacy. Conseguentemente, basandoci sull'assunto che nel diritto di accesso agli atti amministrativi si concretizza un sistema che, pur promuovendo la trasparenza, non sacrifica la riservatezza individuale al fine di garantire una miglior tutela della privacy, sembra doveroso riportare di seguito alcuni principi chiave in materia.

Il principio di limitazione della finalità rappresenta un principio cardine in materia di dati personali, tanto da essere ricompreso nell'articolo 8 della Carta di Nizza. Tale principio prevede che i dati personali siano raccolti per finalità determinate esplicite e legittime e

[26]Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, il Regolamento è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, a partire dal 25 maggio 2018. Lungo questo testo esso verrà indicato anche come "Regolamento" o "GDPR

[27]Alongi, Pompei, Diritto alla privacy e alla protezione dei dati personali, tab edizioni, 2021, p. 41

che siano successivamente trattati in modo non incompatibile con tali finalità.[28] Innanzitutto rappresenta una garanzia di controllo e prevedibilità per per la persona a cui i dati si riferiscono (l'interessato)[29]: solo conoscendo le finalità, che devono essere spiegate in modo sufficientemente preciso, l'interessato può valutare se il trattamento dei suoi dati è lecito e realmente necessario. In secondo luogo, la finalità è strettamente legata con l'identità del titolare del trattamento, ossia di colui che gestisce i dati, e alle responsabilità che ne derivano. Se il titolare del trattamento è colui che stabilisce scopi e mezzi del trattamento dei dati, il responsabile del trattamento, invece, esegue il trattamento per conto del primo, perseguendo le finalità prestabilite. D'altra parte, la valutazione di compatibilità sulle finalità ulteriori rende il principio meno rigido e consente di includere anche la necessità di trattamento e di circolazione dei dati. Ciò avviene, quando le finalità aggiuntive, precedentemente non dichiarate, risultano essere "non incompatibili" con quelle originarie. Ad esempio, occorrerà verificare se esiste un legame logico o una relazione implicita tra le varie finalità, il contesto in cui i dati sono stati raccolti e le ragionevoli aspettative degli interessati riguardo a come verrano usati in futuro. Tale principio è strettamente connesso con quello di minimizzazione dei dati. Questi due principi formano insieme un criterio di necessità e proporzionalità che ha guidato lo sviluppo fondamentale del diritto alla protezione dei dati. Il principio di minimizzazione dei dati prevede che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.[30] In altre parole, una volta definite le finalità, è essenziale che i dati raccolti e trattati non siano eccessivi, superflui e irrilevanti rispetto tali scopi.

Il Regolamento non si limita a ribadire il principio di minimizzazione, ma lo irrobustisce legandolo al concetto di accountability[31]. Questo significa che il titolare del trattamento, ossia colui che tratta i dati deve dimostrare attivamente di aver rispettato questo principio. In altre parole, non basta più dire di aver rispettato la legge, bisogna poterlo provare. Inoltre la minimizzazione dei dati assume un ruolo centrale nella costruzione dei dati by

[28] come previsto dall'art. 5 comma 1 lett. b) GDPR
[29] Licia Califano, La Protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale, Torino, Giappichelli, 2023
[30] Art. 5 comma 1 lett. c) GDPR
[31] Si tratta di un approccio, adottato dal GDPR, basato sull'accountability, ossia l'accezione inglese di responsabilizzazione di titolari e responsabili, ovvero sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento

design e by default. Si tratta di due concetti fondamentali delineati nel GDPR il primo riguarda la protezione dei dati fin dalla progettazione, il secondo la protezione dei dati per impostazione predefinita. Difatti, la minimizzazione dei dati diviene parametro fondamentale sin dalle prime fasi di ideazione di un sistema che gestisce dati personali, al fine di rendere il trattamento il più scrupoloso possibile, utilizzando solo i dati strettamente indispensabili per proteggere la privacy dell'interessato. Parimenti, richiede l'uso di tutte quelle misure, come la pseudonimizzazione, che minimizzando la personalità del dato, rendono i dati meno riconducibili a una persona specifica, riducendo in tal modo drasticamente i rischi per la privacy e la libertà dei soggetti interessati[32].

In sintesi, il principio di minimizzazione dei dati è un pilastro fondamentale, affermatosi in seguito al susseguirsi di una serie di normative europee e nazionali dalla Convenzione 108/1981 al GDPR. Questo principio, strettamente correlato a quello di limitazione delle finalità, richiede che il trattamento dei dati personali sia sempre necessario, proporzionato e limitato a quanto strettamente indispensabile. Nonostante alcune iniziali complessità l'integrazione di questi principi con l'introduzione di strumenti come la *privacy by design* e la *privacy by default* ha rafforzato notevolmente la tutela della riservatezza individuale, bilanciandola efficacemente con le esigenze di trasparenza e libera circolazione dei dati.

1.4 Disciplina del diritto di accesso: quali atti sono accessibili

Il legislatore ha riscritto la definizione di "oggetto dell'accesso" tenendo in considerazione le analisi e i dibattiti scaturiti dal testo normativo iniziale. L'articolo 22, primo comma, lettera *d)* mantiene una definizione precisa, estesa e flessibile del documento amministrativo[33]. Questa flessibilità viene ulteriormente rafforzata dai contributi di dottrina e giurisprudenza. Ora, per documento amministrativo si intende "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale.*"[34]Tuttavia, non è più rilevante se il documento sia stato creato

[32]Licia, Califano, La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale, Torino, Giappichelli, 2023
[33] F. Pubusa, Diritto di accesso e automazione, Torino, Giappichelli, 2006
[34] come sancito all'articolo 22 comma 1 lett d) della l. 241 del 1990

direttamente dall'amministrazione, né rileva la sua appartenenza ad un procedimento specifico o la natura della sua disciplina. Le caratteristiche fondamentali richieste sono che l'amministrazione ne sia in possesso e che il documento riguardi un'attività di interesse pubblico, andando oltre la sola attività amministrativa in senso stretto.

In primo luogo, emerge l'accessibilità degli atti interni, fino a quel momento sempre riservati. Conoscere questi documenti è fondamentale per tutelare efficacemente i diritti dei cittadini, dal momento che costituiscono la fonte principale per ricostruire come si forma una decisione amministrativa. Tuttavia, conoscere gli atti interni consente anche di conoscere l'organizzazione dell'amministrazione dato lo stretto legame tra quest'ultima e l'attività svolta. Difatti, tendenzialmente le decisioni sull'organizzazione hanno un impatto significativo sull'attività e ne sono spesso la causa. L'organizzazione è orientata all'azione e ne rappresenta, in un certo senso, l'inizio; di conseguenza, se l'organizzazione non rispetta i principi di imparzialità e buon andamento, nemmeno l'attività che ne deriva potrà farlo.

É ormai pacificamente riconosciuta l'accessibilità di documenti provenienti da privati, specialmente quando tali documenti vengono impiegati nell'ambito dell'attività amministrativa. In tal caso, in quanto finalizzati al perseguimento di un interesse pubblico devono essere sottoposti alle stesse regole degli atti prodotti direttamente dall'amministrazione. Da ciò ne discende che è impossibile soddisfare le esigenze di accesso senza conoscere il contenuto. Lo stesso vale per i documenti frutto dell'attività di diritto privato dell'amministrazione.[35] Ciò che rende il documento accessibile non è la sua origine, ma il suo legame con l'interesse pubblico nell'ambito dell'attività a cui si riferisce. Pertanto finché l'attività di diritto privato ha come scopo il perseguimento di questo interesse, è senz'altro certa l'accessibilità dei relativi atti. Di conseguenza, possiamo affermare che gli unici atti di diritto privato che possono essere legittimamente sottratti all'accesso sono quelli che non sono destinati al perseguimento di un interesse pubblico.

L'ambito oggettivo di applicazione dell'accesso è piuttosto vasto. Il suo scopo principale consiste nel rendere consultabile ogni documento che ha contribuito alla formazione della

[35] F. Pubusa, Diritto di accesso e automazione, op. cit.

decisione amministrativa, poco importa il contesto in cui sia stato generato o chi l'abbia creato, rilevando solo la sua funzionalizzazione all'interesse pubblico. Questa interpretazione è stata confermata dalla norma di chiusura presente nel terzo comma dell'articolo 22, il quale sancisce tutti i documenti amministrativi sono accessibili, a meno che non rientrino in una delle cause di esclusione elencate nell'articolo 24. Da ciò ne discende che il legislatore ha voluto rendere tassativo l'elenco delle eccezioni descritte in quest'ultima disposizione. Inoltre, lo stesso articolo 22, al quarto comma, chiarisce, risolvendo i dubbi emersi in passato, che l'oggetto dell'accesso può essere solo un documento amministrativo. Questo significa che nessuna notizia o informazione può essere richiesta o ottenuta prima che abbia assunto la forma di documento.

Inoltre, si sottolinea che il diritto di accesso è esercitabile solo nei confronti di documenti amministrativi materialmente esistenti al momento della richiesta e che la pubblica amministrazione effettivamente detenga nella stessa data.[36] Sembra opportuno specificare che spetta al richiedente provare se l'amministrazione detenga effettivamente i documenti per i quali viene chiesto l'accesso. Di conseguenza non è possibile richiedere all'amministrazione notizie o informazioni riguardanti atti che non hanno ancora assunto la veste documentale. Pertanto, non sono accessibili documenti come bozze, appunti, comunicazioni informali o altri atti preparatori relativi alla fase istruttoria o di formazione dei provvedimenti amministrativi, né i supporti tecnici che sono alla base dell'emissione di tali atti. Poiché, come evidenziato più volte dalla giurisprudenza, non è ammissibile una richiesta di accesso che non riguardi documenti specifici, ma che miri invece a ottenere informazioni che richiederebbero un'attività di elaborazione dati da parte dell'Amministrazione. In tal senso depone la previsione dell'articolo 2 comma 2 del d.P.R n. 184/2006 in base al quale "l*a pubblica amministrazione non è tenuta ad elaborare dati in suo possesso al fine di soddisfare le richieste di accesso."*Tuttavia, l'accesso deve ritenersi consentito anche se l'istante non abbia effettiva certezza dell'esistenza del documento oggetto della richiesta. In tal caso è dovere della pubblica amministrazione rilasciare un dichiarazione che attesti l'inesistenza del documento. Ulteriormente è importante sottolineare che una richiesta di accesso è da ritenersi inammissibile se formulata in modo troppo ampio e generico, senza specificare quali atti

[36] secondo quanto previsto all'articolo 2, comma 2, del D.P.R. n. 184/2006 (il "Regolamento sull'accesso ai documenti amministrativi")

o documenti si vogliano consultare. Per esempio, non si potrà richiedere di accedere "tutta la documentazione" relativa a un'intera attività o a un procedimento indefinito, poiché qualora l'amministrazione fosse tenuta a soddisfare una richiesta del genere, sarebbe costretta a svolgere una vasta attività di ricerca, catalogazione e sistemazione di documenti che non rientra tra i doveri previsti dalla legge. Questa impostazione è confermata sia dalla dottrina che dalla giurisprudenza, le quali ribadiscono nella relative pronunce che la domanda di accesso debba avere un oggetto determinato e non possa essere generica.

A questo punto, giova domandarsi se il diritto di accesso riguardi solo i documenti cartacei o si estenda anche ai documenti informatici e alle loro copie. Secondo quanto stabilito dal Codice dell'Ammnistrazione Digitale (d'ora in poi C.A.D.) per "documento informatico" si intende "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*[37]" Pertanto, il documento informatico, differentemente da quello cartaceo, rileva a prescindere dalla materialità o meno del supporto. Per capire se un documento informatico può costituire oggetto di una richiesta di accesso, è utile esaminare nuovamente la definizione di documento amministrativo data dal legislatore[38]. La lettura della norma, come analizzata in precedenza non sembra lasciare spazio a dubbi circa il fatto che nella definizione di documento amministrativo, fornita nel suddetto articolo, debba essere ricompreso anche il documento informatico. Inoltre, si osservi che il Codice dell'Amministrazione Digitale definisce "il duplicato informatico" come "*il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.*"[39]Sul punto la dottrina ha evidenziato che sebbene idealmente il documento informatico sia un'unica entità, può esistere in molteplici "memorizzazioni" su supporti informatici anche diversi e separati. In virtù del fatto che al documento informatico non si possa applicare pienamente il principio di unicità dell'originale, non è possibile distinguere un originale informatico dai suoi duplicati identici, a differenza di quanto avviene con le copie di un documento cartaceo. Il che significa che tali duplicati, potenzialmente illimitati, non sono altro che

[37] come riportato all'art. 1, comma 1, lett. p), D. Lgs, n. 82/2005 (c.d. Codice dell'Amministrazione Digitale)
[38] art. 22, comma 1, lett. d) l. 241 del 1990
[39] art. 1, comma 1, lett. i-quinquies), D. Lgs, n. 82/2005 (c.d. Codice dell'Amministrazione Digitale)

lo stesso documento su supporti differenti. In ragione di ciò si può agevolmente dedurre che anche i duplicati dei documenti informatici possono costituire oggetto di una richiesta di accesso.

La nuova normativa ha modificato la disciplina dei casi di esclusione dell'accesso, previsti all'articolo 24, in particolare introducendo nuove ipotesi di limitazione e definendo con maggiore precisione quelle già esistenti, nonché recependo alcune disposizioni regolamentari a livello legislativo. Il primo comma, lettera *a)*, stabilisce che non possono in alcun modo essere accessibili i documenti coperti da segreto di Stato[40], nonché quelli soggetti ad altri vincoli di segretezza o divieti di divulgazione espressamente previsti dalla legge. Ulteriori ipotesi di esclusione, saranno poi definite da un regolamento governativo, volto a tutelare gli interessi indicati al sesto comma dell'articolo 24, e da regolamenti interni adottati da ciascuna. Originariamente, come in parte analizzato in precedenza, la norma già prevedeva l'esclusione del diritto di accesso per tutti quei documenti coperti dal segreto di Stato, come previsto dalle leggi vigenti, nonché nei casi di segreto o di divieto di divulgazione espressamente stabiliti dalla legge o dal regolamento governativo di attuazione. Con l'introduzione della legge n. 15 del 2005, sono stati ampliati i casi in cui l'accesso è precluso, aggiungendo nuove categorie di atti sottratti alla visione dei cittadini.

Anzitutto, è stato escluso l'accesso nei procedimenti tributari, per i quali continuano ad applicarsi le norme speciali che li regolano. Allo stesso modo, sono escluse dall'accesso le attività delle pubbliche amministrazioni volte all'adozione di atti normativi, atti amministrativi generali, di programmazione o di pianificazione, anch'esse regolate da disposizioni particolari. Un'ulteriore limitazione riguarda i procedimenti selettivi, quando coinvolgono documenti contenenti valutazioni di natura psico-attitudinale su terzi – ad esempio, le schede psicologiche o le prove attitudinali dei candidati a un concorso. In tali casi, per tutelare la riservatezza dei soggetti coinvolti, ogni amministrazione è tenuta a

[40] Si tenga conto di quanto stabilito nella legge n. 801 del 1997, intitolata "Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato". Occorre evidenizare come siano rilevanti al fine di escludere l'accesso non sonlo le ipotesi di cui all'art, 12 della stessa lege, ma anche quelle previste nel resto della normative. Dunque, l'incidenza di questa disciplina sull'accesso risulta ampliata di gran lunga.

redigere propri regolamenti interni, che individuano con precisione quali documenti in loro possesso non sono accessibili.

Al di là di queste ipotesi specifiche, il nuovo comma 6 dell'articolo 24 elenca una serie di interessi da tutelare che, se compromessi, giustificano l'esclusione del diritto di accesso. Tra questi vi sono la sicurezza nazionale, la difesa e le relazioni internazionali, poiché la diffusione di determinati documenti potrebbe mettere a rischio la stabilità dello Stato. Seguono gli interessi legati alla politica monetaria e valutaria, la cui compromissione potrebbe avere ripercussioni economiche. Sono inoltre tutelati l'ordine pubblico e l'attività di contrasto alla criminalità, così come la riservatezza della vita privata: rientrano in quest'area i dati personali – come informazioni sanitarie, finanziarie, epistolari – e quelli sensibili delle imprese, la cui divulgazione violerebbe la privacy. Infine, sono esclusi dall'accesso anche gli atti relativi alla contrattazione collettiva nazionale del lavoro, incluse le trattative sindacali e i mandati interni dei negoziatori, per garantire la riservatezza del processo negoziale.

In conclusione, il legislatore ha ridefinito l'oggetto dell'accesso, ampliando la nozione di documento amministrativo per ricomprendere ogni rappresentazione (grafica, informatica, ecc.) di attività di pubblico interesse detenuta dall'amministrazione, indipendentemente dalla sua origine o specificità procedurale. In questo modo si rendono ostensibili anche gli atti interni e i documenti di origine privata o di diritto privato che abbiano rilevanza pubblica, sottolineando il ruolo che ricoprono nella formazione della volontà amministrativa e nell'organizzazione interna. Tuttavia, il diritto di accesso non è illimitato: è circoscritto ai documenti materialmente esistenti al momento della richiesta, escludendo mere informazioni o richieste generiche che implichino un'elaborazione dati da parte della P.A. La legislazione vigente precisa, inoltre, che nella nozione di documento amministrativo sono pienamente ricompresi anche i documenti informatici e i loro duplicati, ormai considerati equivalenti all'originale cartaceo. In sintesi, l'approccio legislativo mira a garantire la massima accessibilità, prevedendo eccezioni tassative per bilanciare l'esigenza di trasparenza con altri interessi tutelati.

1.5 Soggetti coinvolti nel diritto di accesso agli atti: legittimati, controinteressati e pubbliche amministrazioni nell'era digitale

Il diritto di accesso viene attribuito, secondo quanto stabilito all'articolo 22, comma 1, lettera b), ad ogni privato portatore di un interesse diretto, concreto e attuale, legato ad una posizione giuridicamente tutelata, a sua volta collegata al documento oggetto della richiesta di accesso: l'interesse in questione può essere individuale, ma anche pubblico o diffuso. Si badi bene che la formulazione attuale di questo articolo è più dettagliata rispetto a quella originale, che risulta caratterizzata da una certa vaghezza, generando non pochi problemi interpretativi tra gli esperti di diritto e i giudici. Inizialmente, la legge stabiliva genericamente che il diritto d'accesso era riconosciuto a "chiunque vi avesse interesse per la tutela di situazioni giuridicamente rilevanti." Pertanto, non era chiaro cosa si intendesse esattamente per "tutela" o per "situazione giuridicamente rilevante". L'interpretazione che si è affermata ha chiarito che non era necessario avere per forza un diritto o un interesse tutelato in modo forte, come i diritti soggettivi o gli interessi legittimi, essendo sufficiente che la richiesta di accesso fosse collegata a un interesse che avesse una qualche rilevanza per l'ordinamento giuridico, anche un semplice interesse di fatto. In sostanza, si potrebbe affermare che la normativa vigente ha tentato di rendere più chiari e precisi i requisiti per l'esercizio del diritto di accesso, superando le incertezze esistenti in passato. Un altro aspetto importante da considerare è che, fin dalla sua prima versione, l'articolo 22 non limitava il diritto di accesso ai soli cittadini italiani riconoscendolo in capo a chiunque. Questo significa che anche gli stranieri e gli apolidi hanno il diritto di richiedere l'accesso ai documenti, a nulla rilevando lo status di cittadino in tal proposito. L'unico requisito fondamentale è la titolarità dell'interesse a tutela una situazione giuridicamente riconosciuta, indipendentemente dal fatto che chi la detiene sia un cittadino o meno. Sebbene il riconoscimento del diritto di accesso a chiunque sembrava garantirne una vasta applicazione, in realtà, la sua era controbilanciata e ridimensionata dalla previsione di una serie di condizioni per la sua legittimazione. Queste ultime limitavano sensibilmente il suo raggio d'azione. Successivamente, l'introduzione dell'articolo 2 del Regolamento del 27 giugno 1992 n.352[41], ha complicato

[41] Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

ulteriormente le cose, introducendo una nuova condizione. Specificatamente si stabiliva che l'interesse alla tutela di situazioni giuridicamente rilevanti, per poter legittimare l'accesso, doveva essere personale e concreto. L'elemento della personalità imponeva che la situazione giuridica alla base della richiesta fosse direttamente collegabile alla sfera giuridica del richiedente. Il requisito della concretezza, poi, implicava che il semplice elemento personalistico della situazione non fosse di per sé sufficiente. Difatti, la domanda doveva essere respinta se colui che la presentava non avrebbe potuto ottenere un vantaggio attuale e tangibile dall'accesso al documento. Questa aggiunta da parte del Regolamento ha suscitato non poche critiche da parte di numerosi studiosi del diritto, i quali ne hanno contestato la legittimità. Le principali critiche poggiavano sul fatto che il regolamento governativo avrebbe dovuto limitarsi a disciplinare le modalità di esercizio del diritto di accesso, e non certo introdurre nuovi requisiti, tanto meno restrittivi. In sostanza, sulla base del combinato disposto del vecchio articolo 22, primo comma e dell'articolo 2, primo comma del d.P.R. n. 352 del 1992, capiamo che l'operatività del diritto di accesso risultava molto limitata. Innanzitutto, bisognava avere un interesse personale e concreto a tutelare una situazione che avesse una sua rilevanza giuridica. In secondo luogo, doveva esserci un collegamento chiaro tra questo interesse e i documenti da consultare. Conseguentemente in mancanza di uno di questi due requisiti fondamentali la richiesta di accesso non poteva essere accettata.

A seguito della l. n. 15 del 2005 il nuovo articolo 22 mira a fare chiarezza sul diritto di accesso ai documenti amministrativi, stabilendo che tutti i soggetti privati che hanno un interesse diretto, concreto e attuale – anche di natura pubblica o diffusa – legato a una situazione giuridicamente protetta e collegata al documento richiesto, possono esercitarlo. Se da un lato questa riformulazione scioglie alcuni dubbi, specificando meglio chi sono i titolari del diritto, dall'altro ne genera di nuovi.
Ad esempio, se è vero che l'attuale formulazione prevedendo "tutti i soggetti privati" garantisce un'ampia operatività, non si può ignorare che la precedente dicitura "chiunque" era ancora più inclusiva, dal momento che comprendeva sia i soggetti pubblici che privati. Questo significa che, pur con l'intento di chiarire, la nuova norma potrebbe aver involontariamente ristretto il campo rispetto a prima. In sostanza, la portata dell'accesso è stata limitata, poiché il richiedente deve necessariamente essere un soggetto privato. Per quanto concerne, invece l'accesso ai documenti tra le Pubbliche Amministrazioni, questo

è comunque garantito e disciplinato, anche se non in modo approfondito, dall'articolo 58 del d.P.R n. 445 del 2000[42]. Inoltre, è implicito nello stesso articolo 22 quinto comma, il quale stabilisce che quando un'amministrazione pubblica acquisisce documenti amministrativi, e non si tratta di accertamenti d'ufficio, deve farlo seguendo il principio di leale cooperazione. Tale disposizione sembra aver introdotto una disciplina speciale per l'accesso tra le amministrazioni, caratterizzata dall'assenza di un vero e proprio procedimento di accesso e pertanto basato su una notevole semplificazione. Questa semplificazione deriva dall'instaurarsi di un rapporto particolare tra enti pubblici, improntato per l'appunto sulla leale collaborazione.

Per quanto riguarda gli altri requisiti, il legislatore ha previsto che l'interesse legittimante per l'accesso agli atti, debba essere diretto, concreto e attuale, riducendo ulteriormente la portata del diritto d'accesso. Pertanto, è venuta meno la possibilità di effettuare una richiesta di accesso preventiva, ossia finalizzata a tutelare la propria sfera giuridica da una lesione verosimile e realistica, ma non attuale. Non è stato quindi preso in considerazione il parere di molti esperti giuridici che avevano fortemente criticato questa restrizione, ritenendola eccessiva. Lo stesso intento emerge con chiarezza dal modo in cui viene definita la situazione che sottendente la richiesta. Difatti, non si parla più di situazione giuridicamente rilevante, ma di situazione "giuridicamente tutelata". In questo modo si è sostituito un concetto relativamente ampio con uno più circoscritto. Se prima, infatti, come sostenuto da esperti e tribunali, una situazione "giuridicamente rilevante" non doveva essere per forza un diritto soggettivo o un interesse legittimo, ora solo questi ultimi rientrano tra le situazioni "giuridicamente tutelate", con conseguente limitazione dell'ambito entro cui esercitare il diritto di accesso. La novella, quindi, ha chiarito chi siano i soggetti legittimati, ma ha notevolmente ridotto le possibilità di accoglimento della richiesta. Da ciò ne discende che la valenza dell'istituto è oggi ancora più che prima di carattere generale.

Una novità significativa nel procedimento di accesso viene introdotta con la previsione della figura dei controinteressati, ai sensi dell'articolo 22, primo comma, lettera *c).* Si tratta di coloro che vedrebbero la loro riservatezza potenzialmente danneggiata, qualora la richiesta di accesso venisse accolta. Tali soggetti sono identificabili, o facilmente

[42] Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. L'ultimo aggiornamento dell'atto risale al 24/02/2025

identificabili, attraverso il documento stesso che si chiede di consultare. Questa disposizione rappresenta un importante cambiamento nella disciplina del diritto di accesso, in quanto mette in luce una categoria di persone finora rimasta priva di uno specifico riconoscimento legislativo. Di conseguenza il loro regime giuridico ha suscitato non pochi dubbi o perplessità. La nuova norma ha permesso di chiarire la posizione e il ruolo del controinteressato nel procedimento di accesso, nonché la tutela processuale a cui questi soggetti hanno diritto.

È subito chiara la somiglianza tra la definizione di controinteressato all'accesso e quella degli interventori necessari diversi dal destinatario di un provvedimento, previsti dall'articolo 7, comma primo. Si tratta in entrambi casi di soggetti portatori di interessi specifici che l'amministrazione non può ignorare quando decide relativamente al contenuto di un provvedimento, altrimenti il procedimento di formazione della volontà risulterebbe incompleto o viziato. Per questo motivo, sono considerati interventori necessari, proprio come i destinatari diretti di un provvedimento, e godono delle stesse facoltà e diritti. Il controinteressato, come previsto all'articolo 22, è portatore di un interesse di grandissima rilevanza, ossia il diritto alla riservatezza, tale da limitare o escludere l'esercizio del diritto di accesso. Di fronte a una richiesta di accesso l'amministrazione ha il compito primario di individuare eventuali controinteressati al fine di informarli dell'avvio del procedimento di accesso. È esonerata da questo obbligo solo se identificarli non è un'operazione semplice, in ossequio al principio che impone di non aggravare inutilmente il procedimento. I controinteressati, una volta individuati hanno la facoltà di presentare memorie e documenti, per illustrare le proprie ragioni e difendere i propri interessi, di cui l'amministrazione dovrà tenere conto nell'adozione della decisione. Dunque, si potrebbe affermare che la nuova normativa amplia e rafforza le informazioni su cui poggia la decisione amministrativa in ordine alla richiesta di accesso ai documenti, rendendo la decisione più equilibrata e ponderata. A tutto ciò, logicamente segue il regime di tutela processuale del controinteressato, al quale deve essere notificato necessariamente il ricorso contro il diniego di accesso, o in caso di accoglimento della richiesta, gli deve essere riconosciuta la facoltà di eventualmente impugnare il relativo provvedimento.

É opportuno sottolineare in questa sede che la scelta di menzionare il diritto alla riservatezza fin dal primo articolo della legge sull'accesso non è casuale. Questo

riferimento, insieme all'introduzione della figura del controinteressato, dimostra che la legge riconosce alla riservatezza una dignità speciale rispetto al diritto d'accesso. Proprio per questo motivo la riservatezza viene prima di tutti gli altri limiti all'ostensione, rispetto ai quali si differenzia per delicatezza e complessità di bilanciamento[43].

La nuova normativa ha accolto l'evoluzione normativa e giurisprudenziale del concetto di riservatezza e del suo rapporto con la trasparenza. Tale evoluzione, ha accentuato dubbi soprattutto riguardo a quanto potere discrezionale ha l'amministrazione quando deve bilanciare le esigenze di riservatezza e di accesso. Tuttavia, non si può negare che già la disciplina precedente, unitamente alle disposizioni del testo unico sulla privacy, già offriva una tutela soddisfacente della riservatezza. É vero che la decisione sull'accesso veniva presa senza coinvolgere il titolare della riservatezza, e l'amministrazione aveva una certa discrezionalità, ma i principi che guidavano questo potere consentivano di raggiungere soluzioni che proteggevano entrambi gli interessi in gioco.

Pertanto, l'impostazione originaria della legge 241, confermata poi dalla giurisprudenza era il risultato di un bilanciamento legislativo, dove si prevedeva che interessi generali come la trasparenza e il buon andamento dell'amministrazione non potevano cedere di fronte a un singolo interesse privato.

In sintesi, l'introduzione della figura del controinteressato rappresenta un'innovazione cruciale nella disciplina del diritto di accesso riconoscendo finalmente un ruolo e una tutela processuale a chi rischia di vedere la propria riservatezza compromessa. Questa novità chiarisce una categoria di soggetti finora ambigua e garantisce che l'amministrazione, nel decidere sull'accesso, consideri tutti gli interessi in gioco, rendendo la sua valutazione più **e**quilibrata e informata. Inoltre, la costante evoluzione normativa continua a raffinare il delicato equilibrio tra trasparenza e riservatezza, cercando di rispondere alle complessità emergenti.

L'articolo 23 non è stato modificato dalla nuova normativa, pertanto i destinatari del diritto di accesso restano oltre alle pubbliche amministrazioni, anche le aziende autonome e speciali, gli enti pubblici e i soggetti che gestiscono servizi pubblici. La norma, inoltre, stabilisce in modo esplicito che anche i documenti detenuti dalle Autorità di garanzia e di vigilanza sono accessibili.

[43] F. Pubusa, Diritto di Accesso e automazione op. cit.

Un importante precisazione è stata introdotta all'articolo 22, primo comma, lettera *e)*, il quale stabilisce cosa debba intendersi per «pubblica amministrazione»: il termine comprende non solo gli enti di diritto pubblico, ma anche i soggetti privati che svolgono attività di interesse pubblico, regolata sia dalla normativa nazionale che da quella dell'Unione Europea[44].

Ancora una volta il legislatore ha introdotto una esplicita previsione al fine di chiarire dubbi generati dalla normativa precedente, adottando in tal modo una visione ampia del concetto di pubblica amministrazione in linea con l'evoluzione del tema e con la realtà attuale. È opportuno sottolineare che oggi l'interesse pubblico può essere efficacemente perseguito non solo dalle amministrazioni pubbliche utilizzando strumenti e modalità di tipo privatistico, ma anche da soggetti privati, i quali possono scegliere di operare secondo le regole del diritto privato o di quello pubblico. In ogni caso, nella materia in esame, si applica il principio di funzionalizzazione dell'attività all'interesse pubblico. [45]Pertanto, non assume rilievo né la natura del soggetto agente, né il regime giuridico, pubblico o privato, cui l'attività e i relativi atti fanno riferimento, acquisendo rilevanza esclusivamente la finalità pubblica[46]. Se un'attività è orientata al perseguimento di un interesse pubblico viene automaticamente assoggettata ai principi cardine dell'attività amministrativa, ossia l'imparzialità e la trasparenza. Di conseguenza, i relativi atti non possono essere sottratti al diritto di accesso, salvo che ricorre una delle cause di esclusione previste all'articolo 24, comma 3, della legge 241 del 1990.

Se da un lato potrebbe essere stata chiarito in modo soddisfacente cosa si intende per pubblica amministrazione, non si può dire lo stesso per l'espressione "enti pubblici". L'articolo 23 non risolve i dubbi legati a tale definizione, soprattutto per quanto riguarda la sua ampiezza e la possibilità di includervi anche gli enti locali. Non contribuisce a chiarire tali dubbi la previsione all'articolo 29, primo comma, che nel delinearne l'ambito di applicazione precisa che essa si riferisce ai procedimenti amministrativi svolti dalle amministrazioni statali, dagli enti pubblici nazionali e da tutte le amministrazioni

[44] TAR Sicilia-Palermo, sez. I, 9 novembre 2005, n. 5000, ha escluso l'accessibilità degli atti posti in essere da un commissario ad acta nominato in sede di giudizio di ottemperanza, in quanto non essendo un organo dell'amministrazione i suoi atti non sono riconducibili ad essa

[45] F. Pubusa, op. cit.

[46] Cons. Stato, Ad. Plen., 5 settembre 2005 n. 5 conferma tale indirizzo, ammettendo la trasmissibilità dell'obbligo di ostensione ad una società per azioni nata dalla privatizzazione di un ente pubblico

pubbliche, riaprendo in tal modo i dubbi sorti dall'articolo 23, in quanto ha un significato così ampio da poter includere gli enti locali.
In conclusione, sebbene il legislatore abbia compiuto significativi sforzi per definire l'ambito soggettivo del diritto di accesso e per adottare un concetto di amministrazione più ampio coerente con l'evoluzione normativa e giurisprudenziale, permangono incertezza interpretative soprattutto in relazione alla categoria degli enti pubblici e alla loro effettiva inclusione nel campo di applicazione della disciplina. Sarebbe sicuramente auspicabile un ulteriore intervento chiarificatore da parte del legislatore per garantire una tutela piena e completa del diritto di accesso dei cittadini, assicurando una uniforme applicazione dei principi di trasparenza e imparzialità.

Capitolo II

Il diritto di accesso nell'era digitale: sfide e opportunità

2.1 L'Europa e la transizione digitale

l'Europa aveva posto grande attenzione sulla digitalizzazione, ritenendola di estrema rilevanza per la crescita economica del continente, anche prima della pandemia da Covid-19. Tuttavia, la crisi sanitaria ha evidenziato il ruolo fondamentale rivestito dalle tecnologie nella realtà odierna, poiché in particolare durante il periodo di lockdawn hanno consentito di continuare a svolgere attività quotidiane come la scuola o il lavoro da remoto. Questo ci ha permesso di capire non solo la stringente necessità di sviluppare ulteriormente le tecnologie, ma anche il loro fondamentale apporto per la crescita economica del continente.
In risposta all'eccezionale crisi, l'Unione Europea ha stanziato ingenti finanziamenti per la ripresa economica degli Stati membri attraverso i loro Piani di ripresa e resilienza (PNRR), da attuare entro il 2026. Per accedere a questi fondi, i Paesi europei, inclusa l'Italia, hanno dovuto proporre riforme e investimenti focalizzati su una digitalizzazione in linea con la strategia europea. Tale strategia europea si basa principalmente su quattro pilastri: competenze digitali, infrastrutture digitali, trasformazione digitale delle imprese e digitalizzazione dei servizi pubblici. Conseguentemente, questa politica

europea ha avuto un'influenza diretta sulla governance italiana per l'innovazione della pubblica amministrazione, in quanto l'Italia ha dovuto conformarsi alle raccomandazioni europee. Infatti, il PNRR delinea un percorso ambizioso per la digitalizzazione delle istituzioni pubbliche. Tale piano delinea strategia, riforme e strumenti di digitalizzazione che si inseriscono nel quadro normativo preesistente, sviluppandosi secondo le linee guida stabilite dalla Commissione europea. Senza dubbio possiamo affermare che l'impatto di questi cambiamenti è profondo e influenza in modo significativo la governance italiana dell'innovazione nella pubblica amministrazione[47].

Negli ultimi anni, le istituzioni europee hanno posto la digitalizzazione al centro delle loro priorità, definendo una strategia comune per gli Stati membri, il cui scopo è quello di plasmare il futuro digitale dell'Europa e monitorare i progressi di ogni Paese attraverso l'indice DESI [48](Digital Economy and Society Index). Le direttive della politica digitale europea influenzano direttamente i progetti del Piano nazionale di ripresa e resilienza (PNRR) italiano, per i quali il legislatore nazionale sta intervenendo con provvedimenti urgenti. Da ciò discende che per comprendere le scelte legislative italiane sul digitale, è quindi essenziale conoscere la visione dell'Europa, e del resto la stessa normativa italiana prevede che l'attuazione della digitalizzazione a livello nazionale debba da sempre garantire la "*partecipazione [...] alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea"*[49].
Il Consiglio europeo, composto dai capi di Stato e di governo dell'UE, dal suo presidente e dal presidente della Commissione europea, come ben sappiamo, svolge la funzione di definire le priorità e gli orientamenti politici generali dell'Unione. Tradizionalmente adempie tale funzione mediante le conclusioni adottate all'esito di ogni riunione, ove vengono proposte e valutate le azioni da intraprendere e gli obbiettivi

[47] Macrì Indra, Digitalizzazione. Innovazione e Sicurezza nella p.a., Walter Kluters, 2022
[48] l'indice di digitalizzazione dell'economia e della società (DESI) ha sintetizzato gli indicatori sulla performance digitale dell'Europa ed è stato utilizzato per monitorato i progressi compiuti dai paesi dell'UE, in https://digital-strategy.ec.europa.eu/it/policies/desi

[49] Art. 15 comma 3 dlgs 82 del 2005

da raggiungere. Tali conclusioni possono anche indicare scadenze o suggerire proposte legislative, influenzando così l'agenda politica dell'Unione.
Inoltre Il Consiglio europeo è tenuto ad adottare anche un' "agenda strategica" che individua i settori prioritari a lungo termine e le modalità per raggiungere gli obiettivi fissati.

In ambito economico, il Semestre europeo è un ciclo di procedure finalizzato a coordinare e sorvegliare le politiche economiche e di bilancio degli Stati membri dell'Unione Europea.
In ambito economico, il Semestre europeo è un ciclo di procedure finalizzato a coordinare e sorvegliare le politiche economiche e di bilancio degli Stati membri dell'Unione Europea, che si svolge sotto l'attenta guida della Commissione europea e del Consiglio Europeo[50].
Difatti, ogni stato membro, entro il mese di aprile, è tenuto a presentare il proprio Programma Nazionale di Riforma (PNR), che fa parte del Documento di Economia e Finanza (DEF), dinanzi alla Commissione. Quest'ultima dopo aver attentamente analizzato questi programmi è tenuta a proporre specifiche raccomandazioni per ogni paese, le quali vengono poi a loro volta discusse dal Consiglio d'Europa. Una volta che sono poi approvate nella loro versione finale dal Consiglio Europeo, il Consiglio dell'Unione Europea le adotta ufficialmente nel mese di luglio, pubblicando nella Gazzetta ufficiale dell'Unione Europea. Tali raccomandazioni, formulate dal consiglio dovranno poi essere attuate dagli stati membri. Nelle raccomandazioni, emesse nel corso dell'emergenza sanitaria data dalla pandemia da Covid-19, le istituzioni europee hanno evidenziato l'esigenza di innovare la pubblica amministrazione e di potenziare le politiche digitali, in particolare per quanto concerne le competenze digitali e lo sviluppo di infrastrutture che garantiscano connessioni veloci.
In particolare, la raccomandazione del 2019[51] ha evidenziato che l'Italia abbia un bisogno urgente di migliorare le proprie competenze digitali. In proposito lo stesso Consiglio ha ribadito che aumentare l'efficienza della pubblica amministrazione italiana e la sua

[50]Anzalone, Macri, Siragusa, La nuova contabilità delle amministrazioni pubbliche, Milano, 2015, p. 234
[51] Raccomandazione del Consiglio del 09/07/2019 sul programma nazionale di riforma 2019 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2019 dell'Italia (2019/C 301/12), GUUE C 301/69 del 05/09/2019

capacità di supportare le imprese influenzerebbe positivamente il sistema economico, favorendo investimenti e innovazione.

Sebbene la legge delega del 2015 per la riforma della pubblica amministrazione italiana avesse affrontato questioni cruciali come la complessità delle procedure, la mancanza di trasparenza e la scarsa digitalizzazione, l'Europa ha notato che l'implementazione dei servizi pubblici digitali in settori chiave (come i pagamenti online) è ancora ritardata da una pianificazione incoerente, risorse finanziarie insufficienti e un coordinamento carente. A questo si aggiungono l'età media elevata dei dipendenti pubblici e il loro basso livello di competenze digitali, che contribuiscono ulteriormente a rallentare il processo.

Nelle raccomandazioni del 2020[52], il Consiglio europeo affronta la crisi scatenata dalla pandemia di Covid-19, sottolineando la necessità di agire su diversi fronti. L'obiettivo principale è rafforzare la resilienza dei sistemi sanitari, mitigare le conseguenze socioeconomiche attraverso il supporto a imprese e famiglie, e garantire la sicurezza sul lavoro per far ripartire l'economia. Si ribadisce inoltre che Stati membri e UE devono collaborare per un ritorno alla normalità, puntando a una crescita sostenibile che integri la transizione ecologica e la trasformazione digitale.

L'emergenza ha messo in luce quanto sia fondamentale migliorare l'istruzione (in particolare a distanza) e le competenze digitali. È emersa con forza la centralità delle infrastrutture digitali per l'economia, soprattutto per le piccole e medie imprese italiane. Nonostante un'infrastruttura veloce e affidabile sia vitale per garantire servizi essenziali in settori come sanità, istruzione e amministrazione, l'Europa rileva che l'Italia è ancora in ritardo nella copertura della fibra ottica nelle aree rurali e ne incoraggia l'espansione.

Una grande attenzione è rivolta anche all'efficienza della pubblica amministrazione. Le istituzioni europee ritengono che la sua efficacia sia cruciale per non rallentare l'attuazione delle misure di ripresa economica. I principali problemi evidenziati sono la lunghezza delle procedure (inclusa la giustizia civile), la scarsa digitalizzazione.

[52] Raccomandazione del Consiglio del 20/07/2020 sul programma nazionale di riforma 2020 dell'Italia e che formula un parere del Consiglio sul programma di stabilità 2020 dell'italia (2020/C 282/12) GUUE C 282/74 del 26/08/2020.

Nel febbraio del 2020, appena prima che la pandemia dilagasse, imponendo il fermo o la distanza da numerose attività produttive, la Commissione Europea ha dichiarato la sua transizione politica verso il digitale all'interno del documento "Plasmare il futuro digitale dell'Europa", Questo documenta presenta la politica digitale dell'Unione, riprendendo il programma della Presidente Ursula Von der Layen, dove si stabilisce che "*L'Europa deve guidare la transizione verso un pianeta in salute e un nuovo mondo digitale".*[53]

Il documento in questione descrive gli ambiziosi obbiettivi per i prossimi anni, posti in essere al fine di creare un futuro migliore per tutti. In generale, le tecnologie digitali hanno radicalmente trasformato il nostro modo di lavorare, viaggiare, fare affari e interagire, e in particolare l'enorme quantità di dati generate da queste interazioni, se correttamente utilizzata, può dar vita a nuovi modelli di creazione del valore[54].

In definitiva, nel contesto digitale, se da un lato tecnologie come i sistemi di telecomunicazione, l'intelligenza artificiale e l'informatica quantistica presentano grandi vantaggi, dall'altro non sono prive di rischi e hanno costi significativi. Difatti, i cittadini sono esposti frequentemnete al rischio di perdere il controllo sui propri dati personali e la loro attenzione è costantemente sollecitata da stimoli artificiali. Oltretutto, l'attività informatica dolosa può minacciare il benessere individuale, arrivando a perturbare anche le nostre infrastrutture e la sicurezza. Da qui deriva la necessità di delineare un quadro normativo che sia il più possibile chiaro ed esaustivo.

2.2 Analisi dell'impatto della digitalizzazione sui procedimenti amministrativi

Il rapporto tra pubblica amministrazione italiana e la tecnologia digitale può essere descritto come un lungo e complesso processo, ciò in considerazione di ragioni sia di carattere endogeno sia esogeno[55]. In particolare, per quanto riguarda i primi, l'amministrazione ha mostrato una notevole resistenza al cambiamento e l'assenza di adeguate competenze digitali. Da un punto di vista esterno (fattori esogeni), la frammentarietà e la settorialità degli interventi di politica legislativa hanno determinato

[53] Bruxelles, 19/02/2020 COM(2020) 67 final Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Plasmare il futuro digitale dell'Europa".
[54] Macrì Inda, Digitalizzazione, innvazione e sicurezza nella p.a., op. cit.
[55] E. D'Orlando e G. Orsoni, *La digitalizzazione e l'organizzazione della pubblica amministrazione*, in «Istituzioni del federalismo: rivista di studi giuridici e politici», XLIV, 2, 2023, pp. 279 ss.

l'assenza di un quadro normativo di riferimento uniforme, rendendolo di non agevole attuazione. Facendo un bilancio dell'attuale percorso, ciò che colpisce maggiormente è l'impatto delle nuove tecnologie, il quale non è più un semplice strumento, ma un elemento costitutivo del potere statale, in grado di influenzarne l'organizzazione, le attività e i meccanismi di controllo e di verifica, segnando l'avvento di uno "Stato Digitale"[56]. A fronte di questo scenario, negli ultimi anni, si sono verificati due fenomeni significativi. Innanzitutto, è cresciuta la consapevolezza del ruolo cruciale che la digitalizzazione ricopre per l'innovazione della pubblica amministrazione. Conseguentemente, si sta puntando a investire sulla formazione e sullo sviluppo di competenze digitali adeguate. In questa ottica, il Piano nazionale di ripresa e resilienza (PNRR)[57] ha tra i suoi obiettivi principali l'accelerazione del digitalizzazione della pubblica amministrazione, ponendo un forte accento proprio sul potenziamento del "capitale umano". Questo ha portato il Ministero per la Pubblica Amministrazione a varare un nuovo progetto formativo specifico, mirato a fornire le competenze essenziali per rendere la transizione digitale efficace a ogni livello. Inoltre, la "materia" è divenuta oggetto di una disciplina più organica che consente alla dottrina, grazie anche al supporto delle decisioni dei tribunali, di iniziare a riorganizzare e inquadrare le conseguenze di questa trasformazione sui principi fondamentali del diritto amministrativo. A livello nazionale, la fonte più importante in questo ambito è il Codice dell'Amministrazione Digitale (CAD)[58]: testo unico che raccoglie e sistematizza le regole sull'uso dell'informatica nella pubblica amministrazione nei suoi rapporti con cittadini e imprese. Nel corso degli anni il CAD ha subito diverse modifiche e aggiornamenti principalmente per enfatizzare il suo ruolo di "carta di cittadinanza digitale", per promuovere l'integrazione e la collaborazione tra i vari servizi pubblici digitali, nonché per rafforzare i diritti digitali dei cittadini e valorizzare il patrimonio informativo della pubblica amministrazione.

Di pari passo, anche a livello europeo sta emergendo una visione strategica sulla digitalizzazione comincia a delinearsi un sistema delle fonti più organico, completato

[56] L. torchia, Lo Stato digitale. Una introduzione, Bologna, il Mulino, 2023.
[57] Il Piano nazionale di ripresa e resilienza, o PNRR è il piano approvato nel 2021 dall'Italia per rilanciarne l'economia dopo la pandemia Covid-19, al fine di permettere lo sviluppo sostenibile , tecnologico la digitalizzazione del Paese
[58]. Dlgs.D n. 82/2005 e s.m.i

dall'entrata in vigore del regolamento sull'intelligenza artificiale[59]. Questo regolamento è il risultato di un lungo processo di analisi e consultazione e segue l'adozione di numerosi atti non vincolanti (soft law) volti a stabilire gli obiettivi della nuova regolamentazione, con il triplice intento di controllare l'uso dell'IA, garantire uniformità, stabilendo una normativa chiara e coerente, nonché creare un governo efficace. Tutto ciò produrrà ricadute evidenti sui sistemi nazionali delle fonti e, in particolare, sulle fonti che disciplinano le pubbliche amministrazioni, essendo il diritto amministrativo ormai strettamente legato e influenzato dal diritto europeo[60].

L'impulso per quel percorso di riforme, che ha reso la digitalizzazione della pubblica amministrazione un fattore cruciale per la crescita del paese, affonda le sue radici in un documento chiave del 1979. Si tratta del Rapporto sui principali problemi della amministrazione dello stato, redatto dal ministro della funzione pubblica Massimo Severo Giannini durante il governo Cossiga. Questo documento è universalmente riconosciuto come il punto di svolta del riformismo nell'amministrazione italiana. Il Rapporto Giannini del 1979 metteva in luce lo stato arretrato della pubblica amministrazione italiana rispetto all'innovazione tecnologica. Specificatamente, il testo sottolineava come i sistemi informativi non erano più usati solo per la gestione interna, ma stavano diventando essenziali per le funzioni amministrative rivolte all'esterno, influenzando direttamente l'erogazione dei servizi e l'interazione con cittadini e imprese.

Inoltre, dal suddetto Rapporto emergeva la consapevolezza che l'informatizzazione della pubblica amministrazione fosse un elemento chiave per lo sviluppo della stessa, dato il loro stretto legame. Si era iniziato ad avvertire la necessità di porre in essere una costante attività di controllo dei flussi, delle modalità e dei tempi dell'agire amministrativo[61]. In sostanza, si potrebbe affermare che il Rapporto Giannini abbia posto le basi per una riforma globale che ha interamente ridefinito il funzionamento delle istituzioni pubbliche.In particolare, ha stabilito nuovi criteri per definire le responsabilità, ha distinto chiaramente i ruoli politici da quelli dirigenziali e ha chiarito chi fosse il responsabile di ogni singolo procedimento amministrativo.

[59] Si parla del Regolamento Europeo sull'Intelligenza Artificiale (noto come AI Act), approvato formalmente dal Consiglio dell'Unione Europea nel maggio 2024, il quale sta progressivamente entrando in vigore, introducendo il primo quadro normativo completo al mondo per l'IA.

[60] D'Orlando e Orsoni, *La digitalizzazione,* cit., p. 279 ss

[61] G. MELIS, Storia dell'amministrazione italiana, Bologna, 1996 pag. 503

Sembra ora opportuno proseguire analizzato brevemente le prime tappe della digitalizzazione amministrativa nell'ordinamento giuridico italiano. Tra i primi interventi normativi che meritano di essere menzionati, nell'ambito dell'informatizzazione della pubblica amministrazione troviamo sicuramente la legge sul Procedimento Amministrativo n. 241 del 1990, la quale, come esaustivamente analizzato in precedenza, ha ampliato la definizione di "documento amministrativo"oltre a stabilire principi come l'efficacia, l'economicità e la trasparenza. Difatti, l'articolo 22, comma 1, lettera d), i, non lo ha più limitato alla sola forma grafica, ma ha incluso anche la forma elettromagnetica, cioè digitale. Certamente anche il Il Decreto Legislativo n. 39 del 1993[62] ha ricoperto un ruolo fondamentale nella digitalizzazione della pubblica amministrazione, poiché ha trasformato i principi in azioni concrete. Nello specifico tale decreto ha reso operativi i principi di efficienza e trasparenza attraverso l'introduzione di un sistema informatico in ogni ufficio, creando così una fitta rete di collegamenti tra le amministrazioni. Questo sistema fu istituito al fine di migliorare la produttività e contenere i costi, anche grazie al principio di interconnessione tra i vari sistemi informatici pubblici.

Il d.lgs 39 del 1993 ha segnato un punto di svolta, riconoscendo che il diritto amministrativo doveva allinearsi con gli sviluppi della telematica. Questa evoluzione era spinta anche da una crescente richiesta di trasparenza e di accesso alle informazioni da parte di cittadini e imprese, i quali consideravano i dati pubblici una risorsa fondamentale per la propria efficienza. Lo stesso decreto ha istituito l'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA)[63], ossia un organo consultivo del Presidente del Consiglio dei Ministri, cui è attribuita la funzione di valutare le proposte in materia di informatica pubblica e di redigere un piano triennale per garantire il coordinamento e la gestione dei sistemi informativi automatizzati delle pubbliche amministrazioni.

Tuttavia, il vero cambiamento radicale rispetto al passato si è avuto con l'approvazione della legge 15 marzo n. 59 del 1997[64], la quale ha segnato l'inizio di una riforma profonda, trasformando l'approccio culturale della Pubblica Amministrazione e modernizzando la gestione delle dinamiche documentali. Difatti, l'articolo 15 della stessa legge stabilisce che «*Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con*

[62] Recante Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche
[63] Art. 4 d.lgs 39 del 1993
[64] Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa.

strumenti informatici o telematici, contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge». Grazie a questa legge per la prima volta nell'ordinamento italiano è stato riconosciuto il "principio di equivalenza", il quale stabilisce la stessa validità legale tra documenti digitali e documenti cartacei. Conseguentemente potremmo affermare che la concezione del documento amministrativo è passata da una logica esclusivamente cartacea a una prettamente informatica[65]. Sempre l'articolo 15 della suddetta legge ha demandato l'applicazione del principio di equivalenza a specifici regolamenti da emanare. Successivamente, il d.P.R n. 513 del 1997[66] ha dato attuazione a tale norma, introducendo per la prima volta nel nostro ordinamento il sistema della firma digitale. Questo decreto ha stabilito che la firma digitale avesse la stessa validità legale della firma autografa su carta e ha riconosciuto al documento informatico sottoscritto digitalmente la stessa efficacia probatoria di una scrittura privata, come previsto dall'articolo 2702 del codice civile.

Il cerchio si conclude con il d.P.R. 28 dicembre n. 445 del 2000, noto come Testo unico sulla documentazione amministrativa. Quest'ultimo ha consolidato gli sviluppi precedenti, chiarendo che che la forma scritta di un atto è valida anche se realizzata con strumenti informatici, e che gli atti creati digitalmente sono considerati originali e primari, da cui è possibile ricavare copie e riproduzioni su altri supporti[67].

In sostanza, tale disciplina rappresenta il primo grande passo verso la modernizzazione telematica della pubblica amministrazione, sia rendendo i procedimenti più agili e la ricerca dei documenti più rapida ed efficace, sia segnando l'inizio di un'era di maggiore efficienza e contenimento dei costi.

Inoltre, la digitalizzazione ha significativamente influenzato non solo la natura dell'atto amministrativo, ma anche le procedure che stanno alla base dell'elaborazione dello stesso. Difatti, è ormai opinione consolidata che la digitalizzazione ha avuto dei riflessi sull'aspetto temporale, strutturale e anche sulla stessa nozione del procedimento amministrativo.

---

[65] G. CIACCI, G. BUONOMO, Profili di informatica giuridica, CEDAM, 2018

[66] Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59

[67] Per un commento al DPR 28 dicembre n. 445 del 2000 v. F. PATRONI GRIFFI, Un'introduzione al testo unico sulla documentazione amministrativa: metodologia e procedure, in Comuni d'Italia, 2001,

Prima dell'avvento della legge 241 del 1990 non erano previsti termini per la conclusione del procedimento, anzi l'attesa era considerata quasi un elemento fisiologico. Tuttavia, il fattore temporale nell'agire amministrativo acquisiva rilevanza quasi esclusivamente per scopi statistici o organizzativi. L'entrata in vigore della legge sul procedimento amministrativo ha ribaltato questa visione, imponendo l'obbligo di concludere i procedimenti con un provvedimento ufficiale e introducendo una normativa specifica sui termini di conclusione, successivamente aggiornata dalla legge n. 15/2005.

Pertanto, si potrebbe affermare che il principio di speditezza ha sostituito la tradizionale libertà in merito al tempo dell'agire amministrativo e ha introdotto una regolamentazione specifica che garantisce una gestione più rapida degli interessi.

Tuttavia, dal momento in cui il procedimento è gestito digitalmente tempo e spazio reali vengono sostituiti da tempo e spazio virtuali. Inoltre, una procedura digitalizzata risolve problemi di tempo e distanza poiché si svolge e si sviluppa interamente in rete, garantendo trasparenza e un facile accesso a chiunque sia interessato. A ciò si aggiunga anche che ogni funzionario che si occupa di una fase del procedimento viene maggiormente responsabilizzato, poiché è ora possibile tracciare con esattezza il momento (data e ora) in cui ogni operazione viene completata, prevenendo così ritardi o inattività.

La digitalizzazione del procedimento, come accennato in precedenza, ha avuto anche un notevole impatto sulla struttura e sulla nozione dello stesso.

Storicamente il procedimento amministrativo fu definito da Sandulli come una "sequenza di atti e operazioni" funzionalmente collegate per arrivare all'atto principale, ovvero il provvedimento amministrativo, che produce effetti giuridici sul cittadino[68]. Questa nozione formale mette in luce l'aspetto cronologico, essendo una fattispecie a formazione progressiva, poiché l'effetto giuridico si realizza solo dopo che tutti gli atti della sequenza sono stati compiuti. Questi atti, prodotti da soggetti e in momenti diversi, sono uniti da un comune obiettivo. Il carattere formale della nozione deriva dal fatto che la stessa non specifica i singoli passaggi, ma solo il modo in cui devono susseguirsi. Conseguentemente, sussiste una separazione tra il concetto di procedimento e quello di provvedimento finale, inteso come una realtà sostanziale svincolato dal procedimento che l'ha generato.

[68] A. SANDULLI, Manuale di diritto amministrativo, Napoli, 1989,

Nell'ambito di un contesto digitale le decisioni prese dalle diverse autorità coinvolte nel processo possono essere espresse quasi sempre contemporaneamente. Di conseguenza, muta il rapporto tra gli atti endoprocedimentali: non seguono più una sequenza logica e lineare, ma si sviluppano in modo contestuale. Da ciò discende che le singole decisioni non hanno più un valore isolato, ma contribuiscono insieme alla creazione di un unico documento digitale. Quest'ultimo si forma progressivamente e si sviluppa orizzontalmente, superando la tradizionale struttura verticale del procedimento.

In sostanza, il lungo e complesso percorso della digitalizzazione della pubblica amministrazione italiana, descritto come una vera e propria "lunga marcia", è stato caratterizzato da ostacoli significativi, ma anche da momenti da importanti momenti di svolta cruciale che hanno ridefinito il ruolo dello Stato nell'era moderna. L'analisi appena condotta ha evidenziato come gli ostacoli iniziali non fossero legati solo a fattori interni, quali per esempio la carenza di competenze digitali adeguate, ma anche da scelte legislative e politiche esterne che hanno proceduto per anni, in modo frammentario e settoriale, impedendo la creazione di un quadro normativo organico e di facile applicazione.

Successivamente con l'avvento di un nuovo modello di "Stato digitale", la tecnologia non è più un semplice strumento operativo a disposizione del potere pubblico, ma si è trasformata in un suo elemento intrinseco e ineliminabile. Per stato digitale si intende un'entità in cui l'innovazione tecnologica permea ogni aspetto dell'azione, dell'organizzazione e persino dei meccanismi di controllo e di sindacato sul potere. L'impulso decisivo per questo cambiamento è emerso inizialmente dal sopra citato Rapporto Giannini del 1979, un documento che per primo ha riconosciuto l'arretratezza della PA italiana e ha posto le basi per una riforma che puntava a una maggiore efficienza e trasparenza. In seguito, una serie di interventi normativi hanno scandito le tappe principali del processo di modernizzazione. In primo luogo la legge 241 del 1990 sul procedimento amministrativo che ha aperto la strada alla nozione di documento elettronico, passando poi al Decreto Legislativo 39/1993, che ha trasformato i principi in azioni concrete istituendo una rete informatica tra gli uffici e l'AIPA.

Ad ogni modo, la vera svolta si è avuta con la Legge 59/1997, che ha sancito per la prima volta il principio di equivalenza giuridica tra il documento digitale e quello cartaceo, un'innovazione fondamentale poi attuata dal d.P.R. 513/1997 con l'introduzione della

firma digitale. Questo percorso si è infine consolidato con il Testo Unico sulla documentazione amministrativa (D.P.R. 445/2000), che ha riconosciuto agli atti digitali il ruolo di originali primari, chiudendo così il cerchio.

Parallelamente a questa evoluzione normativa avvenuta a livello nazionale, la prospettiva si è ampliata anche a livello europeo dove una visione strategica della digitalizzazione sta portando alla creazione di un sistema normativo più organico, destinato a completarsi con l'entrata in vigore del Regolamento sull'Intelligenza Artificiale. Tale normativa, spinta dall'intento di garantire uniformità, certezza del diritto e un controllo efficace dell'IA, sarà destinata a produrre significative ricadute sugli ordinamenti nazionali, a conferma di come il diritto amministrativo sia notevolmente influenzato da quello europeo e in costante evoluzione. Infine, l'impatto della digitalizzazione si è esteso oltre la mera gestione documentale, ridefinendo il concetto stesso di procedimento amministrativo. Il passaggio da un'era in cui l'attesa era considerata un dato fisiologico, prima della L. 241/1990, a un'epoca in cui il principio di speditezza è diventato operativo, è stato reso possibile anche dalla tecnologia.

In conclusione possiamo affermare he la digitalizzazione non costituisce un semplice aggiornamento tecnologico, ma una vera e propria rivoluzione culturale, legislativa e strutturale che ha permesso d trasformare la pubblica amministrazione italiana in un'entità più efficiente e trasparente e soprattutto capace di rispondere alle sfide emergenti del XXI secolo.

2.2.1 Il ruolo del Codice dell'Amministrazione digitale nell'agevolare l'accesso telematico

Il Codice dell'Amministrazione Digitale[69] (d'ora in poi CAD) è il principale punto di riferimento normativo che ha guidato il percorso di digitalizzazione che ha attraversato l'ordinamento giuridico nazionale negli ultimi due decenni. Sebbene tale testo costituisca

[69] DECRETO LEGISLATIVO 7 marzo 2005, n. 82

il cuore della normativa primaria in tema di digitalizzazione, la sua forma attuale è il risultato di un lungo processo evolutivo. Difatti, dalla sua introduzione, ha subito quasi quaranta modifiche, a partire dal decreto legislativo 159 del 2006 fino alla recente conversione del cosiddetto "Decreto Semplificazioni"avvenuta con legge dell'11 settembre 2020, n. 120. In particolare hanno avuto un notevole impatto sulla normativa precedente: il d.lgs. 179/2016 e il d.lgs. 217/2017, emanati al fine di armonizzare il Codice dell'Amministrazione Digitale con il regolamento europeo eIDAS, ovvero Regolamento UE 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno[70]. Questo regolamento è diventato vincolante a partire dal 1° luglio 2016, e in quanto tale i suoi effetti giuridici sono direttamente applicabili in tutte le legislazioni nazionali, secondo quanto stabilito all'articolo 288 del trattato sul funzionamento dell'Unione Europea. Conseguentemente, seppur con ritardo rispetto alla data di applicazione del Regolamento, il Governo ha emanato il decreto legislativo n. 179 del 2016, recante "Modifiche ed integrazioni del Codice dell'Amministrazione digitale". Tale decreto ha introdotto significative modifiche alla disciplina del CAD, che vanno anche oltre la necessità di adattamento al dettato normativo comunitario. invero, gli interventi principali ridefiniscono l'ambito oggettivo di applicazione del testo e l'assetto di gestione documentale della pubblica amministrazione.[71]

Pertanto, si potrebbe affermare che lo scopo di questo cruciale riferimento normativo consiste nel modernizzare e allo stesso tempo rendere più efficienti e trasparenti i servizi pubblici attraverso l'innovazione digitale.

In pratica, il CAD mira a spostare l'erogazione dei servizi pubblici verso soluzioni completamente digitali. L'obiettivo è ridurre l'uso della carta, digitalizzare le procedure e le comunicazioni, e mettere a disposizione servizi online facili da usare e sicuri.

[70] R. Arcella e G. Vitrani, Il Codice dell'amministrazione digitale : disciplina e applicazioni, Milano, Giuffrè Francis Lefebvre, 2024.

[71] F. Minazzi, Il codice dell'amministrazione digitale riformato : valore del documento informatico, copie analogiche di documento analogico ed informatico, formazione del documento informatico, rapporti con la Pubblica Amministrazione, comunicazioni e notificazioni, documento informatico sottoscritto con firma elettronica, Milano, Giuffrè, 2017.

Il CAD punta a semplificare e automatizzare le procedure burocratiche. L'uso degli strumenti digitali consente di ridurre i tempi di gestione, contenere gli errori e ottimizzare le attività, rendendo l'intero sistema più efficiente. Inoltre, il codice incoraggia l'uso di tecnologie all'avanguardia per migliorare la qualità dei servizi offerti, con l'obiettivo di creare servizi più moderni, personalizzati ed efficienti, che rispondano meglio alle esigenze di cittadini e imprese. Un esempio concreto è l'adozione di strumenti come la firma digitale e l'identità digitale sicura (SPID), che semplificano i processi di interazione con la pubblica amministrazione. Infine l'ultimo, ma fondamentale obiettivo del CAD consiste nel rendere le informazioni più accessibili, garantendo una maggiore trasparenza sull'operato della PA, facilitando al contempo l'accesso ai servizi per tutti i cittadini, inclusi quelli con esigenze speciali, e imprese.

Il codice dell'amministrazione digitale ha in parte integrato, in parte sostituito abrogandole, una serie di disposizione del d.P.R 445 del 2000, ossia il Testo Unico in materia di documentazione amministrativa, il quale sicuramente incentiva l'utilizzo di strumenti informatici e telematici nell'attività amministrativa. Il d.P.R. n. 445 ha adottato un approccio prudente verso la digitalizzazione della pubblica amministrazione, prevedendo una transizione lenta e progressiva. Al contrario, il Codice dell'Amministrazione Digitale ha accelerato questo processo, stabilendo che il modo di operare dell'amministrazione deve essere tendenzialmente esclusivo e digitale. Occorre, pertanto, analizzare più nel dettagli i due testi per mettere in luce le loro differenze e implicazioni.

Originariamente, l'articolo 6 del Testo Unico consentiva alle amministrazioni di sostituire i documenti cartacei, per i quali era imposta la conservazione, con copie fotografiche o altre riproduzioni che ne garantissero la conformità all'originale. Tale norma, inoltre, specificava che l'obbligo di conservazione e la validità probatoria erano soddisfatti anche mediante supporti ottici. Successivamente, subentrato il CAD, veniva abrogata questa disposizione. Difatti, l'articolo 43 del CAD, che ora regola la riproduzione e la conservazione dei documenti, riconosce la validità giuridica delle riproduzioni su supporto informatico, a condizione che siano conformi all'originale, e i documenti già conservati su supporti informatici conservano la loro validità Inoltre, il terzo comma

consente la conservazione su carta solo per *"esigenze correnti"*[72], mentre per la conservazione permanente si confermano le modalità digitali[73]. In generale l'articolo 42 del CAD invita le pubbliche amministrazioni a valutare la convenienza di digitalizzare i propri documenti cartacei, con l'intento di giungere alla dematerializzazione dei documenti e degli archivi. Pertanto le Pubbliche Amministrazioni sono tenute a considerare il rapporto costi-benefici e, in caso di valutazione positiva, pianificare la sostituzione degli archivi fisici con quelli digitali. Inoltre, l'articolo 23, comma 7, chiarisce che gli obblighi di conservazione ed esibizione dei documenti, imposti dalla legge, sono considerati pienamente rispettati anche se vengono utilizzati strumenti informatici e telematici.

Oltre che per la conservazione, le amministrazioni possono usare le moderne tecnologie anche per scrivere i propri atti. Difatti, l'articolo 7 del Testo Unico stabilisce che gli atti possono essere scritti con qualunque mezzo che ne garantisca la conservazione. In aggiunta a questa disposizione l'articolo 40 del CAD precisa che le amministrazioni dotate di adeguate risorse tecnologiche sono tenute a redigere i loro atti direttamente in formato digitale. Per quanto riguarda le copie in formato cartaceo sono permesse solo se strettamente necessarie e nel rispetto del principio di economicità. Inoltre, alcuni documenti storici o di particolare valore possono essere redatti in originale su carta, se suscettibili di assumere valore di testimonianza storica e archivistica[74], ma ciò deve essere specificato da un apposito regolamento[75]. Per concludere, occorre ricordare che l'articolo 22 del codice, sancisce una sorte di norma di chiusura, in base alla quale per ogni operazione riguardante la produzione, l'immissione, la conservazione, la trasmissione dei dati, documenti o atti, avvenuta mediante strumenti informatici o telematici, devono essere individuati o resi facilmente individuabili sia le amministrazioni interessate che coloro che hanno eseguito l'operazione.
In sostanza, confrontando il Testo Unico sulla documentazione amministrativa (D.P.R. n. 445/2000) e il Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005) emerge

[72] F. Pubusa, Diritto di accesso e automazione, cit., p. 177 ss.
[73] L'art.44 specifica i requisiti cui devono conformarsi i sistemi di automazione: si tratta della capacità di garantire l'identificazione certa del soggetto che ha formato il documento, dell'amministrazione da cui proviene, la sua integrità, nonché la reperibilità, la sua leggibilità, di ogni informazione necessaria per l'identificazione
[74] F. Pubusa, Diritto di accesso e automazione, cit., 177 ss.
[75] secondo quanto previsto ex. Art. 17, primo comma, l. 400 del 1988

chiaramente la diversità di approccio normativo, cui abbiamo poc'anzi accennato. Difatti, Il Codice dell'Amministrazione Digitale ha ridimensionato drasticamente il ruolo del supporto cartaceo, che diventa marginale rispetto alla conservazione, riproduzione e redazione degli atti amministrativi.

Mentre il Testo Unico originariamente attribuiva al documento informatico l'efficacia probatoria di cui all'art. 2712 c.c., che riguarda le riproduzioni meccaniche, stabilendo tra l'altro che se il documento era firmato con firma digitale o firma elettronica avanzata, veniva parimenti riconosciuta l'efficacia di piena prova, ex art. 2702, fino a querela di falso, garantendo così la provenienza da chi l'aveva sottoscritto, invece il Codice dell'Amministrazione Digitale attribuisce l'efficacia di "piena prova", ai sensi dell'articolo 2702 c.c. ai documenti sottoscritti con firma digitale o firma elettronica qualificata, eliminando però il richiamo all'art. 2712 c.c. per il documento informatico in sé.

Oltretutto, per quanto concerne il requisito della forma scritta, mentre il Testo Unico stabiliva che il documento informatico firmato con firma elettronica soddisfacesse tale requisito, lo restringe alla firma elettronica qualificata o alla firma digitale, specificando che deve essere sempre garantita l'identificabilità dell'autore e l'integrità del contenuto.

Tutt'al più entrambe le normative riconoscono la validità del documento informatico, della sua registrazione e trasmissione telematica, salvo che non rispettino le normative vigenti.

Per quanto concerne invece la trasmissione dei documenti informatici essa può avvenire per via telematica, come enunciato all'art. 4, comma 2, del Codice dell'Amministrazione Digitale. Differentemente dal precedente Testo Unico, che si limitava a considerare il documento inviato e pervenuto al destinatario una volta trasmesso al suo indirizzo elettronico, il nuovo Codice risulta più preciso: il documento si intende spedito nel momento in cui il mittente lo invia al proprio gestore e consegnato quando diventa disponibile nella casella di posta elettronica del destinatario[76]. Più in generale, la trasmissione telematica, se consente la consegna del documento, equivale alla notifica a mezzo posta.[77]Infine, il codice, precisa che la trasmissione di un documento a un'amministrazione, con qualsiasi mezzo che ne accerti la fonte, soddisfa il requisito della

[76] come previsto all'articolo 45 comma 2 del CAD
[77] come ribadito all'articolo 48 comma 2 del CAD

forma scritta senza la necessità di inviare il documento originale, secondo quanto previsto all'articolo 45 primo comma. Tutto ciò presuppone l'esistenza di un "domicilio informatico", un concetto implicito, ma fondamentale per le norme in esame. In proposito, il Testo unico stabiliva che per garantire la validità legale di un documento informatico, la sua data e ora di creazione, invio e ricezione fossero opponibili a terzi solo se conformi alle regole tecniche di validazione temporale. In questo contesto, l'articolo 46 del Codice dell'Amministrazione Digitale (CAD) riprende e precisa quanto già previsto dall'articolo 16 del precedente Testo Unico, stabilendo che "*Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite".* Ciò significa che i documenti trasmessi telematicamente tra pubbliche amministrazioni possono contenere esclusivamente le informazioni indispensabili per lo scopo della loro acquisizione al fine di tutelare adeguatamente i dati sensibili e giudiziari.

In conclusione, in seguito all'analisi di questi due testi, si potrebbe affermare che il Codice dell'Amministrazione Digitale (CAD) gioca un ruolo cruciale nell'agevolare l'accesso telematico.

Invero, il CAD, a differenza del precedente Testo Unico, non si limita a consentire l'uso degli strumenti digitali, ma lo rende una prassi obbligatoria e preferenziale per la Pubblica Amministrazione, assumendo un approccio atto accelerare il processo di modernizzazione, semplificare le procedure favorire la trasparenza. Specificatamente, l'introduzione di strumenti come la firma digitale e l'identità digitale (SPID) ha reso l'interazione con la PA più sicura ed efficiente, superando le precedenti complessità burocratiche. Inoltre, la più dettagliata regolamentazione della trasmissione telematica e del domicilio informatico, ha generato un quadro normativo chiaro e completo che stabilisce i tempi e le modalità di invio e ricezione dei documenti, garantendo efficacia legale anche ai documenti trasmessi in formato digitale.

In sintesi, il CAD ha trasformato la digitalizzazione da una possibilità a una necessità, spingendo la PA a evolvere e a offrire servizi accessibili, efficienti e trasparenti a cittadini e imprese, agevolando in maniera decisiva l'accesso telematico.

2.3 Sicurezza e protezione dei dati

2.3.1 I rischi legati alla sicurezza dei dati amministrativi digitali

Al giorno d'oggi l'equilibrio tra trasparenza e privacy costituisce una delle principali sfide per le pubbliche amministrazioni. La digitalizzazione, come è ormai noto, va di pari passo con la crescente disponibilità di dati in possesso delle pubbliche amministrazioni. Di conseguenza, le istituzioni pubbliche sono sempre più spesso tenute a bilanciare il diritto di accesso alle informazioni pubbliche riconosciuto in capo ai cittadini con la necessità di tutelare la privacy individuale. Il GDPR, come ampiamente analizzato in precedenza, offre un quadro normativo uniforme e completo, ma la sua applicazione è talvolta resa complessa a causa delle diverse interpretazioni del dettato normativo, rendendo difficile per le amministrazioni decidere quali dati condividere senza violare i diritti dei singoli. Inoltre, un altro aspetto critico in tale contesto è rappresentato dal sicurezza informatica: infatti assicurare che i dati sensibili siano tutelati da accessi non autorizzati o da eventuali violazioni è essenziale per mantenere la fiducia del pubblico. Senza tralasciare che in tale contesto la formazione del personale e dei cittadini sui loro diritti e responsabilità è essenziale per garantire una comprensione condivisa. In sostanza, trovare un equilibrio tra un uso efficace delle risorse pubbliche e la tutela dei dati personali è di fondamentale importanza nel contesto digitale odierno.

I dispositivi sempre più interconnessi, grazie anche all'espansione dell'Iot, nonché le avanzate tecniche di ingenerai sociale sui quali si basano, creano un ambiente fertile per il proliferare di minacce informatiche. La digitalizzazione, infatti, porta con sé non solo benefici ma anche rischi concreti.

Pensiamo, per esempio agli attacchi ransomware[78] che bloccano l'accesso ai dati, richiedendo un riscatto per sbloccarli, causando ingenti perdite economiche e danni reputazionali.

[78] Il ransomware è un software malevolo che "infetta" dispositivi come PC, tablet, e smartphone, bloccando l'accesso ai loro contenuti (file, foto, video, ecc.).Per riottenerli, viene richiesto un riscatto (da qui il termine "ransom"). La richiesta di pagamento, spesso accompagnata da un ultimatum temporale, appare sullo schermo del dispositivo, minacciando la perdita definitiva dei dati se il versamento non viene effettuato entro un periodo prestabilito.

Inoltre, sempre utilizzando l'ingegneria sociale si possono ingannare i dipendenti di un'organizzazione con l'intento di ottenere credenziali o dati sensibili, molto spesso tramite email di phishing.[79]

Per mitigare questi rischi, è essenziale che le amministrazioni adottino un approccio proattivo, investendo non solo in tecnologie avanzate, ma anche nella formazione del personale e nella creazione di una cultura della sicurezza a tutti i livelli. Per completare la descrizione dei rischi legati all'ingegneria sociale e garantire un effettiva comprensione delle minacce odierne, è opportuno in questa sede fare riferimento anche allo smishing e al vishing. Il primo è una forma di truffa che si avvale di sistemi di messaggistica, ove si invitano i destinatari a compiere azioni (come per esempio cliccare un link) o fornire urgentemente informazioni, con l'intento di appropriarsi di dati per fini illeciti, frequentemente per sottrarre denaro da conti o carte di credito. Si tratta di una minaccia particolarmente pericolosa in quanto i criminali che sfruttano lo smishing sfruttano la paura di un pericolo imminente per spingere le vittime ad agire d'impulso, cogliendoli alla sprovvista.

Similmente, il vishing è una forma di truffa prettamente telefonica, sempre più diffusa, utilizzata al fine di appropriarsi di dati personali, specie di natura bancaria, per poi sottrarre cospicue somme di denaro. Generalmente, in tali truffe e le vittime vengono contattate telefonicamente da criminali che si spacciano per operatori di banche o istituti finanziari e con la scusa di problemi di sicurezza o di presunte "anomalie" li inducono a divulgare dati sensibili, quali per esempio riferimenti del conto corrente o della carta di credito[80]. Questo metodo, seppur apparentemente banale , si rivela spesso efficace, soprattutto nei confronti delle persone più anziane.

Per fronteggiare queste minacce informatiche, un'organizzazione non deve solo prevenire gli attacchi ma anche pregarsi a gestirli Proprio per queste ragione risulta di fondamentale importanza investire nella cosiddetta "cyber resilience", ossia una strategia che mira a mitigare i danni di un attacco e a garantire la continuità operativa. Questa strategia di resilienza affonda le proprie radice su tre aspetti principali: il monitoraggio continuo al fine di individuare tempestivamente eventuali attività sospette, la gestione degli incidenti,

[79] ll phishing è una truffa informatica in certi soggetti, fingendosi un'entità affidabile (come una banca o un'azienda), inviano messaggi fraudolenti, solitamente via email, per indurre le vittime a fornire dati sensibili come password, numeri di carta di credito e altre informazioni personali

[80] Garante per la protezione dei dati personali, "Cybersecurity", disponibile su: https://www.garanteprivacy.it/temi/cybersecurity, 18 agosto 2025.

che consiste nell'aver un chiaro piano di azione in caso di attacco informatico, e infine la pianificazione della continuità operativa per ripristinare rapidamente i servizi e i dati dopo un incidente.

Tutto ciò che abbiamo premesso evidenzia come la sicurezza informatica debba essere prioritaria in qualsiasi organizzazione. Al giorno d'oggi, è diventato di fondamentale importanza adattare le difese a minacce sempre più sofisticate, anche attraverso l'uso di tecnologie innovative come l'intelligenza artificiale, grazie alla quale si possono analizzare ormai enormi quantità di dati in tempo reale per rilevare e prevenire attacchi, identificando rapidamente comportamenti anomali, in modo tale da eliminare o attenuarne le conseguenze in maniera tempestiva. Tuttavia, per contrastare gli attacchi basati sull'ingegneria sociale, è necessaria una costante e capillare formazione del personale, poiché la componente umana costituisce la base dell'attacco medesimo. Difatti, secondo i recenti studi sensibilizzare i dipendenti sui rischi e sulle best practices può ridurre significativamente la probabilità di un attacco, oltre a essere un obbligo normativo[81].

Da ciò discende l'importanza di prevedere misure di sicurezza adeguate fin dalla progettazione di qualsiasi attività di trattamento dati. Questo approccio, noto come "privacy by design", enunciato all'articolo 25 del GDPR , assicura che le misure di protezione siano parte integrante del sistema.

Generalmente, la normativa distingue le misure di sicurezza in due categorie principiali: misure tecniche e misure organizzative. Le prime si distinguono a loro volta in misure fisiche come il controllo degli accessi a server e la protezione degli spazi fisici e misure informatiche come la crittografia, i firewall e i software antivirus. Le secondo, invece, includono le politiche aziendali, la formazione del personale, la definizione di ruoli e responsabilità, e i piani di risposta agli incidenti.

A parte questo breve cenno, torneremo ad approfondire queste misure di sicurezza e la loro applicazione in un'analisi successiva.

In conclusione, la protezione dei dati personali e la sicurezza dei sistemi digitali sono elementi fondamentali per garantire un'amministrazione digitale affidabile. I benefici della digitalizzazione sono ormai noti , ma al contempo i rischi per la sicurezza e la

[81] cfr. art. 32, par. 4, GDPR

privacy devono essere affrontati con serietà attraverso misure adeguate e complete. Difatti, solo in questo modo la pubblica amministrazione può sfruttare appieno i vantaggi del digitale, tutelando al contempo i diritti e la sicurezza dei cittadini. In sostanza, gestire efficacemente queste sfide è fondamentale per mantenere la fiducia dei cittadini e garantire l'accettazione a lungo termine dell'amministrazione digitale.

2.3.2 L'importanza della protezione dei dati nel rispetto del GDPR

Il GDPR rappresenta la più significativa riforma in materia di protezione dei dati personali a livello europeo. Il regolamento è entrato in piena applicazione il 25 maggio 2018, introducendo un quadro normativo armonizzato volto a garantire un elevato livello di tutela dei diritti fondamentali dei cittadini nell'ambito dei trattamenti di dati personali, imponendo a tutti i soggetti coinvolti – comprese le Pubbliche Amministrazioni – obblighi stringenti in materia di sicurezza, trasparenza e correttezza del trattamento[82].
Uno dei principi cardine introdotti dal Regolamento è quello della accountability (responsabilizzazione), che segna un passaggio cruciale rispetto al previgente sistema normativo. Non è più sufficiente, infatti, che i titolari del trattamento rispettino formalmente gli adempimenti previsti dalla legge; essi devono anche essere in grado di dimostrare, in ogni momento, di aver adottato misure organizzative e tecniche idonee a garantire la protezione dei dati personali[83].
Tale principio assume particolare rilievo nelle Pubbliche Amministrazioni, le quali, trattando numerosi dati spesso particolari o giudiziari, sono chiamate ad assicurare livelli di protezione adeguati al rischio e documentare con trasparenza le proprie scelte.
Accanto all'accountability, il GDPR ha introdotto i principi di privacy by design e privacy by default, imponendo che la protezione dei dati sia integrata fin dalla fase di progettazione dei sistemi e dei processi informatici.
Da ciò né deriva che le soluzioni tecnologiche adottate dalle amministrazioni devono essere concepite in modo da minimizzare i dati trattati e limitarne l'accesso

[82] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (GDPR), in G.U.U.E., L 119, 4 maggio 2016
[83] G. Finocchiaro, Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, Zanichelli, 2017.

esclusivamente a quanto strettamente necessario per il perseguimento delle finalità istituzionali.

Un ulteriore aspetto di particolare rilievo è rappresentato dalla valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment o "DPIA"), prevista dall'art. 35 del GDPR. Nei casi in cui un trattamento presenti rischi elevati per i diritti e le libertà degli interessati – ad esempio, nell'uso di sistemi di videosorveglianza su larga scala o di piattaforme digitali che raccolgono dati sensibili – l'amministrazione è tenuta a condurre un'analisi preventiva, individuando i potenziali rischi e definendo le misure tecniche ed organizzative idonee a mitigarli[84].

Non meno importante è l'obbligo di notifica delle violazioni dei dati personali (data breach), che rafforza il principio di trasparenza nei confronti sia delle autorità di controllo, sia degli interessati.

Secondo l'articolo 4, comma 12, del GDPR, la violazione dei dati personali (o data breach) è una violazione della sicurezza che causa, accidentalmente o illegalmente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali. In sostanza, un data breach è un incidente di sicurezza che riguarda dati personali e impedisce al titolare del trattamento di rispettare i principi stabiliti dall'articolo 5 del GDPR.

Come sottolineato nelle linee guida del Gruppo di lavoro ex articolo 29, "mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali". Quando avviene un data breach, i dati personali, che dovrebbero essere protetti, sono consultati, copiati, trasmessi, rubati o utilizzati da persone non autorizzate[85].

In caso di violazione dei dati, i titolari del trattamento devono informare tempestivamente il Garante per la protezione dei dati personali e, qualora la violazione possa comportare

[84] Garante per la Protezione dei Dati Personali, Linee guida sulla valutazione d'impatto relativa alla protezione dei dati (DPIA), 2018. In particolare, di recente nella Relazione annuale 2024 il Garante ha espresso pareri favorevoli diversi schemi di decreto del Ministero del Lavoro e delle Politiche Sociali, tutti attinenti al trattamento di dati personali. In particolare, con riferimento al SIISL e all'uso di strumenti di Intelligenza Artificiale, la Relazione richiama: "[…] *il trattamento dei soli dati personali necessari al raggiungimento della specifica finalità, la messa a disposizione dei dati di contatto solo previa autorizzazione degli interessati, e l'introduzione di misure specifiche per i trattamenti effettuati mediante IA, tra cui: verifica della qualità dei modelli di calcolo, e obbligo per titolare di misure tecniche organizzative adeguate.*

[85] G. Coraggio, Privacy e Data Protection, IPSOA, 2022

un rischio elevato per i diritti e le libertà degli individui, anche i cittadini direttamente coinvolti[86].

In ogni caso, una volta riscontrata un violazione il titolare del trattamento deve intervenire per arginarne o quantomeno attenuarne gli effetti, valutando i probabili rischi e le misure necessarie per ridurli. n particolare, il rischio si considera presente presente quando il data breach può causare un danno fisico, materiale o immateriale agli interessati, come il furto d'identità, la discriminazione, il danno alla reputazione o perdite economiche ingenti e non. In sostanza, una corretta valutazione del rischio, condotta in modo oggettivo, deve tenere in considerazione sia le probabilità che la gravità delle possibili conseguenze della violazione.

Tale meccanismo ha la finalità di garantire non solo la tempestività degli interventi correttivi, ma anche la consapevolezza dei cittadini rispetto a eventuali minacce per la loro sfera privata.

Il rispetto del GDPR, dunque, non costituisce un mero adempimento burocratico, bensì un elemento essenziale per la costruzione di un rapporto di fiducia tra cittadini e istituzioni. Nell'era della digitalizzazione amministrativa, infatti, l'accesso digitale ai dati pubblici può realizzarsi pienamente solo se accompagnato da un solido sistema di tutele a garanzia della riservatezza, della sicurezza e dell'integrità dei dati personali. In questo senso, la normativa europea si configura come uno strumento di bilanciamento tra esigenze di trasparenza e di protezione, contribuendo a delineare un modello di amministrazione digitale capace di coniugare efficienza, accessibilità e tutela dei diritti fondamentali.

2.3.3 La vlutazione d'impatto sulla protezione dei dati

Come già analizzato in precedenza, una delle novità più significative apportate dl GDPR è stata l'introduzione del principio di accountability, in forza del quale il titolare del trattamento deve dimostrare di aver effettuato tutto il necessario affinché il trattamento avvenisse nel rispetto dello normativa vigente. Per raggiungere tale scopo il titolare del trattamento può avvalersi di un istituto che costituisce l'architrave dell'impianto

[86] G. Sartor, Data breach e obblighi di notifica: il nuovo sistema di responsabilità, in Il diritto dell'informazione e dell'informatica, 2019, pp. 201-220.

normativo in materia di privacy: la valutazione d'impatto dei dati personali (cosidetta DPIA, ossia Data protection Impact Assesment), previsto all'articolo 35 del GDPR.
La valutazione d'impatto sulla protezione dei dati (DPIA) è necessaria quando, dopo un'attenta analisi, il titolare del trattamento identifica che l'attività prevista comporta un rischio elevato per i diritti e le libertà degli interessati.

Come specificato nelle Linee Guida dell'ex Gruppo di Lavoro Articolo 29 (ora EDPB), la valutazione del "rischio elevato" spetta al titolare del trattamento. Per farlo, deve considerare la tipologia dei dati, oltre alla natura e alla portata complessiva del trattamento.

Qualora non fosse possibile determinare a priori la probabilità o la gravità del rischio e quali trattamenti presentino un rischio elevato per i diritti degli interessati, il GDPR indica alcuni casi in cui risulta obbligatoria la DPIA. In particolare quest'ultima risulta obbligatoria in tre casi specifici, ossia per trattamenti che prevedono una profilazione sistematica degli individui e che hanno effetti legali o significativi su di essi, per trattamenti su vasta scala di categorie particolari di dati (ad esempio, genetici o biometrici) o di dati relativi a condanne penali, e infine per la sorveglianza sistematica su larga scala di un'area accessibile al pubblico. Tuttavia, la lista fornita dal GDPR non può considerarsi esaustiva. Difatti, l'EDPB (Comitato europeo per la protezione dei dati), il cui scopo è quello di assicurare coerenza alle posizioni dei singoli stati membri, ha indicato dei criteri comuni affinché le autorità nazionali di controllo possano pubblicare elenchi specifici di trattamenti per i quali è richiesta la DPIA. In Italia, per esempio, il Garante della Privacy ha fornito una propria lista, in linea con gli altri garanti europei, di casi in cui la valutazione è ritenuta frequentemente necessaria. Per esempio il Garante della privacy ha recentemente stabilito che si rende necessario effettuare tale valutazione anche in caso di trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici avanzati dai quali deriva la possibilità di effettuare un controllo a distanza a distanza dell'attività dei dipendenti. I motivi principali risiedono nel potenziale impatto che il controllo a distanza può comportare sui diritti e le libertà fondamentali dei lavoratori, che sono considerati un gruppo "vulnerabile" ai fini della protezione dei dati, nonché la natura dei dati raccolti che possono riguardare aspetti molto personali

dell'attività lavorativa (tempi di inattività, le interazioni, le abitudini e, potenzialmente, i movimenti), comportano un'invasione significativa della sfera privata dell'individuo.

La decisione finale spetta comunque al titolare del trattamento, che deve considerare la natura, l'ambito e la finalità del trattamento per determinare se il rischio è elevato o meno, effettuando una valutazione caso per caso, pur sempre avvalendosi di una serie di indicatori di rischio rigorosamente individuati priori. Occorre inoltre specificare, come specificato nel GDPR, che in caso di dubbio circa la svolgimento della DPIA, si ritene che quest'ultima debba sicuramente essere effettuata in quanto strumento di ausilio per i titolari del trattamento utilizzato al fine di garantire il rispetto della normativa in materia di protezione dei dati.

Una volta stabilita la necessità di svolgere DPIA, la valutazione deve essere effettuata prima di dare avvio alla procedura per il trattamento dei dati. In tale contesto, le procedure interne poste in essere dal titolare del trattamento ricoprono un ruolo cruciale, in quanto definiscono chiaramente sia le funzioni aziendali incaricate di svolgere la DPIA, sia i contenuti specifici che la valutazione deve includere.

In definitiva, la DPIA si configura come uno strumento indispensabile che concretizza l'approccio di accountability richiesto dal GDPR. Non è un mero adempimento formale, ma un processo di analisi e gestione del rischio che spinge il titolare del trattamento a riflettere in modo proattivo sull'impatto delle proprie scelte. Attraverso la DPIA, le organizzazioni sono chiamate a identificare, valutare e mitigare i potenziali rischi per i diritti e le libertà degli interessati, garantendo così che la protezione dei dati sia integrata fin dalle prime fasi di progettazione e che il trattamento avvenga sempre in modo conforme e sicuro.

2.3.4 Strumenti e misure di sicurezza per la protezione dei dati

Tra i principi fondamentali enunciati nel GDPR si annovera la necessità di garantire la sicurezza dei dati personali. Difatti, l'articolo 5 comma 1, lettera *f)* prevede il principio di riservatezza e integrità applicabile al trattamento dei dati, stabilendo che "*i dati devono essere trattati n maniera da garantire un'adeguata sicurezza dei dati personali, compresa*

la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali". Tale obbligo, prima dell'introduzione del GDPR, era già previsto dal Codice della Privacy prima delle modifiche apportate dal D.Lgs. n. 101/2018. Tuttavia, le misure di sicurezza venivano definite in modo generico nell'Allegato B del suddetto Codice, e si limitavano a una serie di indicazioni minime. Sebbene tali misure potevano essere considerate sufficienti per trattamenti di dati semplici, si rivelavano spesso insufficienti spesso inadeguate per proteggere sistemi più complessi e invasivi, come quelli basati sull'intelligenza artificiale[87]. In tali contesti, le vecchie normative non garantivano un livello di protezione sufficiente, evidenziando la necessità di un approccio più solido come quello introdotto dal GDPR. Proprio per colmare tale mancanza il legislatore comunitario ha introdotto l'obbligo per i titolari e i responsabili del trattamento di adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato.

In sostanza, per garantire la sicurezza dei dati amministrativi digitali, non è sufficiente adottare soluzioni tecnologiche isolate, ma occorre un approccio multilivello, capace di integrare misure tecniche, organizzative e giuridiche. Tale impostazione è coerente con il principio di "adeguatezza" previsto dal GDPR, secondo il quale le misure di protezione devono essere proporzionate ai rischi derivanti dal trattamento dei dati personali[88].

Le misure tecniche, come anticipato in precedenza, sono l'insieme di strumenti, principalmente informatici, usati per proteggere l'hardware e il software di un'organizzazione (come le reti, i dispositivi e le applicazioni aziendali). Generalmente, la loro implementazione è affidata a specialisti come il CISO (Chief Information Security Officer) o altri esperti informatici. Da ciò si può agevolmente dedurre che il coinvolgimento di un esperto in privacy e compliance è cruciale per assicurarsi che le soluzioni tecniche non siano solo sicure, ma anche pienamente conformi alle normative sulla protezione dei dati.

L'articolo 32 del GDPR offre una lista non esaustiva di alcune possibili misure tecniche per dare un'idea delle possibili soluzioni previste per garantire un'adeguata protezione dei dati.

[87] G. Coraggio, Privacy e Data Protection, IPSOA, 2022

[88] Regolamento (UE) 2016/679 (GDPR), art. 32, relativo alla sicurezza del trattamento

Un primo strumento fondamentale è rappresentato dalle tecniche di crittografia e anonimizzazione, che consentono di proteggere le informazioni sia durante la fase di trasmissione che in quella di conservazione. La crittografia, infatti, garantisce la riservatezza dei dati, rendendoli illeggibili a soggetti non autorizzati, mentre l'anonimizzazione e la pseudonimizzazione riducono i rischi di identificazione indebita degli interessati, specie nei casi di trattamenti su larga scala[89].

Altrettanto rilevante è l'adozione di efficaci controlli di accesso, che si concretizzano nell'utilizzo di sistemi di autenticazione forte (ad esempio tramite SPID o CIE) e nella gestione differenziata dei privilegi in base al ruolo ricoperto dagli utenti. Siffatto approccio consente di limitare l'accesso ai soli soggetti autorizzati, riducendo la possibilità di violazioni derivanti da abusi interni o da attacchi esterni[90].

In tale contesto, sembra opportuno evidenziare che il legislatore nazionale si è adoperato per identificare misure tecniche specifiche idonee al trattamento di determinate categorie di dati[91], indicate come misure di garanzia, secondo quanto previsto all'articolo 2-septies del Codice della Privacy.

Inoltre, come anticipato sopra, la tutela dei dati, tuttavia, non può prescindere dalla formazione del personale. Molte violazioni, infatti, derivano non da attacchi sofisticati, ma da errori umani, scarsa consapevolezza o comportamenti negligenti. Da ciò si può agevolmente dedurre che investire nella cultura della sicurezza, attraverso corsi di aggiornamento e linee guida operative, significa rafforzare la resilienza complessiva dell'amministrazione[92].

Un ulteriore pilastro della sicurezza è costituito dai piani di continuità operativa e di disaster recovery, strumenti indispensabili per garantire la resilienza dei sistemi informativi pubblici.

Tali procedure assicurano che, in caso di incidenti o attacchi informatici, l'operatività possa essere ripristinata tempestivamente, riducendo al minimo l'interruzione dei servizi ai cittadini[93].

---

[89] F. Pizzetti, Privacy e il diritto europeo alla protezione dei dati personali, Torino, Giappichelli, 2019

[90] Garante per la Protezione dei Dati Personali, Linee guida su autenticazione forte e gestione degli accessi, 2021.

[91] in linea con quanto stabilito all'articolo 9 comma 4 del GDPR

[92] M. Bassini, Il fattore umano nella protezione dei dati personali: tra formazione e responsabilità, in Federalismi.it, n. 5, 2020.

[93] Agenzia per l'Italia Digitale (AgID), Linee guida sulla continuità operativa nella Pubblica Amministrazione, 2020.

Infine, riveste un ruolo strategico l'attività di audit periodici e di monitoraggio costante dei sistemi informativi. Attraverso controlli regolari è possibile individuare vulnerabilità, valutare l'efficacia delle misure adottate e predisporre correttivi prima che si verifichino eventi dannosi. In quest'ottica, la collaborazione con organismi nazionali ed europei di cybersicurezza, come l'Agenzia per la Cybersicurezza Nazionale (ACN) o l'ENISA, rappresenta un supporto fondamentale per la Pubblica Amministrazione[94].

Alla luce di tali considerazioni, emerge chiaramente come la digitalizzazione della Pubblica Amministrazione, pur offrendo enormi opportunità in termini di efficienza, accessibilità e trasparenza, porti con sé la responsabilità di garantire la protezione dei dati trattati. Il diritto di accesso non può, dunque, essere concepito come un valore assoluto, ma deve armonizzarsi con il diritto fondamentale alla protezione dei dati personali, così come sancito dal GDPR e riconosciuto dalla Carta dei diritti fondamentali dell'Unione Europea.

La sfida attuale consiste, quindi, non solo nel garantire l'apertura e la fruibilità delle informazioni pubbliche, ma anche nel preservarne la sicurezza, l'integrità e la riservatezza. Solo attraverso tale equilibrio sarà possibile costruire un modello di amministrazione digitale realmente affidabile, capace di coniugare trasparenza, innovazione tecnologica e tutela effettiva dei diritti dei cittadini[95].

2.4 Trasparenza e open data

2.4.1. Il ruolo degli open data nel promuovere la trasparenza amministrativa

Il riuso delle informazioni pubbliche, cui abbiamo già accennato nel corso della trattazione, si riferisce all'obbligo, da parte delle pubbliche amministrazioni, di rendere i dati in loro possesso accessibili e riutilizzabili da chiunque, cercando al contempo di dare impulso all'economia dei dati e permettendo così ai cittadini di crearne un nuovo valore. In tale contesto, il ruolo delle pubbliche amministrazioni risulta di cruciale importanza

[94] Agenzia per la Cybersicurezza Nazionale, Rapporto sulla sicurezza cibernetica in Italia, Roma, 2023; ENISA, Cybersecurity Threat Landscape 2023

[95] R. Dagostino, La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà, in P.A. Persona e Amministrazione, vol. 14, n. 1, 2024

per due ordini di ragioni: deve rendere i documenti disponibili sui propri siti istituzionali o su richiesta, e deve stabilire le condizioni di riuso tramite l'apposizione di apposite licenze. Tali licenze possono introdurre restrizioni, ad esempio limitando l'uso per fini commerciali, e rendono evidente come i dati riutilizzabili possano essere molto eterogenei tra loro. Tuttavia, se la pubblica amministrazione non pone limiti all'utilizzo del dato pubblico, allora tale dato può essere definito "aperto", o secondo la nota locuzione inglese, "open data"[96].

Nell'ambito della digitalizzazione della pubblica amministrazione, non esiste una norma costituzionale che disciplini espressamente gli open data. Nonostante l'assenza di una norma esplicita, la dottrina maggioritaria ha individuato un possibile fondamento costituzionale nell'articolo 33 comma 1 della costituzione nella parte in cui stabilisce che "*l'arte e la scienza sono libere e libero ne è l'insegnamento".* Secondo questa interpretazione, il diritto di accesso ai dati — e quindi anche agli Open Data — sarebbe una diretta conseguenza del diritto alla libertà di scienza. L'accesso libero ai dati e alle informazioni assurge a requisito fondamentale per la conoscenza, la valutazione e l'innovazione. Pertanto, nel permettere l'accesso ai dati, la pubblica amministrazione promuove l'accesso alla conoscenza, e i dati aperti rappresentano la piena attuazione di questo principio costituzionale.

Per quanto concerna la definizione giuridica, gli open data sono chiaramente disciplinati sia nel diritto europeo che nelle normative nazionali. A livello europeo, la direttiva di riferimento è la (UE) 2019/1024 del Parlamento europeo e del Consiglio, che si intitola "relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico." Nonostante emerga lo stretto legame tra il concetto di dato aperto e di riutilizzo delle informazioni, la direttiva non fornisce una definizione esplicita di "dato aperto", pur dedicando l'articolo 2 alla definizione, ma chiarisce due concetti fondamentali.

Innanzitutto, chiarisce che per "formato aperto" bisogna intendere "*un formato di file indipendente dalla piattaforma e messo a disposizione del pubblico senza restrizioni che impediscano il riutilizzo dei documenti"*[97]. Inoltre, chiarisce che per "standard formale aperto" bisogna intendere *"uno standard che è stato definito in forma scritta, precisando*

[96] S. Rossa, Contributo allo studio delle funzioni amministrative, Cedam, novembre 2021, p, 176 ss
[97] Art. 2 n 14) Direttiva (UE) 2019/1024

in dettaglio i requisiti per assicurare l'interoperabilità del software.[98]*"* Queste due definizioni pur non fornendo una definizione diretta di dato aperto, risultano di estrema rilevanza se lette in combinato disposto con le altre disposizioni della direttiva, le quali a loro volta stabiliscono che il concetto di apertura dei dati si riferisce a dati informati aperti che possono essere liberamente utilizzati e riutilizzati da chiunque vi abbia interesse e per qualsiasi finalità. Combinando le norme europee, si può definire il dato aperto come dato in formato informatico standard, indipendente dalla piattaforma e interoperabile. Inoltre, l'Unione Europea introducendo il principio di "open by design and by default", ha sottolineato l'importanza di creare i dati già in un formato aperto, fin dalla loro origine. L'obiettivo ultimo è quello di andare oltre la semplice pubblicazione di documenti preesistenti e generare dati che possiedano sin da subito tutte le proprietà tecniche necessarie per essere pienamente riutilizzabili.

Nell'ordinamento nazionale, invece, è possibile rinvenire una definizione giuridica nel codice dell'amministrazione digitale, secondo il quale si devono considerare dati aperti "*i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione (...), oppure sono resi disponibili a costi marginali per la loro divulgazione (...)"*[99]. Tale norma mette in luce tre elementi chiave e interconnessi del concetto di open data: un principio di apertura che prevede che i dati siano liberamente accessibili a chiunque e per qualsiasi scopo, un'attuazione tecnica che richiede che i dati siano in un formato aperto, leggibile da ogni computer, e delle modalità di accesso che impongono alle amministrazioni di renderli disponibili tramite strumenti digitali e in modo tendenzialmente gratuito.

[98] Art. 2 n 15) Direttiva (UE) 2019/1024
[99] Art. 1 comma 1, lett l-ter del CAD

Senza dubbio dall'analisi comparata delle definizioni europee e nazionale emerge una forte coerenza. Difatti, la ratio alla base delle due normative è identica, in quanto entrambe mirano a permettere il libero utilizzo e riutilizzo dei dati aperti, e richiedono le medesime caratteristiche tecniche[100].

A tal punto è opportuno passare brevemente in rassegna la disciplina normativa degli open data, la quale deve necessariamente essere integrata con alcune disposizioni del Codice dell'Amministrazione Digitale appositamente dedicate ai dati aperti, in particolare con riferimento al Capo V intitolato "Dati delle pubbliche amministrazioni, identità digitali, istanze e servizi online"[101].

L'articolo 50 del CAD si basa su un assunto fondamentale, ossia che ogni ogni azione della pubblica amministrazione genera dati. Conseguentemente, sulle amministrazioni ricade il compito di creare, raccogliere, conservare e rendere disponibili tali dati attraverso strumenti digitali e le tecnologie dell'informazione e della comunicazione (ICT)[102]. Tutto ciò al fine di permettere ad altri soggetti, in particolare cittadini e imprese, di accedere e riutilizzare queste informazioni. Tali aspetti regolati dal decreto legislativo n. 36 del 2006 e dal decreto legislativo n. 102 del 2015[103], e devono sempre rispettare la normativa sulla protezione dei dati personali. Questo concetto è rafforzato dal principio **"o**pen data by default**"** secondo cui tutti i dati e i documenti pubblicati dalla Pubblica Amministrazione che non hanno una licenza specifica sono considerati dati aperti, eccezion fatta per i dati personali che rimangono protetti, secondo quanto stabilito all'articolo 52 del CAD. Grazie a questa disposizione, le amministrazioni pubblicano gli open data sui propri siti istituzionali. In questo modo, i cittadini e le imprese possono facilmente accedervi e riutilizzarli. Inoltre, si ritiene che il principio in questione e la relativa normativa si debbano applicare altresì per tutte le amministrazioni pubbliche. Difatti, nel novero dei soggetti che possono accedere ai dati e fruirne liberamente, qualora

---

[100] S. Rossa, Contributo allo studio delle funzioni amministrative, cit., p. 179

[101] Cfr. Artt. 50 a 57 bis d.lgs. 82 del 2005

[102] ICT è l'acronimo dell'espressione inglese *Information and Communications Technology*, che si traduce in "tecnologia dell'informazione e della comunicazione". La sigla identifica la scienza che studia le attività e le tecniche per ricevere, trasformare e trasmettere le informazioni, https://www.nextre.it/ict-cose/,

[103] emanati in Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE

l'utilizzo si rende necessario per garantire lo svolgimento di compiti istituzionali, vi rientrano proprio le pubbliche amministrazioni[104].

Infine, l'articolo 51 del CAD stabilisce che le Linee guida dell' AGID (Agenzia per l'Italia Digitale) definiscono le soluzioni tecniche per proteggere dati e documenti digitali, con il duplice obbiettivo di garantire l'integrità, la disponibilità e l'accessibilità dei dati e assicurare la continuità operativa delle infrastrutture digitali delle amministrazioni.

In definitiva, l'open data rappresenta un pilastro essenziale della digitalizzazione pubblica. Dalla sua base costituzionale, che lo lega alla libertà scientifica, fino alla sua attuazione pratica attraverso il Codice dell'Amministrazione Digitale e le linee guida di AGID, il quadro normativo mira a un unico obiettivo: trasformare i dati pubblici in una risorsa accessibile e riutilizzabile. Questo non solo accresce la trasparenza, ma genera valore economico e sociale, dimostrando come l'apertura sia la chiave per un'amministrazione più efficiente e vicina ai cittadini.

2.4.2 Gli open data come fondamento dell'open government

Con l'espressione open government, o "governo aperto" si fa riferimento alla capacità delle pubbliche amministrazioni di essere pienamente trasparenti nelle proprie attività e decisioni, il che implica non solo rendere accessibili servizi e informazioni, ma anche ascoltare attivamente e rispondere attivamente alle esigenze della società civile. Secondo quanto stabilito l'Open Government Partnership (OGP), un'iniziativa multilaterale lanciata nel 2011 che coinvolge 65 Paesi, i principi chiave che un governo deve avere per essere considerato aperto sono la trasparenza, la partecipazione e la collaborazione.

La trasparenza consiste nel rendere totalmente accessibili i dati e le informazioni della Pubblica Amministrazione, e non si configura solo come un dovere nei confronti dei cittadini ma anche come una necessità per la stessa amministrazione. In tal modo, infatti, si perviene la diffusione di notizie false o ambigue e si migliorano i processi decisionali e operativi interni, rafforzando il rapporto di fiducia tra cittadini e istituzioni proprio

[104]S. Rossa, Contributo allo studio della funzione amministrativa, cit, p. 179 ss.

facendo leva sul principio di trasparenza. Per fare qualche esempio, a livello internazionale la Corte europea dei diritti dell'uomo ha sancito questo principio, e oggi oltre 90 Paesi democratici hanno adottato un Freedom of Information Act (FOIA), di cui abbiamo parlato in precedenza. Quest'ultimo definisce precisi obblighi di informazione per la Pubblica Amministrazione e garantisce ai cittadini il diritto di richiedere qualsiasi dato in suo possesso, con l'unica eccezione di quelli che riguardano la sicurezza nazionale o la privacy. Da ciò si può agevolmente dedurre che il pieno accesso alle informazioni costituisce un pilastro essenziale della trasparenza totale. Come analizzato nel precedente paragrafo, gli open data sono lo strumento principale per garantire la trasparenza e l'accessibilità delle informazioni pubbliche. Questa pratica richiede che le pubbliche amministrazioni rendano i propri dati disponibili a tutti in un formato aperto e strutturato, il quale permette di analizzare e combinare informazioni da diverse fonti, rendendo possibile lo sviluppo di nuove applicazioni e servizi utili sia per la società che per il mercato. Un altro principio chiave dell'Open Government è la partecipazione dei cittadini, secondo il quale è necessario coinvolgerli nei processi decisionali, ascoltare le loro esigenze e avvalersi della loro collaborazione per la creazione di progetti e servizi rappresenta una naturale evoluzione delle moderne democrazie. In tal modo, non solo migliora la qualità delle decisioni amministrative e l'efficacia delle politiche pubbliche, ma rafforza anche il rapporto tra l'amministrazione e la collettività[105].

Tuttavia, non si può non far riferimento ad un altro principio chiave dell'open government, ossia l'accountability o responsabilizzazione. In base a tale principio la collettività ha il diritto di essere informata, di criticare le scelte dell'amministrazione e di ricevere risposte in merito. L'accountability presuppone la trasparenza, in quanto le amministrazioni sono tenute a rendere pubbliche le loro scelte e le relative motivazioni, e la partecipazione, garantendo spazi per il confronto e per le eventuali critiche.

Come accennato poc'anzi, la natura stessa dei dati aperti consente di concretizzare i principi di trasparenza, partecipazione e collaborazione. Più specificamente, gli open data, proprio in quanto aperti, consentono alla pubblica amministrazione di agire con maggiore trasparenza, essendo, infatti, tale dati liberamente accessibili e riutilizzabili da

[105] N. Iacono, G. Ruiu, *Open Government*, a cura di Formez PA, Dipartimento della Funzione Pubblica, ottobre 2015, disponibile all'indirizzo:https://egov.formez.it/sites/all/files/open_government.pdf

chiunque si può agevolmente verificare la correttezza delle decisioni amministrative. Tuttavia, il vero e proprio scopo dell'accessibilità dei dati va oltre la semplice trasparenza: punta a garantire la partecipazione dei cittadini alle decisioni pubbliche e a favorire la loro collaborazione con le istituzioni. In questo senso, gli open data possono essere considerati l'emblema dell'unione dei principi di open government. La loro gestione e analisi, oggi conosciuta come "Open Data Analysis pubblica"- che si configura come una vera e propria funzione nativa digitale - , costituisce un tassello fondamentale nel processo di digitalizzazione dell'amministrazione[106].

In conclusione, gli open data non sono solo il risultato della digitalizzazione, ma ne costituiscono un elemento fondamentale. Attraverso la "Open Data Analysis pubblica", l'amministrazione si evolve: non si limita più a pubblicare passivamente i dati, ma li trasforma in una risorsa dinamica per un'amministrazione più efficiente, responsabile e, soprattutto, più vicina ai cittadini. In questo senso, gli open data rappresentano un pilastro essenziale per costruire un governo aperto e democratico nell'era digitale.

2.4.3 Dalla funzione conoscitiva digitalizzata all'Open Data Analysis: la nascita di una funzione amministrativa nativa digitale

L'amministrazione pubblica, analogamente a qualunque soggetto razionale (o che tale venga considerato), raccoglie informazioni relative alla realtà concreta in cui opera. In particolare, l'attività conoscitiva riguarda l'acquisizione di dati indispensabili allo svolgimento dell'istruttoria. Questa attività si colloca in una fase ben definita del procedimento amministrativo, connessa all'adozione dell'atto finale. Proprio per questa ragione, essa è regolata, anche se non sempre in modo pienamente esaustivo, dalla legge n. 241 del 1990.

Nonostante ciò, l'interesse della dottrina verso l'attività conoscitiva della pubblica amministrazione non è sorto con l'entrata in vigore della legge n. 241/1990: già prima di questa normativa, dunque in assenza di una disciplina generale del procedimento amministrativo, l'attività conoscitiva rappresentava oggetto di ampio approfondimento teorico da parte degli studiosi.

[106] S. Rossa, Contributo allo studio della funzione ammnistrativa, cit., p. 185

Uno dei primissimi studi monografici ad affrontare il nesso tra conoscenza e attività amministrativa è attribuibile a Franco Levi, il quale nel 1967 pubblicò *L'attività conoscitiva della pubblica amministrazione*. Come si legge nell'Introduzione dell'opera – «questo lavoro si propone di portare in luce alcuni problemi concernenti, sub specie iuris, l'attività svolta dalla pubblica amministrazione per conoscere la situazione di fatto, in senso sociale, in cui si trova ad operare[107]» – Levi si dedica a un tema allora innovativo, considerando che la sua analisi anticipa di ben ventitré anni l'entrata in vigore della legge sul procedimento amministrativo. Nonostante ciò, quello studio resta oggi una pietra miliare nel dibattito giuridico su questi temi.

Non è necessario essere esperti del settore per comprendere come le tecnologie digitali abbiano influenzato praticamente ogni ambito della vita umana, impattando in maniera determinante anche i poteri pubblici e la pubblica amministrazione, con un'attenzione particolare al campo del diritto amministrativo.

In tale contesto, è mutato anche il modo in cui le amministrazioni pubbliche possono svolgere la loro attività conoscitiva**,** come argomentato in precedenza. Viviamo in un'epoca storica in cui la dimensione reale e quella virtuale si fondono e sovrappongono sempre più, tanto da far scomparire il confine tra online e offline. Questa condizione è ben descritta, tra gli altri, dal concetto coniato da Luciano Floridi dell'"onlife": un'esistenza immersa in una infosfera, un ambiente digitale in cui la vita online e offline coincidono[108]. In tale contesto, il dato assume oggi una centralità senza precedenti nella storia dell'umanità, e il suo impatto—sia sulle persone che sulle istituzioni, pubbliche o private—è stato, ed è destinato a essere, disruptive[109].

In sostanza , oggi i dati sono fondamentali per l'attività conoscitiva della pubblica amministrazione, che si esercita soprattutto ai fini dell'istruttoria procedimentale, come sottolineato anche nel piano nazionale di ripresa e resilienza (PNRR).

La discrezionalità nell'ambito dell'istruttoria, il principio inquisitorio e la libertà nella scelta degli strumenti istruttori stanno portando sempre più le amministrazioni pubbliche

[107] F. Levi, l'attività conoscitiva della pubblica amministrazione, Giappichelli, Torino, 1967
[108] Il riferimento è a L. Floridi, The onlife Manifesto. Being a human in a hyperconnected Era, Springer, Heidelberg New York, 2015
[109] S. Rossa, Contributo alla funzione ammnistrativa, cit, p. 195 ss

a svolgere la loro funzione cognitiva — in particolare l'istruttoria procedimentale — attraverso strumenti digitali. Le tecnologie dell'informazione e della comunicazione (ICT) agiscono come un vero e proprio motore del processo conoscitivo, potenziando notevolmente questa funzione, il cui punto di partenza rimane indiscutibilmente il dato.

Prima dell'avvento delle tecnologie digitali, l'attività conoscitiva si basava essenzialmente su documenti cartacei: anche nelle verifiche sul campo o nelle ricognizioni, i risultati venivano formalizzati "su carta". Il passaggio alla gestione digitale del dato rappresenta, al confronto, una svolta radicale in termini di economicità ed efficienza per l'amministrazione.

Difatti, le tecnologie digitali hanno consentito il passaggio da un processo statico fondato sui documenti cartacei in uno dinamico, grazie al trattamento e alla fruizione digitale dei dati. La cosiddetta *Big Data Analysis* consente all'amministrazione di porre in essere una funzione conoscitiva più accurata, veloce ed efficace, pur mantenendo la stessa natura che aveva prima della digitalizzazione.[110] Il passaggio a questa nuova prospettiva porta a considerare un elemento fondamentale: l'innovazione nella conservazione e fruizione del dato digitale è poco significativa se il dato viene visto isolatamente. Il vero salto qualitativo si ottiene quando i vantaggi della gestione digitale—rispetto ai tradizionali documenti—divengono esponenzialmente più incisivi nel contesto dell'analisi aggregata. In sostanza, i benefici si moltiplicano quando i dati sono trattati in massa. Pertanto, per sfruttare appieno l'attività conoscitiva, resa più potente grazie alle tecnologie digitali, la pubblica amministrazione deve fare affidamento sull'elaborazione dei cosiddetti **Big Data**[111].

Come già evidenziato, nelle fonti giuridiche, sia a livello nazionale che internazionale, è possibile trovare una definizione di *open data*, ma ciò non accade per i *big data*. Non

[110] Bruno Carotti (a cura di), *Le funzioni amministrative digitali. Intervista a Stefano Rossa*, Osservatorio sullo Stato Digitale – IRPA, 2023

[111] si tratta di "una raccolta di dati informatici così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza", definizione tratta da *Wikipedia*, voce Big Data

esistono fonti normative, primarie o secondarie, che forniscano una definizione chiara di quali dati possano essere classificati come *big data.*

In primo luogo, è evidente che per big data si intende una quantità enorme di dati che possono essere combinati tra loro per produrre ulteriori dati, che vengono considerati come nuovi dati[112]. Affinchè questa combinazione di dati possa essere utile, è necessario che gli stessi siano eterogenei, ossia che non siano omogenei. Inoltre, è fondamentale che l'elaborazione di questi dati avvenga rapidamente: senza tale velocità, analizzare enormi volumi di dati diventerebbe troppo costoso sia in termini di tempo che di risorse economiche[113]. Esperti e studiosi hanno classificato le caratteristiche dei big data come le 3V: velocità, varietà e volume. Tale Teoria, nota appunto come teroia delle 3 V, fu elaborate circa vent'anni fa, e con il tempo è stata arrichita dalla previsioni di alter 2 V, che si sono rese necessarie per le definizione di questo tipo di dati, ossia la veridicità e il valore. Il **primo indica che** devono essere precisi e affidabili per una corretta analisi, il secondo invece che i dati, sebbene possano generare valore, necessitano di adeguati investimenti per essere analizzati correttamente.

Le caratteristiche sopra indicate mostrano come **l'**analisi dei Big Data **(**Big Data Analysis) risulti estremamente vantaggiosa per l'attività conoscitiva della pubblica amministrazione, soprattutto per quanto riguarda l'istruttoria. Infatti, l'analisi dei big data permette ball'amministrazione di svolgere un'indagine preliminare molto più approfondita, precisa e rapida rispetto alle tradizionali modalità documentali. Pertanto, si potrebbe affermare che la big data anlysis assume un ruole determinate per garantire il soddisfacimento dell'interesse pubblico e per l'azione ammnistrativa, in particolare per la funzione conoscitiva dell'ammnistrazione.

La funzione conoscitiva della pubblica Amministrazione, pur se potenziata grazie alla Big Data Analysis rimane del resto la medesima funzione descritta da Franco Levi nel 1967. Certo, oggi è più precisa, completa, efficace ed efficiente, a è pur sempre la stessa attività cognitiva originaria. La diffusione delle ICT non genera una funzione conoscitiva

[112] In proposito vedi anche da ultima Cass. Civ., Sez. I, n. 15096 del 2015, , p. 4.4.4: «colui che compie operazion di trattamento di tali informazioni può trarre un valore aggiunto informativo dal loro accostamento, comparazione, esame analisi, congiunzione, rapporto od incrocio, non estraibile dai dati isolatamente considerati»

[113] F. Costantino, Lampi. Nuove frontiere delle decisioni ammnistrative tra open e big data, Giuffrè, Milano, 2017

nuova, ma potenziano quella "tradizionale" esistente già prima della digitalizzazione: una funzione proattiva, in cui l'amministrazione ricerca attivamente e concretamente le informazioni necessarie al proprio agire. In sostanza, la big data analysis consente semplicemente di svolgere meglio ciò che la pubblica amministrazione ha sempre fatto, concretizzando i principi fondamentali dell' attività amministrativa — imparzialità, buon andamento, efficienza, efficacia ed economicità. Difatti, si parla di funzione ammnistrativa digitalizzata, ossia una funzione già esistente migliorata dall'uso delle tecnologie dell'informazione. Ma non di *funzione amministrativa nativamente digitale*[114].

Pertanto, quando si parla di funzione ammnistrativa digitalizzata si fa riferimento ad una funzione presistente resa più efficacia grazie all'uso delle nuove tecnologie. l'uso delle ICT nella funzione conoscitiva della pubblica amministrazione rappresenta una delle due facce del concetto di digitalizzazione: la faccia in cui la digitalizzazione è intesa come processo attraverso il quale le amministrazioni si organizzano per esercitare funzioni già esistenti (come l'attività conoscitiva proattiva), utilizzando le ICT per perseguire principi classici come imparzialità, buon andamento, efficienza, efficacia ed economicità: questa è la digitalizzazione come strumento di potenziamento. D'altro canto esiste anche una digitalizzazione differente, ossia quando le ammnistrazioni svolgono nuove funzioni che non esistevano prima dell'avvento dell'era digitale. Si parla in tal caso di funzioni amministrative digitali, le quali affondano le loro radici nei principi dell'open government, come trasparenza, partecipazione, collaborazione.

Nel caso della funzione conoscitiva, il cambio di paradigma non deriva tanto dalla Big Data Analysis, quanto dall'Open Data Analysis: l'analisi dei dati aperti pubblici trasforma profondamente la funzione conoscitiva, generando un nuovo modello conoscitivo, progettato per operare secondo i valori dell'accessibilità, della condivisione e del coinvolgimento civico.

L'analisi dei big data è spesso utilizzata dalla pubblica ammistrazione con particolare riferimento all'istruttoria procedimentale: l'amministrazione analizza enormi volumi di dati, spesso esterni alla propria sfera operativa, li raccoglie, li combina con altre fonti e da essa trae informazioni utili per perseguire i propri fini istituzionali. Questa attività conoscitiva è esercitata internamente, in quanto diretta all'ammnistrazione stessa, la quale

[114] S. Rossa, Contributo alla funzione ammnistrativa, cit., p. 205

in tal mdoo svolge una funzione ammnistrativa digitalizzata, ossia una funzone che ha sempre esercitato nel corso del tempo, ma con mezzi e strumenti evoluti.

Diversamente, **l'**Open Data Analysis introduce un cambiamento significativo: la pubblica amministrazione, anziché ricercare dati esterni in maniera proattiva, organizza e analizza i dati in suo possesso e li rende disponibili come Open Data**.** In tal modo, la funzione conoscitiva amministrativa non è più attiva in prima persona, ma diventa un facilitatore, mettendo a disposizione i dati affinché siano soggetti terzi, tra cui cittadini, imprese, a prenderne visione e analizzarli autonomamente. Di conseguenza, la funzione cognitiva della PA non è più finalizzata direttamente a fornire informazioni all'ente stesso, ma diviene un mezzo che diffonde la conoscenza verso l'esterno, e contempo il tramite attraverso cui la conoscenza viene resa accessibile a terzi.

La funzione amministrativa conoscitiva derivante dall'analisi dei dati aperti rappresenta una funzione completamente *nuova che si discosta da* quella "tradizionale" descritta precedentemente sotto diversi aspetti . Innanzitutto, muta il soggetto destinatario del processo conoscitivo: mentre nella funzione "tradizionale" esso è l'amministrazione stessa, invece nella funzione "innovativa" sono i cittadini e le imprese che ne traggono beneficio. Inoltre, si differenziano anche per quanto riguarda l'oggetto della conoscenza (da un lato big data e open data dall'altro), le modalità pratiche (ricerca proattiva contro apertura dei dati da parte dell'amministrazione), e le discipline di riferimento (da un lato procedimento amministrativo ex legge n. 241/1990 dall'altro regolamentazione sull'accesso, sul riuso dell'informazione e sul Codice dell'Amministrazione Digitale).

Ancora più incisivo , tuttavia, è stato il mutamento dei principi ispiratori. Se la funzione conoscitiva "tradizionale" vuole realizzare i principi amministrativi classici, quali imparzialità, buon andamento, efficienza, efficacia e economicità, invece la funzione conoscitiva "innovativa" mira a realizzare i principi cardine dell'**Open Government** — trasparenza, partecipazione e collaborazione — in quanto si concentra sul garantire ai cittadini la possibilità di conoscere, anziché renderli principali soggetti destinatari della conoscenza.

Proprio per queste ragioni, e grazie al ruolo centrale assunto delle tecnologie digitali nella gestione, nell'analisi, nella conservazione e nella fruizione degli open data **—**

possiamo senza dubbio affermare che l'Open Data Analysis pubblica rappresenta come una *funzione amministrativa nativa digitale*, ossia una funzione amministrativa completamente nuova, che si è sviluppata solo grazie all'avvento delle ICT.

2.4.4 L'importanza di garantire la qualità e l'affidabilità dei dati

Nell'odierna società dell'informazione, i dati rappresentano una risorsa fondamentale per le organizzazioni. Tuttavia, la loro utilità è strettamente legata alla qualità e all'affidabilità con cui vengono gestiti. L'articolo 5 del Regolamento (UE) 2016/679 (GDPR) stabilisce principi fondamentali come la qualità dei dati.

Invero tale principio fu introdotto per la prima volta nella Convenzione 108 del 1981, di cui abbiamo già parlato in precedenza[115], ossia uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali, il cui scopo è "*quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)*".[116] Tale Convenzione stabiliva determinati requisiti che dovevano essere rispettati per garantire correttezza nel trattamento dei dati personali, ed oggi sono stati ripresi nell'articolo 5 del GDPR. L'articolo 5 dello stesso regolamento, come è ormai noto, enuncia il principio di minimizzazione dei dati[117], imponendo che i dati siano "adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità per le quali sono trattati". Questo significa che non devono essere raccolti o trattati dati superflui rispetto alla finalità per le quali è previsto il trattamento.

Inoltre, qualora l'obiettivo potesse essere raggiunto utilizzando dati anonimizzati o pseudonomizzati, si deve privilegiare questa alternativa per evitare l'uso di dati personali. Si tratta del noto principio di privacy by design and by default, il quale deve essere

[115] Si veda al riguarda cap. 1, par. 1.3
[116] Art. 1 della Convenzione 108 del 1981
[117] Anche qui si rinvia al cap. 1, par. 1.3

integrato fin dalla fase di progettazione del trattamento[118]. In aggiunta, nello stesso regolamento viene stabilito che i dati trattati devono essere esatti, aggiornati e se inesatti, si deve provvedere alla loro correzione su richiesta dell'interessato. Ad esempio, un'azienda non può usare i dati di fatturazione per aggiornare gli indirizzi dei clienti e inviare loro comunicazioni commerciali senza aver ottenuto un nuovo consenso. Difatti, l'esattezza dei dati è estremamente rilevante, soprattutto con riferimento ai sistemi di profilazione e intelligenza artificiale, che analizzano enormi quantità di dati (big data)[119] per prendere decisioni che possono influenzare significativamente la vita delle persone, come l'accesso a benefici assicurativi o previdenziali, in quanto dati non accurati potrebbero comportare discriminazioni gravi. Inoltre, l'attualità del dato è essenziale: l'uso di informazioni obsolete potrebbe generare valutazioni errate, poiché il "profilo" di un individuo può sensibilmente cambiare nel corso del tempo[120].

Inoltre, è importante ribadire il principio di limitazione della conservazione, anch'esse previsto all'articolo 5 del GDPR, secondo il quale i dati personali devono essere necessariamente conservati per un periodo non superiore a quello strettamente necessario per la finalità del trattamento. Pertanto, una volta raggiunto lo scopo, i dati devono essere cancellati, o altrimenti, anonimizzati. In quest'ultimo caso, la normativa sulla protezione dei dati non si applicherà più, dal momento che non sono più identificabili gli interessati[121].

Oltretutto la normativa ISO/IEC 27001[122] fornisce un quadro di riferimento per la gestione della sicurezza delle informazioni, il cui obbiettivo è quello di proteggere i dati e le informazioni da minacce di qualsiasi genere, al fine di assicurarne l'integrità, la riservatezza, e la disponibilità attraverso un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) certificato.

[118] Autore non specificato, "Principio di qualità dei dati, in https://protezionedatipersonali.it/qualita-dei-dati?utm_, consultato 16 agosto 2025
[119] Si rinvia al paragrafo precedente
[120] Belisario, Riccio, Sforza, GDPR e normative privacy commentario, Wolter Kluters, 2022
[121] Sul punto si veda anche Corte di Cassazione, sez. pen. III, Sent. N. 3702, 1° febbraio 2022 in materia di trattamento illecito di dati giudiziari e ammnistrativi.
[122] Lo standard ISO/IEC 27001 è una norma internazionale che contiene I requisiti per impo https://it.wikipedia.org/wiki/ISO/IEC_27001stare e gestire un SGSI,

Un eventuale la mancata adozione di misure idonee ad assicurare il rispetto della qualità e dell'affidabilità dei dati può portare gravi conseguenze legali e reputazionali. Ad esempio, nel 2018, Marriott International ha subito una sanzione di 124 milioni di dollari ai sensi del GDPR per violazioni derivanti da una gestione inadeguata dei dati.

A tal proposito, sembra opportuno analizzare più specificatamente questo caso di studio significativo, caratterizzato dalla pesante sanzione pecuniaria inflitta alla catena di alberghi Marriot, in quanto evidenzia la cruciale necessità di proteggere l'integrità e la riservatezza dei dati per prevenire violazioni e danni ingenti.

Nell'ottobre del 2020 l'ICO (Information Commisioner's Office), autorità garante per la protezione dei dati personali nel Regno Unito, ha inflitto una pesante sanzione pecuniaria pari circa a 18, 4 milioni di sterline al Marriot International poiché l'azienda in questione non è riuscita a porre in essere sistemi adeguati di tutela dei dati personali di milioni di clienti. La sanzione è avvenuta in seguito ad un cyberattacco verificatosi nei confronti della catena alberghiera Starwood hotel, successivamente acquista da Marriot. Tuttavia, il cyberattacco è stato rilevato solo quattro anni più tardi, a settembre 2018, proprio grazie alle indagini dell'ICO. Queste ultime hanno anche indicato come gli hacker sono riusciti a penetrare nel sistema di Starwood hotel: hanno installato un malware che ha dato loro accesso da remoto con permessi da ammnistratore e hanno usato altri strumenti per rubare le credenziali di accesso di alcuni utenti, tramite cui hanno potuto violare il database di Starwood, rubando i dati di prenotazione di milioni di clienti. Sebbene Marriot abbia tentato di attenuare le conseguenze tempestivamente informando subito l'ICO e i clienti per cercare di limitare il danno, l'autorità, dopo un'attenta valutazione, ha comunque sanzionato l'azienda, ritenendo che non avesse adottato le misure di scurezza necessarie, né a livello tecnico, né a livello organizzativo. Proprio per questa ragione, l'ICO ha stabilito che Marriot ha violato i principi del GDPR, in particolare l'articolo 5, comma 1, lettera f) sull'integrità e la riservatezza dei dati, nonché l'articolo 32 relativo alla sicurezza del trattamento[123].

[123] "Marriot hotel: multa da 20,4 milioni di euro a seguito di data breach", in https://www.feder-privacy.org/informazione/societa/marriott-hotel-multa-da-20-4-milioni-di-euro-a-seguito-di-un-data-breach, 16 agosto 2025

Pertanto, garantire la qualità e l'affidabilità dei dati non è solo una best practice tecnica, ma un obbligo giuridico che implica responsabilità e trasparenza[124]. Le organizzazioni devono implementare politiche di governance dei dati efficaci, condurre audit regolari e adottare tecnologie che assicurino la protezione e l'integrità delle informazioni. Solo così è possibile tutelare i diritti degli individui, rispettare gli obblighi normativi e mantenere la fiducia degli stakeholder.

Inoltre, l'affidabilità e la qualità dei dati è estremamente importante anche per migliorare il processo decisionale, poiché solo con informazioni precise, complete e aggiornate si possono assumere decisioni efficaci. Difatti, data di alta qualità consento di avere un quadro chiaro della situazione e riducono la possibilità di errore. Da ciò si può agevolmente dedurre che sia che si tratti di un'azienda che pianifica una nuova strategia di marketing o di un governo che delinea politiche sanitarie, l'efficacia delle scelte è in ogni caso determinata dalla qualità dei dati. Infine, mantenere sin dall'inizio l'affidabilità dei dati consente di operare in modo più efficiente e di ottimizzare le risorse, poichè dati di scarsa qualità otre ad aumentare il rischio di incorrere in errori rallentano enormemente i processi e aumentano i costi.

Capitolo III

Il diritto di accesso ai dati sanitari: equilibri e prospettive

La disciplina dei dati personali e dei soggetti del trattamento: inquadramento normative

G. Coraggio, Privacy e Data Protection, IPSOA, 2022

Nel seguente capitolo si vuole approfondire il tema del diritto di accesso ad una particolare categoria di dati, ossia i dati sanitari. un diritto fondamentale che si inserisce nel più ampio quadro della protezione dei dati personali, con particolare riferimento al settore sanitario. Tuttavia, per comprendere appieno la portata e le implicazioni giuridiche di tale diritto, occorre, in via preliminare, chiarire alcuni concetti essenziali in materia di protezione di dati personali.

In particolare, si ritiene necessario, al fine di garantire una trattazione esaustiva, soffermarsi sulla definizione di dato personale**,** sulla classificazione delle sue diverse categorie, nonché sull**'**identificazione dei soggetti coinvolti nel trattamento **e** sulla nozione stessa di trattamento ai sensi del Regolamento (UE) 2016/679. Si tratta di elementi che rappresentano il cuore concettuale per effettuare un'analisi consapevole e coerente del diritto di accesso ai dati sanitari, oggetto della presente trattazione.

All'interno del Regolamento UE 2016/679 i dati personali sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente. L'identificabilità può avvenire non solo attraverso elementi univoci come il nome e il cognome, ma anche tramite dati che, combinati tra loro, consentono di risalire all'identità dell'individuo come per esempio, il codice fiscale, l'indirizzo IP, il numero di targa, le immagini o la voce, che rappresentano dati identificativi diretti o indiretti.

A tal punto, pare opportuno evidenziare come all'interno del suddetto regolamento un particolare occhio di riguardo sia riservato ai dati "particolari" – precedentemente noti come dati "sensibili" – disciplinati dall'articolo 9 del Regolamento stesso[125]. All'interno di tale categoria vanno ricomprese

tutte le informazioni idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale dell'interessato. Proprio in ragione della loro delicata natura e specificità il trattamento di

[125] Nel precedente impianto normativo Italiano, disciplinato dal d.lgs. 196/2003 (noto come "Codice Privacy"), l'articolo 4, comma 1, lettera d), definiva come *dati sensibili* quelle informazioni personali in grado di rivelare, tra le altre cose, l'origine razziale o etnica, le convinzioni religiose, filosofiche o politiche, l'adesione a partiti o sindacati, nonché elementi inerenti allo stato di salute e alla vita sessuale di una persona. Solamente Con l'entrata in vigore del Regolamento (UE) 2016/679 (GDPR), il concetto di *dato sensibile* viene superato e riformulato nella nozione di *categorie particolari di dati personali*, così come disciplinata principalmente all'articolo 9.

tali dati è soggetto a stringenti limiti e può avvenire solo in presenza di determinate condizioni di liceità.

Inoltre, accanto a questi, il GDPR distingue anche i dati giudiziari, che comprendono le informazioni relative a condanne penali, reati o misure di sicurezza ad essi collegate, secondo quanto stabilito all'articolo 10. Più specificatamente ci si riferisce ai dati che possono derivare da provvedimenti giudiziari iscritti nel casellario giudiziale o da procedimenti penali in corso, e che pertanto esigono di essere trattati con particolare accortezza, al fine di evitare il verificarsi di ingiuste discriminazioni o violazioni dei diritti fondamentali della persona che potrebbero derivare da un trattamento inopportuno e poco attento[126].

Ulteriormente, pare opportuno sottolineare in questa sede, che con l'evoluzione delle tecnologie digitali e di dispositivi connessi e la loro sempre più ampia diffusione, emergono nuove tipologie di dati che stanno acquisendo sempre maggior rilevanza sotto il profilo della tutela della privacy.

Tali dati, anche se non sempre possono essere ricompresi nelle categorie particolari o giudiziarie, possono comunque incidere profondamente sulla sfera privata dell'interessato, rendendo necessaria una gestione consapevole e conforme ai principi fondamentali del trattamento dei dati personali.

Per ragioni espositive e al fine di garantire una maggiore chiarezza concettuale all'interno della trattazione, occorre identificare le principali figure coinvolte nel trattamento. Prevista dalla normativa europea in materia di protezione dei dati personali.

Andando per ordine, l'articolo 4 comma 1 paragrafo 1 punto definisce in primis l'interessato

è la persona fisica cui si riferiscono i dati personali oggetto di trattamento. In sostanza, si tratta del soggetto i cui dati vengono raccolti e utilizzati: ad esempio, se un sistema tratta l'indirizzo o il codice fiscale di un individuo, quest'ultimo assume il ruolo di interessato. Successivamente viene definito il titolare del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, l'impresa o qualsiasi altro ente che determina in autonomia le finalità (il perché) e i mezzi (il come) del trattamento dei dati personali (art. 4, par. 1,

[126] Garante per la protezione dei dati personali, Cosa intendiamo per dati personali, in https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali, 20 agosto 2025

punto 7 GDPR). In sostanza, il titolare del trattamento è considerato il principale responsabile delle decisioni assunte in materia di protezione dei dati personali.
Dopodiché il GDPR individua la figura del responsabile del trattamento, ossia il soggetto che tratta e gestisce i dati per conto del titolare, seguendo le istruzioni impartitegli da quest'ultimo limitatamente a specifici compiti. Il più delle volte si tratta di fornitori esterni o partner che gestiscono determinate attività tecniche o organizzative legate al trattamento dei dati[127]. Inoltre lo stesso Regolamento, prevede la possibilità per il responsabile di designare a sua volta e con il consenso del titolare dl trattamento, un sub-responsabile, che è tenuto a svolgere, sotto la sua responsabilità, alcune specifiche attività.[128]
Infine, viene esaustivamente definito il concetto di trattamento, ricomprendendo al suo interno *"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;".*[129] Si ribadisce inoltre che, ai sensi dello stesso Regolamento, tutti i soggetti che effettuano operazioni di trattamento sono tenuti ad adottare misure tecniche e organizzative adeguate per garantire un utilizzo corretto e sicuro dei dati personali, nel rispetto dei diritti e delle libertà fondamentali dell'interessato[130].

3.1 Definizione di dati sanitari: categorie e tipologie

Nella società odierna, i dati sanitari sono diventati una risorsa fondamentale, poiché essi non si limitano alla sole informazioni cliniche, ma includono numerosi dettagli che, se analizzati correttamente, possono contribuire al miglioramento della prevenzione, la diagnosi e l'efficacia dei trattamento.

[127] art. 4, par. 1, punto 8 GDPR
[128] Art. 28, par. 2 del GDPR
[129] art. 4, par. 1, punto 2 GDPR
[130] Su questo punto si rinvia al cap. 2, par.

Nel seguente capitolo, si cercherà di dare una definizione chiara e completa di tali dati, offrendo al contempo una panoramica chiara sulle loro diverse categorie e tipologie, al fine di mettere in evidenza come la loro corretta classificazione sia essenziale per garantirne la sicurezza e l'utilizzo etico e funzionale.

L'articolo 4 del GDPR è una disposizione chiave, poiché sebbene non contenga disposizioni operative chiarisce il significato di parole, concetti e termini in maniera precisa e concisa con lo scopo di evitare incertezze interpretative o nell'applicazione dello stesso Regolamento. Come analizzato in precedenza, il regolamento precisa che per dati personali si debba intendere "*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"*[131]. Inoltre, tale articolo opera un'importante distinzione tra dati personali comuni e categorie particolari dati personali, noti generalmente come dati sensibili, tra i quali per l'appunto vanno ricompresi i dati genetici, i dati biometrici e i dati relativi alla salute, di cui esploreremo qui di seguito la definizione in maniera più approfondita.

Per "Dati generici" si intendono i dati personali con riferimento alle caratteristiche genetiche di una persona fisica che possono essere ereditarie o acquisite. Essi ci forniscono le informazioni sulla salute di una persona che si rilevano attraverso l'analisi di un campione biologico di tale individuo, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.

Per "Dati biometrici" si intendono i dati ottenuti quale risultato di un trattamento tecnico specifico relativi a caratteristiche fisiche, comportamentali o fisiologiche di una persona che ne confermano in modo inequivocabile l'identificazione. Tra gli esempi più ricorrenti abbiamo le impronte digitali, la scansione dell'iride, la scritturazione.

Per "Dati relativi alla salute" si intendono, come riportato al n. 15 dell'art. 4 del citato GDPR *"i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni*

[131] Art. 4 comma 1 del GDPR

relative al suo stato di salute". In tal senso, come pure precisato nei Considerando 35 e 63 del ripetuto GDPR, tra di essi rientrano tutti i dati riguardanti lo stato di salute del soggetto interessato atti a rivelarci il suo stato di salute presente, passato e futuro ed includono diagnosi effettuate, terapie, trattamenti clinici, interventi subiti e qualsiasi altra informazione idonea a delineare lo stato di salute complessivo di quel determinato soggetto.
L'art. 9 del GDPR ha definito tali dati quali *"categorie particolari di dati personali"* il cui trattamento è consentito solo al ricorre di specifiche circostanze.

Per quanto riguarda il trattamento delle categorie particolari di dati personali alla luce del l'art. 9 del GDPR, come anche chiarito dall'Autorità Garante italiana in data 7 marzo 2019, elenca una serie di eccezioni al generale principio del divieto generale di trattare le cosiddette categorie particolari di dati, che pertanto rendono lecito il loro utilizzo. In particolare in ambito sanitario tali eccezioni vengono riconosciute al ricorrere delle seguenti circostanze: motivi di interesse pubblico sulla base di quanto prescritto dal diritto dell'Unione o degli Stati membri individuati dall'art. 2 sexies del Codice, nonché motivi di interesse pubblico nel settore della sanità pubblica, ad esempio per la protezione della salute pubblica in casi di gravi minacce a livello transfrontaliero (es. pandemie) o per garantire adeguati parametri di affidabilità e sicurezza di medicinali, dispositivi medici al fine di approntare adeguate misure di sicurezza e protezione degli individui, 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;
Ulteriormente finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale e pertanto per la gestione dei sistemi e servizi sanitari (cd. finalità di cura) sulla base del diritto dell'Unione o degli Stati membri o conformemente ad un contratto con professionista della sanità, a condizione che siano effettuati da un professionista sanitario (o sotto la sua responsabilità) con obbligo di segretezza (art. 9 comma 2 lettera h e comma 3).
Pertanto per la cd. finalità di cura, diversamente dal passato, il professionista sanitario, peraltro soggetto al segreto professionale (o altro soggetto sempre tenuto al segreto professionale), non deve più richiedere il consenso del paziente per poter espletare i

trattamenti necessari alla prestazione sanitaria richiesta, sia che operi in ambito privato sia che operi nell'ambito della sanità pubblica. Si precisa che per trattamenti necessari si intendono quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (cfr Considerando n. 53 GDPR). Per gli eventuali trattamenti attinenti solo in senso lato alla cura, ma non strettamente necessari, anche se effettuati da professionisti sanitari, sarà comunque richiesto il consenso del paziente, salvo il ricorrere di altri presupposti di liceità (art. 6 e 9 comma 2 GDPR).

Si precisa infine che al ricorrere di un interesse pubblico rilevante ai sensi dell'art, 2 sexies del Codice della Privacy, si possono includere le attività amministrative e certificatorie strettamente connesse ed essenziali per il raggiungimento delle finalità di prevenzione, cura, diagnosi, assistenza, riabilitazione comprese quelle connesse alla gestione del rapporto con il paziente quali prenotazione di prestazioni sanitarie, accettazione, incluse i servizi di messaggistica pro-memoria di appuntamenti (cd. remainder).

Con riferimento al requisito del consenso dell'interessato il Garante per la protezione dei dati personali ha ritenuto opportuno individuare, a titolo esemplificativo, alcune casistiche in cui il trattamento dei dati personali non può essere giustificato da finalità necessarie e, pertanto, viene il richiesto che il consenso sia rilasciato espressamente dall'interessato.

In sostanza, in tutte le ipotesi diverse da quelle sopra elencate è richiesto il consenso specifico dell'interessato (art. 9 comma 2 lettera a), quindi anche per il trattamento di dati connesso all'utilizzo di App mediche, tramite le quali vengono raccolti dati personali di natura sanitaria anche per scopi diversi da quelli legati alla telemedicina, nonché di programmi volti alla fidelizzazione della clientela, per finalità promozionali o commerciali (es. promozioni su programmi di screening, contratto di fornitura di servizi ammnistrativi, come quelli alberghieri di degenza), e infine per trattamenti effettuati con sistemi elettronici quali il Fascicolo sanitario elettronico ed il Dossier sanitario elettronico.

3.1.2 Il contesto normativo: dell'accesso ai dati sanitario: tra GDPR e normativa nazionale

Il diritto di accesso ai dati personali, e in particolare ai dati sanitari, trova il suo fondamento normativo nella tutela dei dati personali offerta dal Regolamento (UE) 2016/679, in combinato disposto con il d.lgs. 196/2003, come modificato dal d.lgs. 101/2018[132]**.**

L'applicazione del Regolamento, unitamente alla normativa prevista dal Codice Privacy**,** **c**ome modificato dal d.lgs. 101/2018, ha sollevato numerosi problemi interpretativi per i titolari e i responsabili del trattamento operanti nel settore sanitario. Più specificatemene, sono sorti dubbi significativi circa le modalità con cui effettuare lecitamente il trattamento dei dati sanitari alla luce del nuovo quadro normativo nazionale e europeo. Proprio in ragione di tali criticità, e in risposta alla richiesta proveniente da vari operatori sanitari e dai responsabili della protezione dei dati personali (DPO), il garante per la protezione dei dati personali è intervenuto in proposdito con apposito provvedimento, ossia il provvedimento n. 55 del 7 del 2019[133], il cui scopo principale è quello di fornire chiarimenti in ordine all'applicazione della disciplina, in particolare con riferimento al settore sanitario.

L**'**articolo 15 del GDPR sancisce espressamente che *"'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 (...)".* Tale diritto assume una particolare rilevanza quando i dati oggetto di accesso riguardano la salute dell'individuo, trattandosi di informazioni rientranti tra le *categorie particolari di dati personali* ai sensi dell'art. 9 del Regolamento. Per quanto riguarda la normativa nazionale, il diritto di accesso ai dati sanitari viene ulteriormente disciplinato da leggi settoriali, tra cui emerge l'articolo 22, comma 7 del Codice Privacy, il quale stabilisce che il trattamento dei dati idonei a rivelare lo stato di salute può essere effettuato anche senza il consenso dell'interessato, qualora sia necessario per tutelare un diritto in sede giudiziaria o per adempiere ad obblighi previsti dalla legge. In tale contesto, bisogna anche tenere in considerazioni, unitamente al Codice

[132] Salvatore Coppola, *Protezione dei dati sanitari, tutti i paletti del Garante Privacy, Agenda Digitale,* 27 marzo 2019, in https://www.agendadigitale.eu/sicurezza/privacy/protezione-dei-dati-in-sanita-tutti-i-paletti-del-garante-privacy/. 20 agosto 2025

[133] Garante per la protezione dei dati personali, *Provvedimento 7 marzo 2019, n. 55 – Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario,* [doc. web n. 9091942], disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942

della Privacy, specifiche disposizioni previste nel Codice di Deontologia Medica[134], nella disciplina sul Fascicolo Sanitario Elettronico[135]**,** nonché nelle linee guida e nei provvedimenti del Garante per la protezione dei dati personali**.**

L'accesso ai dati sanitari non rappresenta solo un diritto strumentale alla tutela della salute, ma anche una manifestazione dell'autodeterminazione informativa e del principio di trasparenza, in particolare in riferimento al rapporto tra struttura sanitaria e paziente. Tuttavia, tale diritto subisce inevitabilmente delle limitazioni, sorrette dall'esigenza di tutela sia delle libertà e diritti altrui, sia del segreto professionale, specialmente nel caso in cui l'accesso sia richiesto da terzi, quali per esempio eredi o congiunti.

Le strutture sanitarie oggigiorno sono tenute a confrontarsi con il complesso quadro normativo sorto con l'avvento del GDPR, nonché con la le disposizioni nazionali applicabili in materia di protezione dei dati personali. Al fine di assicurare conformità alle disposizioni europee è necessario tenere in considerazione non solo la normativa nazionale vigente, ma anche delle indicazioni interpretative fornite dal Garante per la protezione dei dati personali e degli orientamenti applicativi elaborati dal legislatore italiano specificamente per il settore sanitario[136].

L'articolo 4 del GDPR, come accennato in precedenza, chiarisce che i dati relativi alla salute sono "*sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

Più specificatamente nel Considerando n. 35 del GDPR viene stabilito che "*nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono […] qualsiasi informazione*

---

[134] Approvato dal consiglio direttivo dell'Ordine il 11/09/ identifica le regole, ispirate ai principi di etica medica, che disciplinano l'esercizio professionale del medico chirurgo e dell'odontoiatra iscritti ai rispettivi Albi professionali

[135] Sul punto vedi articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221, che definisce FSE, come "l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario, generati da eventi clinici, anche a carattere amministrativo, riguardanti l'assistito (…)".

[136] AA.VV, Data protection e privacy, cit., p. 326 ss.

riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato"[137].

Poiché sull'analisi dell'articolo 9, e in particolar delle deroghe al divieto di trattamento dei dati relativi alla salute, nonché più in generale sul tema del consenso ci siamo già soffermati[138], è opportuno ora analizzare brevemente il ruolo della trasparenza e l'informativa degli interessati.

In merito all'informativa dell'interessato, il Garante ha evidenziato come il Regolamento (UE) 2016/679 non segni una rottura con il passato, ma tutt'al più rafforzi i principi preesistenti in tema di trasparenza. La trasparenza, come ben sappiamo, costituisce un principio fondamentale nel trattamento dei dati personali, e consiste nella necessità di rendere gli interessati pienamente consapevoli del trattamento a cui sono sottoposti i propri dati[139]. Per questo motivo le informazioni devono essere fornite in modo trasparente, intellegibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro**,** agevolmente comprensibile dal pubblico di riferimento. Il GDPR responsabilizza il titolare del trattamento nell'assicurare il rispetto di tali requisiti, conferendogli la facoltà di operare con le modalità che ritiene più efficaci per un corretto adempimento di tale obbligo, considerando sempre il contesto e le specifiche modalità di trattamento. Al riguardo andranno valutati elementi come il dispositivo utilizzato per fornire l'informativa, la natura dell'interazione tra interessato e titolare, nonché eventuali limitazioni tecniche o operative, i quali sono in grado di incidere sulla chiarezza e l'accessibilità delle informazioni.

A tal proposito, il Garante ha indicato specifiche informazioni che devono essere fornite dai titolari del trattamento operanti nel settore sanitario, in particolare con riferimento alle aziende sanitarie, ossia quelle realtà che presentano una pluralità di trattamenti complessi. In questi casi l'Autorità ha suggerito di adottare un approccio informativo progressivo, il cui fine ultimo è quello di riuscire a bilanciare l'obbligo di trasparenza con l'effettiva comprensibilità da parte dell'interessato[140].

---

[137] Coppola, "Protezione dei dati sanitari, tutti i paletti del Garante Privacy", cit.
[138] Sul punto si rinvia al cap. 3, par. precedente
[139] Come previsto dall'articolo 5 del GDPR, che stabilisce i principi applicabili al trattamento dei dati personali, ossia liceità, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, e infine integrità e riservatezza
[140] Coppola, "Protezione dei dati sanitari, tutti i paletti del Garante Privacy", cit

In base a quanto appena stabilito, le strutture sanitarie, ai sensi dell'articolo 79 del Codice della Privacy, possono inizialmente offrire alla generalità dei pazienti un'informativa limitata ai soli trattamenti strettamente connessi all'ordinaria attività di erogazione delle prestazioni sanitarie**.** Nel caso in cui, invece, ci si trovi in presenza di trattamenti ulteriori, tra cui per esempio la fornitura di presidi sanitari**,** le modalità di rilascio telematico dei referti**,** oppure le attività connesse a finalità **di** ricerca scientifica, la relativa informativa allora potrà essere data anche in un secondo momento, ma solo ai pazienti effettivamente coinvolti in tali specifici trattamenti**.** Tale modalità è stata prevista in risposta all'esigenza di arginare il fenomeno di sovraccarico informativo, garantendo allo stesso tempo maggior consapevolezza da parte dl paziente circa le informazioni effettivamente rilevanti per il trattamento ei propri dati personali.

Tra le novità introdotte dal Regolamento in tema di trasparenza, il Garante ha messo in luce **c**he, rispetto a quanto previsto dall'art. 13 del previgente Codice Privacy, il nuovo impianto normativo permette al titolare del trattamento di indicare il periodo di conservazione dei dati personali anche tramite la descrizione dei criteri utilizzati per determinarlo.**[141]**

In particolare, facendo riferimento alla documentazione sanitaria. L'autorità garante della privacy evidenzia come i tempi di conservazione previsti dalla normativa italiana non sono stati alterati con l'avvento del GDPR, anzì rimangono pienamente efficaci. Per fare qualche esempio la documentazione relativa agli accertamenti effettuati per il rilascio dei certificati di idoneità agonistica deve essere conservata per un periodo di almeno cinque anni, come stabilito nell'articolo 5 D.M. 18/02/1982[142]. Ulteriormente, possiamo far riferimento alle cartelle cliniche, le quali devono essere conservate per un periodo illimitato, in linea con quanto stabilito dalla Circolare del Ministero della Sanità n. 900 del 19 dicembre 1986[143]; o ancora le immagini relative alla documentazione radiologica

[141] Conformemente a quanto disposto dagli artt. 13 e 14, sempre par. 2 lett. a) del GDPR

[142] Decreto del Ministero della Sanità 18 febbraio 1982 Norme per la tutela sanitaria dell'attività sportiva agonistica (Pubbl. sulla Gazzetta Ufficiale del 5 marzo 1982, n. 63)

[143] circolare del Ministero della Sanità (n.900 2/AG454/260), emanata il 19 dicembre 1986 stabilisce che "le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico-sanitario".

devono essere conservate per un periodo non inferiore a dieci anni, secondo quanto previsto all'articolo 4 del D. M del 14 febbraio del 1997[144].

In definitiva, tali disposizioni normative coesistono con il GDPR, che non avendo modificato le norme di conservazione già in vigore garantisce la continuità nella gestione dei dati sanitari.

Nel caso in cui non siano previsti in alcuna disposizione normativa specifici tempi di conservazione per determinati documenti, il GDPR stabilisce il principio di limitazione della conservazione, in base al quale "i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;"*[145]*

Il Regolamento sancisce espressamente che la nomina di una Responsabile della protezione dei dati, comunemente noto con l'acronimo inglese DPO è obbligatoria in determinati casi. Più specificatamente l'articolo 37 del GDPR stabilisce l'obbligatorietà della nomina per autorità e organismi pubblici, aziende e organizzazioni private, per le quali scatta l'obbligo solo se l'attività primaria dell'azienda consiste in un monitoraggio regolare e sistematico degli interessati su larga scale, e infine per le aziende che trattano dati sensibili, ma solo se l'attività principale consiste nel trattamento di particolari categorie di dati, come dati biometrici o genetici, effettuato su larga scala.

Alla luce di quanto affermato, risulta evidente che un'azienda sanitaria pubblica, appartenente al Servizio Sanitario Nazionale (SSN), deve obbligatoriamente procedere alla nomina di un DPO, sia in quanto organismo pubblico, sia poiché tratta dati relativi alla salute su larga scala.

Inoltre, anche le strutture sanitarie private, tra cui ospedali, case di curo o residenze sanitarie assistenziali (RSA), devono sottostare a questo obbligo, poiché si ritiene che effettuino trattamenti di dati sanitari su larga scala, come confermato anche dalla line guida del Comitato Europeo per la protezione dei dati.

Pertanto, si potrebbe affermare che in tutti gli altri casi, non esplicitamente menzionati nell'articolo 37 del GDPR, la nomina di un responsabile del trattamento, rimane facoltativa, ma consigliata.

---

[144] Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del D.Lgs. 17 marzo 1995, n. 230. (Pubblicato nella Gazz. Uff. 11 marzo 1997, n. 58)

[145] Art. 5, par.1, lett e) del GDPR

Per aiutare i responsabili e i titolari del trattamento a comprendere, e di conseguenza a dare corretta attuazione, agli obblighi previsti dal GDPR, il Garante per la privacy ha pubblicato delle FAQ (frequently asked question), conformemente a quanto stabilito nelle linee guida del Gruppo Articolo 29 (WP243). Nello specifico, nell'ambito del settore privato, le FAQ precisano che la nomina di un DPO è obbligatoria per entità come: ospedali privati, terme, centri di riabilitazione, laboratori di analisi mediche. Tale obbligo si applica quando queste entità rientrano nei criteri previsti dal sopracitato articolo 37, in quanto effettuano trattamenti di dati personali su vasta scala, soprattutto quelli relativi alla salute[146].

Pertanto, nell'ambito della protezione dei dati personali, e di quelli sanitari in particolare, il DPO viene visto come una figura fondamentale al fine di garantire una corretta applicazione delle norme vigenti in materia. Infine, occorre sottolineare che un DPO può essere designato per più strutture sanitarie, ma decidere l'alternativa migliore spetta sempre al titolare del trattamento.

Il Regolamento e le successive linee guida emanate dal Garante si preoccupano di sottolineare che il singolo professionista sanitario che opera individualmente non è obbligato alla nomina di un DPO.

Tale esenzione si basa sul Considerando n. 91 che specifica l'interpretazione corretta del concetto di trattamento "su larga scala", ove si afferma esplicitamente che il trattamento dei dati di pazienti da parte di un singolo medico o operatore sanitario non dovrebbe essere considerato come un trattamento su larga scala, conformemente a quanto stabilito nelle linee guida del Gruppo Articolo 29.

A tal punto, per fini di chiarezza espositiva, occorre fare un breve cenno anche alle altre attività sanitarie, quali farmacie, parafarmacie e aziende ortopediche. Anche in questi casi, la nomina di un DPO non viene considerata obbligatoria, salvo che si tratti di trattamenti effettuati su larga scala, analogamente a quanto appena visto.

Da ultimo occorre soffermarci sulla disciplina che regola il Registro delle Attività di Trattamento. Trattasi di un documento fondamentale per qualsiasi organizzazione che gestisce i dati personali, previsto dall'articolo 30 del GDPR, serve a tracciare dettagliatamente le operazioni effettuate nell'ambito del procedimento di trattamento dei

[146] Coppola, "Protezione dei dati sanitari, tutti i paletti del Garante Privacy", cit

dati. Tale registro fornisce un quadro costantemente aggiornato su tutti i trattamenti di dati all'interno di un'organizzazione, e costituisce uno dei punti chiave del principio di accountability, di cui abbiamo ampiamente detto in precedenza. Per quanto riguarda la forma, deve essere scritta, anche in via elettronica, e deve essere esibito su richiesta del Garante. Inoltre, secondo quanto stabilito dall'articolo 30 del Regolamento, sono tenuti a redigere siffatto registro le imprese e organizzazioni con almeno 250 dipendenti, nonché qualsiasi titolare o responsabile che, pur avendo meno di 250 dipendenti, effettui trattamenti che possono comportare rischi per le libertà e i diritti degli individui, o che tratti dati in modo non occasionale, o ancora che effettui trattamenti relativi a particolari categorie di dati, quali per esempio dati biometrici, genetici o relativi alla salute, o relativi a condanne penali.

Per quanto riguarda il settore sanitario, invece, l'obbligo di redigere il suddetto registro sussiste sempre, poiché i trattamenti effettuati in tale ambito includono necessariamente categorie di dati particolari, come quelli relativi alla salute[147]. In tal caso, l'obbligo di redigere il registro delle attività di trattamento grava sui singoli professionisti sanitari che operano come liberi professionisti, sui medici di medicina generale e pediatri, sugli ospedali privati, case di cura e RSA, sulle aziende sanitarie pubbliche (facenti parte del SNN), nonché sulle farmacie, parafarmacie e aziende ortopediche.

In conclusione, il diritto di accesso ai dati sanitari, è un aspetto fondamentale della tutela della privacy, che vede coesistere le disposizioni del GDPR con le specifiche normative nazionali. La gestione e il trattamento di questi dati di natura sensibile richiede l'adozione di misure proattive, come il registro delle attività di trattamento, oltre che il rispetto della normativa vigente in materia. Un ulteriore misura di garanzia è rappresentata dalla nomina di un DPO, che sebbene non sia sempre richiesta obbligatoriamente per i singoli professionisti, è essenziale per le organizzazioni che trattano dati su larga scala, assicurando conformità con il principio di trasparenza.

3.2 Il diritto di accesso ai dati sanitari: soggetti e modalità

Nel nostro ordinamento, i principi e gli istituti del diritto amministrativo, come la trasparenza e il diritto di accesso, svolgono un ruolo fondamentale nella tutela della salute

[147] A tal proposito si rinvia all'articolo 9 par.1 del GDPR

e dei dati sanitari dei cittadini. Difatti, in un ordinamento democratico come il nostro, le amministrazioni pubbliche, e di conseguenza anche le strutture sanitarie, sono tenute ad agire in modo trasparente. Questo principio cardine del nostro ordinamento consente ai cittadini di controllare l'operato delle pubbliche amministrazioni, garantendo i loro diritti e migliorando l'interazione con la pubblica amministrazione.

Pertanto, è evidente come i dati e le informazioni detenuti dalle strutture sanitarie assumano un ruolo determinate sia perché strettamente connessi con interessi di primaria importanza, sia perché spesso sono contenuti all'interno dei cd. strumenti della sanità digitale (ovvero la Cartella Clinica Elettronica, il Dossier Sanitario Elettronico e il Fascicolo Sanitario Elettronico), che di fatto costituiscono documenti ammnistrativi di natura informatica[148].

Conseguentemente, le modalità di esercizio del diritto di accesso nel settore sanitario seguono una disciplina particolare, data anche dalla rilevanza che assume il bene salute relativamente a tutte le attività del servizio sanitario nazionale[149]. Proprio per tale ragione, l principio di trasparenza e il diritto di accesso diventano strumenti di tutela essenziali per i pazienti.

Il legislatore ha recentemente affrontato il diritto di accesso alla documentazione sanitaria in un'ottica del tutto nuova. Nel corso degli ultimi anni, le richieste di accesso a dati e documenti sono notevolmente aumentate, spinte da diverse motivazioni. Ad oggi le richieste di accesso si sono moltiplicate, e non riguardano più solo il proprio fascicolo medico, ma spesso perseguono la finalità di indagare circa la correttezza delle cure, per esempio chiedendo di accedere a verbali dei comitati di valutazione dei rischi, ossia comitati interni che valutano i sinistri stradali[150]. Oltretutto ulteriori richieste possono riguardare documenti sanitari di persone decedute, o anche, lo stato di salute dei terzi.

Tuttavia, è importante notare come il diritto di accesso in ambito sanitario conservi una sua peculiarità. Diversamente dal contesto amministrativo tradizionale, ove la richiesta riguarda atti di un procedimento formale, in ambito sanitario la richiesta di accesso si

[148] Rampulla F. C., Ricciardi G. C., Venturi A., *Digitalizzazione delle amministrazioni e accesso a dati e documenti informatici sanitari*, 24 Gennaio 2024, pp. 133 e ss., in www.federalismi.it

[149] Ceresetti G., *Diritto di accesso e atti elle autorità sanitarie, p. 267 ss, in* https://www.ildirittodelleconomia.it/wp-content/uploads/2022/03/12Ceresetti.pdf

[150] Si tratta di collegi indipendenti, che si riuniscono periodicamente e che vengono regolamentati sulla base della singola normativa regionale. Il CVS (Comitato Valutazione Sinistri), a seconda della situazione è composto da professionisti diversi sia esterni, sia interni, in www.legalinsurance.it

riferisce a dati generati durante l'attività di erogazione delle cure, che nella maggior parte dei casi non ha un carattere provvedimentale.

A tal punto, è importante notare che per gestire efficacemente le richieste di accesso relative a dati e documenti sanitari, è necessario bilanciare la trasparenza con la tutela della privacy.

In prima battuta, ci si basava sulle norme generali in materia di accesso documentale e civico[151], successivamente con l'entrata in vigore della Legge Gelli - Bianco (l. 24/2017)[152] si fornisce un quadro normativo più dettagliato. L'articolo 4 di questa legge stabilisce che Le prestazioni sanitarie erogate dalle strutture pubbliche e private sono soggette all'obbligo di trasparenza, nel rispetto del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Di conseguenza, emerge una sfida fondamentale: garantire l'accessibilità dei dati, rispettando al tempo stesso la riservatezza di informazioni particolarmente sensibili, che potrebbero portare all'identificazione di un paziente o a rivelare dettagli persoali che richiedono una particolare protezione.

Poi l'articolo 4 , secondo comma, introduce un termine per la consegna della documentazione sanitaria, molto più breve rispetto a quello previsto dalla l. 241 del 1990, pari a sette giorni. La ragione sottostante questa abbreviazione risiede nella necessità di tutelare I pazienti, che spesso hanno bisogno dei doumenti in tempi celeri, ad esempio per avviare un'azione legale per responsabilità professionale. Tuttavia, lo stesso testo normativo riconosce che il termine di sette giorni può essere impraticabile per le strutture sanitarie, vista la mole di lavoro, e pertanto precisa ache le eventuali integrazioni documentali dovranno essere effettuate entro un massimo di 30 giorni. Quest'ultimo termine diviene il riferimneto per definire il "silenzio" dell'ammnistrazione, che può essere impugnato[153].

Un ulteriore obbligo di trasparenza viene poi introdotto dal terzo comma dello stesso articolo, secondo il quale le struttue sanitarie sono tenute a pubblicare I dati sui risarcimenti ergate negli ultimi cinque anni, permettendo così ai cittadini di consulatre le informazioni

[151] Sul punto si rinvia al cap. 1, par 1.2.1

[152] Recante "Disposizioni in materia di sicurezza delle cure e della persona assistita, nonchè in materia di responsabilità professionale degli esercenti le professioni

[153] Ceresetti G., Diritto di accesso e atti delle autorità sanitarie, op. cit., p, 267 ss.

relative alla responsabilità professionale e al risk menagment, senza doverne fare richiesta[154].

In sostanza, i commi 2 e 3 della legge Gelli-Bianco, mettono in luce le questioni principali dell'accesso in ambito sanitario, ossia la necessità di un'azione rapida per la consultazione dei doumenti sanitari e l'obbligo di pubblicare i dati per la gestione del rischio. Tali principi confermano quanto detto precedentemente sulla peculiarità del diritto di accesso in ambito sanitario, che da sempre cerca di bilanciare l'accessibilità dei dati con la tutela della riservatezza[155].

Per quanto riguarda l'esercizio del diritto di accesso occore distinguere due ipotesi: accesso alla propria documentazione sanitaria e accesso al documentazione sanitarie di terzi.

Un ulteriore casistica, meritevole di una approfondita analisi, si manifesta quando l'istanza di accesso documentale ha per oggetto la documentazione sanitaria di soggetti terzi, poichè in tale contesto si solleva la necessità di ponderazione tra diritti contrapposti. In questo contesto, assume una posizione preminente il limite della riservatezza, che tutela l'interesse privatistico del soggetto cui i dati sanitari si riferiscono, il quale viene definito in questo caso come controinteressato, e si tratta di colui che generalmente vede la sua sfera personale potenzialmente vulnerata dall'ostensione dei dati sensibili.

ll bilanciamento tra il diritto di accesso, espressione del principio di trasparenza, e la tutela della riservatezza del controinteressato non è demandato unicamente a una disciplina normativa prestabilita, sebbene fonti primarie e secondarie forniscano il quadro di riferimento. Difatti spesso nella prassi si riscontra che il compito di dirimere il conflitto viene affidato alla discrezionalità dell'amministrazione sanitaria, la quale è tenuta ad effettuare un'attenta analisi per valutare la legittimità dell'istanza in relazione all'interesse alla riservatezza, al fine di garantire che l'accesso sia concesso solo in presenza di un interesse giuridicamente tutelato e prevalente rispetto alla tutela dei dati personali.

[154] Pierfrancesco Porto, Il principio di trasparenza e il diritto di accesso in ambito sanitario, in "Ratio Iuris" (ISSN 2420-7888),2025, p. 5 ss

[155] ibidem

A tal fine, è importante richiamare l'articolo 24, comma 7 della legge 241 del 1990[156], il quale opera un rinvio esplicito alle disposizioni del Codice della privacy, per le ipotesi in cui la richiesta di accesso abbia ad oggetto *"dati idonei a rivelare lo stato di salute o la vita sessuale".*

In particolare, si stabilisce un parametro rigoroso per le valutazioni dell'istanze di accesso: l'ostensione è consentita unicamente se la situazione giuridica soggettiva, che il richiedente intende tutelare con la richiesta, sia di rango almeno pari al diritto alla riservatezza del controinteressato. Il che significa che tale condizione non si concretizza in un mero bilanciamento formale, ma richiede al contempo che il diritto dell'istante rappresenti un diritto della personalità o in un'altra libertà fondamentale. Da ciò si può agevolmente dedure, che l'ammissibilità dell'istanza di accesso ai dati sanitari di terzi è subordinata alla dimostrazione che la loro conoscenza sia strettamente necessaria per la difesa di una posizione giuridica meritevole di tutela e di pari dignità costituzionale rispetto al diritto alla riservatezza del soggetto cui i dati si riferiscono. Tale principio richiede che venga effettuato un bilanciamento di interessi contrapposti, affidando all'amministrazione la ponderazione specifica delle circostanze, caso per caso, al fine di stabilire l'interesse di volta in volta preminente[157].

Un ulteriore caso di accesso alla documentazione sanitaria di terzi si verifica quando l'istanza di accesso riguarda i dati sanitari di una persona deceduta. In tal caso la situazione è semplificata, poiché il diritto alla riservatezza si estingue con la morte del titolare, non è necessario bilanciare interessi contrapposti[158]. Tutt'al più, l'amministrazione dovrà semplicemente verificare se il richiedente sia titolare di un diritto legittimo o una situazione giuridica che giustifichi la richiesta dei documenti, ovvero che l'accesso sia funzionale alla salvaguardia dei propri interessi.

In aggiunta, un altro caso di accesso ai dati sanitari di terzi è previsto all'articolo 12, comma 4, della legge Gelli - Bianco, cui abbiamo accennato poc'anzi. Questa norma trova applicazione quando è in corso un'azione legale da parte di un paziente contro la compagnia assicurativa, e sancisce espressamente che *"(...) l'impresa di assicurazione,*

---

[156]L 'art. 24 comma 7 della l. 241/1990 prescrive che: *"Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale*

[157] Pierfrancesco Porto, Il principio di trasparenza e il diritto di accesso in ambito sanitario, cit. p. 5 ss

[158] ibidem

l'esercente la professione sanitaria e il danneggiato hanno diritto di accesso alla documentazione della struttura relativa ai fatti dedotti in ogni fase della trattazione del sinistro." Questo significa che in tale contesto il diritto di accesso alla documentazione sanitaria viene concesso non solo al danneggiato (il paziente), ma anche all'impresa di assicurazione e all'esercente la professione sanitaria coinvolto. Lo scopo della stessa disposizione è quello di assicurare a tutte le parti in causa di aver accesso a ogni elemento utile per tutelare la propria posizione in giudizio, secondo il principio della parità processuale.

Inoltre, vi è una disposizione specifica della legge Gelli-Bianco, l'articolo 16, che limita l'accesso ai documenti relativi al risk menagment in ambito sanitario. Tale articolo chiarisce che i verbali e gli atti relativi all'attività di gestione del rischio clinico non possono essere acquisiti o utilizzati in procedimenti giudiziari, creando conseguentemente una preclusione esplicita all'accesso a questa documentazione[159]. Quando si parla di risk menagement si fa riferimento a un processo interno alle strutture sanitarie, finalizzato ad identificare, valutare e prevenire eventi avversi che potrebbero arrecare danno ai pazienti, cercando di sviluppare adeguate misure correttive[160].

La ratio di questa disposizione si può rinvenire nel fatto che si vuole impedire che le analisi interne, le valutazioni relative alle criticità e le strategie correttive messe in atto dalle amministrazioni sanitarie vengano eventualmente usate contro di loro in una disputa legate.

In questo modo, il legislatore vuole incentivare le strutture sanitarie a svolgere attività di prevenzione in modo trasparente, senza il timore che le loro strategie di miglioramento possano ritorcersi contro di loro in tribunale.

Sulla base di questa analisi, è evidente che l'accesso ai dati e documenti sanitari non è solo un modo per conoscere le proprie condizioni di salute o quelle degli altri, ma ha un ruolo chiave nel garantire una maggiore trasparenza nell'erogazione di servizi[161].

Inoltre, la possibilità offerta ai cittadini di accedere a questi dati consente loro di esercitare il diritto alla salute in modo più consapevole, e al contempo rafforza il rapporto di fiducia

[159] V. sul punto Cons. Stato, Sez. III, 23 gennaio 2020, n. 808, in Foro.it., 2020, 4, 3, 202 ss.

[160] Ceresetti G., op. cit., pp. 275 e ss.

[161] Pierfrancesco Porto, Il principio di trasparenza e il diritto di accesso in ambito sanitario, cit. p. 5 ss

tra pazienti e strutture sanitarie, contribuendo a creare un sistema sanitario più efficiente e partecipato.

In definitiva, le varie forme di accesso appena analizzate, anche limitate al settore sanitario, concorrono a rafforzare i principi di trasparenza, partecipazione democratica e buona amministrazione, che guidano l'attività ammnistrativa. Difatti la trasparenza ricopre un ruolo cruciale e si rivela fondamentale su due fronti distinti e complementari. Da un lato, essa rappresenta un motore di efficienza per la pubblica amministrazione, spingendola a un'evoluzione radicale: il passaggio da un modello gestionale basato su processi analogici e documentazione cartacea a uno completamente digitale.

Dall'altro lato, e con un impatto ancora più significativo, una gestione trasparente e digitalizzata è lo strumento chiave per garantire in modo più solido ed efficace i diritti sociali dei cittadini. Questo vale in particolare per settori essenziali come la sanità, l'istruzione e il welfare, dove la chiarezza e la disponibilità delle informazioni sono indispensabili per tutelare i diritti individuali e costruire un rapporto di fiducia tra l'amministrazione e i suoi utenti.

3.2.1 La sanità digitale: Fascicolo sanitario elettronico, Dossier sanitario e telemedicina

Nel contesto di una sempre più rapida digitalizzazione del settore sanitario, l'e-health si afferma come un insieme di tecnologie innovative atte a migliorare l'efficienza, l'accessibilità e la sostenibilità del sistema. Tuttavia, la sua diffusione ha reso necessario l'adeguamento normativo, prestando particolare attenzione alla tutela della privacy e alla protezione dei dati sensibili.

Di seguito esamineremo i principali strumenti e le relative normative che regolano l'uso della tecnologia sanitaria.

Per e-health, o "Sanità in Rete" si intende l'impiego delle tecnologie dell'informazione della comunicazione in diversi ambiti del settore sanitario, dalla prevenzione alla diagnosi, dal trattamento al monitoraggio. Tali tecnologie realizzano un sistema basato sull'individuo, cercando di migliorare l'accesso alle cure e contribuendo a una maggiore efficienza e sostenibilità del settore sanitario. Il minimo comun denominatore per tutte le iniziative e-health sorte negli ultimi anni è la dematerializzazione dei documenti sanitari.

Di seguito analizzeremo le principali aree ove si sviluppano le tecnologie e-health: telemedicina, l'informazione sanitaria online, cartella clinica elettronica, digital well being, ossia tecnologie dedicate al benessere personale e alle prevenzione, nonché m-health, che consiste nell'utilizzo di dispositivi mobili, portatili e indossabili per il monitoraggio della salute, e infine la robotica medica e protesica avanzata, che consiste nell'applicazione della robotica in ambito chirurgico e protesico[162]. Logicamente è assolutamente necessario che la grande quantità di dati relativi alla salute derivante dall'impiego di queste tecnologie avanzate debba essere tratta con il massimo rispetto per la privacy dei pazienti in conformità con gli obblighi previsti dal GDPR.

Il Fascicolo Sanitario Eletttronico (FSE) è "l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito"[163].

Generalmente, viene istituito e gestito dalle Regioni e ha come fine ultimo quello di fornire un quadro clinico del paziente completo ed esaustivo, tenendo costantemente aggiornati i dati generati da diversi professionisti e strutture sanitarie. Oltretutto, al cittadino è anche riservata la facoltà di accedere ai servizi sanitari online tramite il proprio FSE.

Il Fascicolo Sanitario elettronico è formato da un nucleo minimo di dati e documenti, che ne costituiscono la base, ricomprendendo dati identificativi e ammnistrativi del paziente, i referti di esami e visite, i verbali di pronto soccorso, nonché le lettere di dismissione dai ricoveri. A questi si aggiungano il profilo sanitario sintetico (o anche detto Patient Summary), che riassume le informazioni cliniche essenziali, il dossier farmaceutico con la storia dei farmaci prescritti, e per concludere il consenso o il diniego per la donazione i organi o tessuti.

In aggiunto al nucleo minimo, il FSE può essere ulteriormente arricchito con dati e documenti integrativi, quali prenotazioni, prescrizioni, cartelle cliniche complete e vaccinazioni, la cui inclusione è strettamente connessa alle scelte regionali e dal livello di digitalizzazione.

[162] AA.VV, Data protection e privacy, cit., p.328 ss.

[163] Come stabilito nell'art. 12, comma 1, D.L. n. 179/2012 recante "ulteriori misure urgenti per la crescita del paese" convertito con modificazioni dalla L. 17 dicembre 2012, n. 221

In aggiunta, il d.l. n. 34 del 2020[164] ha esteso i contenuti del FSE, ricomprendendo al suo interno anche le informazioni relative alle prestazioni sanitarie erogate al di fuori del Servizio Sanitario Nazionale.

Si sottolinea che i trattamenti di dati effettuati tramite FSE servono per scopi di prevenzione, diagnosi, cura e riabilitazione. Inoltre, tra le modifiche introdotte dal decreto-legge n. 34 del 2020 sopra citato, è venuto meno l'obbligo del consenso dell'assistito per l'istituzione e l'alimentazione del FSE previsto dalla precedente normativa [165]. Sulla base di ciò, il fascicolo viene oggi aggiornato automaticamente dalle strutture sanitarie o dai singoli professionisti competenti. Tuttavia, l'interessato conserva il diritto di limitare l'accesso ai propri dati, rendendoli disponibili solo al personale sanitario che lo ha in cura[166].

È importante sottolineare che l'alimentazione e l'aggiornamento del FSE avvengono automaticamente, senza necessità del consenso dell'assistito, caso diverso è invece il consenso alla consultazione. Difatti, il paziente ha il pieno diritto di esprimere il consenso alla consultazione, che consente agli operatori sanitaria (pubblici e privati) di visionare dati, come ricoveri, referti e farmaci prescritti. Pertanto, si potrebbe affermare che il paziente mantiene pienamente il controllo su chi può accedere al proprio FSE.

È importante specificare che gli organi di governo possono consultare il FSE, ma solo per finalità di programmazione sanitaria o di ricerca e comunque solo in forma anonimizzata ed in conformità con il principio di minimizzazione dei dati.

Oltretutto, l'interessato ha anche la facoltà di richiedere l'oscuramento di determinati dati o documenti sanitari. In tal caso le informazioni non saranno visibili agli operatori sanitari, se non ai professionisti che le hanno generate, salvo revoca espressa del paziente, che può essere disposta in qualsiasi momento.

Per concludere, come accennato in precedenza, occorre ribadire che i trattamenti di dati effettuati tramite FSE sono strettamente regolamentati. Difatti, i dati possono essere impiegati solo con fini di prevenzione, diagnosi, cure e riabilitazione. Inoltre, è evidente

164 Recante "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonchè di politiche sociali connesse all'emergenza epidemiologica da COVID-19."

165 Art. 12 del D.L. 179/2012 2012 recante "ulteriori misure urgenti per la crescita del paese"

166 166AA.VV, Data protection e privacy, cit., p.328 ss

che l'accesso sia limitato solo ai soggetti operanti nel settore sanitario, escludendo figure come periti, compagnie di assicurazione o datori di lavoro.

Con riferimento al Dossier Sanitario Elettronico[167], il Garante della privacy ha generato, grazie le sue linee guida, un quadro normativo chiaro e completo dello stesso. Esso consiste in uno strumento tenuto da una singola struttura al fine di raccogliere le informazioni cliniche di un paziente. L'obbiettivo primario di questo dossier è quello di documentare la storia clinica di un paziente all'interno di un un'unica realtà, differentemente dal FSE che aggrega tutt'al più dati provenienti da diverse fonti e professionisti.

In aggiunta, la sicurezza dei dati contenuti nel dossier sanitario è essenziale e deve rispettare i principi previsti agli articoli 25[168] e 32[169] del GDPR, assicurando la massima tutela per le informazioni personali e i dati sensibili dei pazienti.

Senza dubbio il dossier sanitario si contraddistingiue anche rispetto ad altri documenti, quali per esempio la cartella clinica, le schede del medico di base o quelle di uno specialista. In questi casi la differenza principale può essere rinvenuta nel titolare del trattamento: mentre il dossier è gestito da un'unica struttura sanitaria che aggrega le informazioni provenienti dai vari professionisti che vi operano, invece gli altri documenti clinici, cui abbiamo appena accennato, sono gestiti da un singolo professionista.

In proposito, occorre precisare che, qualora le informazioni provenienti da più professionisti vengano aggregate, si avrà un FSE, se i professionisti agiscono come titolari autonomi del trattamento, viceversa un dossier sanitario, se i professionisti agiscono all'interno della stessa struttura che diviene l'unico titolare.

---

[167] Vedi anche Garante per la protezione dei dati personali, Linee guida in materia di Dossier sanitario del 4 giugno 2015, consultabile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4084632

[168] Il quale stabilisce che "(..) *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*"

[169] Il quale stabilisce che "(..) 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, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

È importante notare che, come visto per il FSE, anche la creazione di un dossier sanitario richiede un'informativa specifica, che deve contenere tutti gli elementi indicati all'articolo 13 del GDPR[170]. Dal momento che l'utilizzo del dossier da parte del professionista rappresenta un trattamento ulteriore dei dati, si tratta un accesso più esteso alle informazioni relative al paziente, e di conseguenza si rende necessario informare il paziente in modo chiaro e specifico circa le modalità con cui è effettuato il trattamento dei suoi dati. Difatti, in assenza del dossier il professionista avrebbe accesso solo alle informazioni fornite dal paziente in quel momento, mentre con il dossier può visionare anche i dati sanitari precedentemente acquisiti nella struttura, anche in reparti diversi dal suo e relativi a patologie differenti.

In definitiva, l'accesso al dossier sanitario deve essere necessariamente limitato al personale sanitario direttamente coinvolto nella cura del paziente. Questo significa che devono ritenersi inclusi medici, infermieri e chiunque altro partecipi alla terapia, come nel caso di ricovero, o di una procedura complessa come il trapianto, che vedono coinvolti molteplici specialisti. Tale principio di minimizzazione acquisisce particolare rilevanza.

Al fine di garantire questo livello di controllo, le strutture sanitarie sono tenute ad adottare specifici sistemi di autenticazione, adattabili ai diversi casi di accesso. Il titolare del trattamento è tenuto a valutare di volta in volta quali dati siano necessari per ciascun profilo professionale, limitando l'accesso alle sole informazioni ritenute indispensabili[171].

Il suddetto principio di minimizzazione ricopre particolare importanza quando l'accesso al dossier viene consentito anche al personale con funzioni amministrative, al fine di evitare che quest'ultimo consulti dati clinici non indispensabili per lo svolgimento delle sue mansioni.

A questo punto, sembra opportuno fare quantomeno un breve cenno alla telemedicina, ossia una modalità di erogazione di servizi sanitari caratterizzata dall'utilizzo di

[170] Il quale stabilisce le informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, ossia "(…) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale (…)"

[171] AA.VV, Data protection e privacy, cit., p.328 ss

tecnologie dell'informazione e della comunicazione (ICT) al fine di collegare pazienti e professionisti in ambito sanitario quando non si trovano materialmente nello stesso luogo fisico. Tale sistema consente la trasmissione sicura di dati medici, esso è stato ideato con lo scopo di supportare la prevenzione, la diagnosi, la cura e il monitoraggio dei pazienti. È importante sottolineare che la telemedicina non sostituisce il tradizionale rapporto medico-paziente, ma lo integra migliorandone l'efficacia.

A livello nazionale il rifermento normativo sono le "Linee guida per i servizi di tele-medicina– requisiti funzionali e livelli di servizio " [172] pubblicate sulla Gazzetta Ufficiale il 2 novembre 2022, il cui scopo è quello di supportare Regioni e Provincie Autonome nella definizione e nella gestione di inziative relative ai servizi di telemedicina.

Generalmente i servizi di telemedicina sono suddivisi in tre macro-aree: telemedicina specialistica, telesalute e teleassistenza. La prima macro categoria comprede servizi come la televisita (visita a distanza), il teleconsulto (consulto tra medici a distanza) e la tele-cooperazione sanitaria. Con la seconda, invece, ci si riferisce ad un ambito più ampio che include al su interno attività di promozione e educazione alla salute. Infine la terza, la teleassistenza riguarda il monitoraggio e il supporto a disatnza dei pazienti.[173]

Le linee guida del Garante della privacy del 19 novembre 2009[174] disciplinano l'erogazioni di referti online, che consentono ai pazienti di accedere a un referto clinico in formato digitale.

Sulla base di quando espressamnte previsto nelle suddette line guida i referti possono essere

inviati tramite posta elettronica o scaricati dal sito web ufficiale della struttura sanitaria. Al fine di garantire la sicurezza di tali documenti, l'invio del referto tramite l'online richiede che questo sia un allegato protetto da una password e che l'indirizzo mail sia

[172] Il documento è stato redatto in coerenza con quanto previsto dal Decreto Ministeriale 23 maggio 2022 n. 77 *"Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*", dal Decreto Ministeriale 29 aprile 2022 "*Approvazione delle linee guida organizzative contenenti il «Modello digitale per l'attuazione dell'assistenza domiciliare*", consulatbile in https://img.healthtech360.it/wp-content/uploads/2022/11/Linee-di-Indirizzo-Servizi-Telemedicina-2022.pdf

[173] T. Casadei, S. Pietropaoli, Diritto e tecnologie informatiche, cit.. p. 69 e ss.

[174] pubblicato, unitamente alla medesima deliberazione, sul sito web dell´Autorità e sulla Gazzetta Ufficiale n. 162 del 15 luglio 2009, consultabile in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1679033

convalidato per evitare l'invio a destinatari indesiderati. L'acceso tramite sito web, invece, prevede l'utilizzo di protocolli sicuri (HTTPS), l'autenticazione tramite credenziali, e infine la previsione di un limite massimo per il tempo di consultazione, pari a 30 giorni. Al contempo deve essere confertita ai pazienti la possibilità di cancellare i propri referti dal sistema in qualsiasi momento.

In ogni caso, la struttura è tenuta a fornire al paziente un'adeguata informative e ottenere un consenso specifico, garantendo sempre la possibilità di ritirare il reperto in formato cartaceo. Queste misure di sicurezza devono grantire la protezione dei dati personali ed essere proporzionate al rischio, come previsto dall'articolo 32 del GDPR.

Al fine di assicurare un corretta erogazione dei servizi di refertazione online è necessario impletare una serie di adempimenti aggiuntivi a tutela dei dati personali. Difatti, le strutture sanitarie sono tenute a garntire sistemi di autenticazione e autorizzazione che limitino l'accesso ai dati in base ai ruoli degli incaricati e alle esiegnze di accesso al trattameneto, e sono tenute ad asssicurare altresì la separazione fisica o logica dei dati particolari (come quelli relative alla salute) da quelli amministrativi[175].

In aggiunta, il titolare del trattamento deve studiare procedure adeguate per intervenire tempestivamente in caso d'emergenza, ad esmepio bloccando l'accesso o l'invio dei referti se un paziente segnala il furto delle proprie credenziali. Prima di porcedere all'erogazione del servizio è obbligatorio effettuare una valutazione d'impatto sulla portezione dei dati (DPIA)[176], secondo quando prevesto dal GDPR[177]. Qualora il servizio venisse affidato a una società esterna, questa deve formalmente essere nominata responsabile del trattamneto dei dati, ai sensi dell'articolo 28 del GDPR, garantendo il rispetto della normativa anche da parte dei fornitori.

In definitiva, il costante sviluppo della sanità digitale, che come abbiamo appena visto si avvale di strumenti come il Fascicolo sanitario, il dossier sanitario e la telemedicina, sta apportando un cambiamento significativo al tradizionale rapporto tra pazienti e sistema sanitario. Questi strumenti, sebbene garantiscono maggior efficienza e accessibilità, richiedno al contempo un quadro solido e una costante attenzione alla sicurezza e alla privacy. La sfida principale per gli operatori del settore rimane quella di integrare queste

[175] AA.VV, Data protection e privacy, cit., p.328 ss

[176] Sul punto si rinvia al cap. 2, par. valutazione d'impatto sulla protezione dei dati

[177] In particolare, come stabilito all'articolo 35 del GDPR

tecnologie avanzate in modo sicuro ed efficace, garantendo al contempo che i dati sensibili dei pazienti siano sempre protetti, pur incentivando un acesso alle cure più rapido ed efficiente per tutti.

3.2.2 Il bilanciamento tra il diritto di accesso del paziente e il diritto alla riservatezza di terzi

Il diritto di accesso agli atti amministrativi nel nostro ordinamento segnò una svolta epocale, poiché ha permesso di superare la segretezza statale he per anni ha caratterizzato lo svolgimento dell'attività delle Pubbliche Amministrazioni. Il punto di svolta, come è ormai noto, è rappresentato dalla legge 241 del 1990, la quale ha rivoluzionato il rapporto tra cittadini e Pubblica Amministrazione, trasformando quest'ultima da un'entità chiusa a un'istituzione trasparente, che opera al servizio dei cittadini. Questa legge, in conformità con i principi di trasparenza e pubblicità dell'azione amministrativa stabilisce che chiunque abbia un interesse diretto, concreto e attuale può richiedere di visionare la documentazione pertinente. L'interesse deve essere collegato a una situazione giuridicamente rilevante tutelata dal richiedente.

In sostanza, la normativa vigente pone in capo alla pubblica amministrazione l'obbligo di rendere accessibili i propri documenti a chiunque dimostri un legittimo e specifico interesse giuridico, garantendo così un maggiore partecipazione civica e un controllo costante sul suo operato.

Premesso ciò, occorre sottolineare come questa dinamica applicata al contesto della sanità, con particolare riferimento alla documentazione sanitaria, rende il percorso da affrontare più complesso e insidioso.

Qualora un paziente richieda una copia della propria cartella clinica, l'accesso ai suoi dati personali è generalmente semplice e senza ostacoli, e al suo interno deve ricomprendere "tutti i dati personali che riguardano l'interessato comunque trattati dal titolare". L'ente sanitario detentore del documento ha l'obbligo di fornire tutti i dati personali relativi al paziente e di renderli facilmente comprensibili per l'interessato. Il Garante per la Protezione dei Dati Personali ha stabilito il diritto dell'interessato ad ottenere l'accesso ai propri dati, specificando che se la cartella clinica è illeggibile a causa della grafia, l'ente sanitario deve trascrivere i dati in modo chiaro.

La legge prescrive che *"I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti che legalmente lo rappresentano, da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare."*[178] Da ciò discende che per i dati sensibili relativi allo stato di salute, le normative sanitarie stabiliscono che la comunicazione al paziente avvenga tramite un medico designato dal paziente o dalla struttura sanitaria stessa. Inoltre, questa regola non si applica se i dati sono stati forniti in precedenza dal paziente stesso, secondo quanto previsto all'articolo 84, comma 2, del Codice privacy. In determinati casi, anche altri professionisti sanitari, non necessariamente medici, possono essere autorizzati per iscritto a comunicare questi dati, a patto che siano stati designati formalmente e che rispettino le appropriate cautele.

Può accadere, alle volte, che l'interessato, odia colui che effettua la richiesta di accesso sia affetto da incapacità. In tal caso, è opportuno operare una distinzione tra incapacità dichiarata e incapacità temporanea. L'ordinamento giuridico italiano prevede diverse figure per tutelare gli interessi dell'individuo incapace, a seconda della gravità e della natura dell'incapacità[179].

In primo luogo l'interdizione che, ai sensi dell'articolo 414 del codice civile, che richiede che venga nominato un tutore che rappresenti legalmente l'infermo. Per interdetto si intende chi è affetto da una grave e abituale infermità mentale che lo rende incapace di badare ai propri interessi[180].

In secondo luogo, di fronte a infermità meno gravi rispetto all'interdizione, si parla di inabilitazione. In quest'ultimo caso viene nominato un curatore che assiste la persona, senza sostituirla completamente. Infine, abbiamo l'amministrazione di sostegno per persone che, a causa di infermità o menomazioni fisiche o psichiche, anche parziali o temporanee, non riescono a gestire i propri interessi. Viene nominato un amministratore di sostegno per compiere gli atti specificamente indicati dal giudice.

In tutti questi casi, il minimo comun denominatore è rappresentato dal fatto l'accesso ai dati sanitari e la gestione degli interessi legati alla salute non spettano più direttamente all'interessato, ma alla figura nominata legalmente per rappresentarlo o assisterlo.

---

178 art. 84, comma 1, del Codice della Privacy

179 Michele A. Nannarone, "Il bilanciamento tra il diritto di accesso e il diritto di riservatezza in sanità", in *Diritto.it*, 26 luglio 2023, disponibile su https://www.diritto.it/il-bilanciamento-tra-il-diritto-di-accesso-e-il-diritto-di-riservatezza-in-sanita, consultato il 22 agosto 2025

180 ibidem

Nel caso di interdizione la situazione risulta piuttosto chiara: il tutore, nominato dal giudice, agisce in totale sostituzione dell'interdetto. Di conseguenza, ogni richiesta di accesso alla cartella clinica, così come qualsiasi altro atto, deve essere presentata esclusivamente dal tutore.

Il caso dell'inabilitato, invece, risulta più complesso e richiede un'attenta analisi. Difatti, Il curatore non sostituisce in toto la persona, ma la assiste solo per specifici atti di particolare importanza, solitamente di natura patrimoniale. Generalmente, essendo la richiesta di una cartella clinica considerata un atto di natura personale, l'inabilitato conserva la piena capacità di agire al fine di effettuare la relativa richiesta di accesso e di prenderne visione. Conseguentemente l'istanza non può essere in alcun modo effettuata dal curatore, ma deve esser presentata direttamente dall'inabilitato.

Con riferimento all'amministrazione di sostegno la situazione più flessibile e dipende interamente da quanto stabilito nel decreto di nomina del giudice tutelare. In quest'ultimo viene specificato in dettaglio i poteri dell'amministratore e per quali atti (se ce ne sono) il beneficiario deve essere assistito. Questo significa che per decretare chi tra l'amministratore di sostegno e l'interessato possa richiedere è essenziale esaminare il decreto di nomina. Se questo non menziona esplicitamente l'accesso alla documentazione sanitaria tra i poteri dell'amministratore, si deve ritenere la richiesta spetti direttamente al diretto interessato.

In assenza di una dichiarazione formale di incapacità, una persona è considerata pienamente capace di accedere alla propria documentazione. Tuttavia, possono emergere dubbi sulla reale capacità di un individuo, e in tal caso è fondamentale vigilare per prevenire eventuali abusi da parte di terzi.

Dopo aver effettuato un'accorta valutazione sulla decisione, è opportuno stabilire se procedere o meno alla nomina di un amministratore si sostegno.

La normativa in materia di accesso ai documenti solleva un'importante questione etica e legale: come deve comportarsi un'autorità pubblica quando riceve una richiesta di accesso a dati sensibili, come quelli relativi alla salute, da parte di un terzo? La risposta risiede nel bilanciamento tra il diritto di accesso del richiedente e il diritto alla riservatezza dell'interessato.

Si premete che un generico riferimento al "diritto di azione e difesa" , pur se costituzionalmente tutelato, non è di per sé sufficiente, ma occorre far valere il diritto sottostante che il terzo vuol far valere sulla base dei dati o dei documenti che chiede di conoscere come parametro di raffronto.

É necessario, inoltre, che che il diritto sostanziale che il terzo intende tutelare sia di "pari rango" rispetto alla riservatezza dell'interessato. Tale criterio si deve ritenere soddisfatto, quand'anche semplicemente il diritto in questione rientra nella categoria diritti della personalità o in quella dei diritti o libertà fondamentali. Difatti, il codice della privacy stabilisce che " *quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della*

persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale"[181].

Più specificatamente, la giurisprudenza ha chiarito che l'Amministrazione, nel valutare una richiesta di accesso a dati sanitari, deve eseguire una duplice verifica. In primo luogo, deve accertare il "rango" del diritto che si intende difendere, essendo i diritti della personalità e le libertà fondamentali, come il diritto alla vita, all'integrità fisica, alla salute, all'onore o le libertà di circolazione, riunione e associazione, considerati di pari rango rispetto alla riservatezza.

In secondo luogo, l'amministrazione deve valutare se sussista l'effettiva "necessità "dei dati ai fini di assicurare un'appropriata tutela per il diritto in questione. Il che implica che anche se il diritto è di pari rango, l'accesso può essere concesso solo se i dati richiesti sono indispensabili per il perseguimento dello scopo dichiarato. Tale seconda fase valutativa può comportare anche un accoglimento parziale della richiesta, qualora solo una parte dei dati richiesti dove soddisfarsi strettamente necessaria per garantire l'effettiva tutela dell'interesse in questione[182].

In sostanza, la decisione definitiva è strettamente connessa non solo dalla natura del diritto in gioco, ma anche dalla sua effettiva e dimostrata esigenza rispetto ai dati specifici richiesti.

In conclusione, da quest'analisi si evince come quando la richiesta di accesso riguarda dati sensibili, come quelli sanitari, la dinamica si fa più complessa.

La richiesta di un paziente per la propria documentazione sanitaria è generalmente agevole, garantendo il pieno controllo sui propri dati personali. Ben diversa è la situazione quando un terzo richiede l'accesso a tali informazioni, poiché in tal l'amministrazione è tenuta ad effettuare un'attenta valutazione, bilanciando il diritto di accesso con quello, fondamentale, alla riservatezza.

É importante ribadire che l'accesso viene concesso, in seguito ad una duplice verifica, solo diritto che il richiedente intende tutelare è di "pari rango" e se i dati richiesti sono effettivamente necessari per lo scopo dichiarato. Tale duplice verifica, che deve essere effettuata caso per caso, è di fondamentale importanza, poiché garantisce che il principio di trasparenza non prevalga indebitamente sulla tutela della dignità e della riservatezza del singolo.

---

181 art. 60 d.lgs. 196 del 2003, cui fa rinvio l'art. 24 L. n. 241/1990 nel testo novellato dall'art. 16 L. 11 febbraio 2005, n. 15

182 Fabio Maria Donelli e Mario Gabbrielli, *Emergenza sanitaria e responsabilità medica*, Maggioli Editore, Santarcangelo di Romagna, 2021.

3.2.3 Il ruolo del Garante per la protezione dei dati personali

La Relazione annuale del Garante per la Protezione dei Dati Personali (Docweb n. 10148845), presentata lo scorso 15 luglio[183], assume estrema rilevanza, poiché fornisce un quadro chiaro e aggiornato sulla tutela della privacy in Italia. É importante analizzare brevemente la relazione del Garante in quanto dedica un particolare attenzione al settore sanitario, che si conferma come uno degli ambiti più delicati a causa della natura sensibile dei dati trattati.

Il comparto sanitario, in particolare, si trova a dover fronteggiare sfide significative, aggravate dalla crescente digitalizzazione dei servizi e dalle continue minacce informatiche, nonché ovviamente dalla natura sensibile dei dati trattati.

Sono diversi gli aspetti che hanno influito sulla sicurezza dei dati, sollevando nuove ed urgenti questioni, tra cui il crescente sviluppo della telemedicina, o l'introduzione del fascicolo sanitario elettronico e la maggiore interconnessione tra sistemi pubblici e privati[184].

In questo scenario, la Relazione del Garante non è solo un resoconto delle attività sanzionatorie e consultive dell'Autorità, ma rappresenta anche una guida fondamentale, fornendo un prezioso strumento di orientamento per tutti gli operatori del settore, inclusi i Responsabili della Protezione dei Dati (DPO), i dirigenti delle strutture sanitarie e gli sviluppatori di soluzioni digitali in ambito medico. Il fine ultimo del Garante rimane quello di assicurare che le misure di sicurezza e i principi dettati dal Regolamento Generale sulla Protezione dei Dati (GDPR**)** siano pienamente rispettati in un contesto in rapida evoluzione[185].

Occorre ora analizzare brevemente le criticità emerse nel 2023, anno in cui l settore sanitario è stato protagonista di una forte ondata di attacchi informatici, rappresentando il 9% degli incidenti di sicurezza segnalati al Garante, con un aumento di oltre quattro volte rispetto all'anno precedente. Si tratta di attacchi informatici che hanno interessato in particolare ospedali, ASL, laboratori diagnostici e servizi di refertazione online. Tra le principali criticità riscontrate dal Garante meritano di essere menzionate il mancato monitoraggio della vulnerabilità, poiché le strutture sanitarie non si sono preoccupate di aggiornare costantemente i propri sistemi per correggere le falle di sicurezza già note, nonché l'insufficienza dei sistemi back-up, rendendo difficile il ripristino dei dati in caso di attacco, poiché non adeguatamente protetti. Ulteriormente,

---

[183] Garante per la Protezione dei Dati Personali, Relazione annuale, presentata il 15 luglio 2024, Docweb n. 10148845, disponibile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10148845

[184] Nadia Martini, "Privacy e Sanità: Le priorità emergenti dalla Relazione del Garante", in Quotidiano Sanità, 25 luglio 2024, disponibile su https://www.quotidianosanita.it/lettere-al-direttore/articolo.php?articolo_id=131203

[185] ibidem

tra le criticità possiamo far riferimento alla mancanza di autenticazione a più fattori, non garantendo così misure di sicurezza aggiuntive per utenti con accessi privilegiati[186].

Un altro importante punto critico è a gestione degli accessi ai dati dei pazienti. In proposito, L'Autorità ha rilevato numerosi casi di accessi non autorizzati al dossier sanitario elettronico da parte di personale non direttamente coinvolto nella cura del paziente[187]. Tali violazioni comportano una lesione non indifferente del diritto alla riservatezza e violano al contempo il principio di minimizzazione dei dati. Per contrastarle efficacemente, è opportuno che le strutture sanitarie adottino rigorose misure di controllo, tra cui la tracciabilità degli accessi, la profilazione dei ruoli del personale e più in generale l'applicazione di un approccio "privacy by design" nella progettazione dei sistemi.

Anche l'evoluzione del FSE comporta nuove sfide. Difatti, il Garante sollecita le Regioni a uniformare la gestione del FSE e a garantire agli utenti un controllo granulare sui propri dati, con la possibilità di oscurare documenti specifici. Inoltre, particolare cautela è richiesta anche per la l'impiego telemedicina e l'utilizzo di piattaforme esterne.

Per quanto concerne l'uso dell'intelligenza artificiale nel settore sanitario , l'autorità garante ha pubblicato un decalogo per un uso etico dell'IA, sottolineando così la necessità di una supervisione umana, della trasparenza e di una valutazione d'impatto sulla privacy. Da ciò discende che anche l'utilizzo dell'IA nella medicina richiede adeguate garanzie per i pazienti.

Oltretutto, nella Relazione del 2024 il Garante ha tenuto a ribadire che, in assenza di un consenso esplicito, è illecito comunicare dati sanitari sensibili, come la sieropositività, anche ai familiari. Si tratta di un principio posto a tutela del paziente al fine di mantenere private le proprie informazioni, anche nei confronti dei congiunti.

Da ultimo, è importante notare come molti dei reclami gestiti dal Garante riguardano la mancata risposta delle strutture sanitarie alle richieste dei pazienti di accedere, rettificare o cancellare i propri dati, il che implica sicuramente una carenza nel garantire i diritti fondamentali riconosciuti dal GDPR.

In seguito alle criticità rilevate, il Garante ha fornito una serie di raccomandazioni pratiche al fine di rafforzare e migliorare la protezione dei dati in ambito sanitario. Si tratta di suggerimenti potenzialmente idonei a trasformare a sicurezza dei dati da un obbligo formale a una componente essenziale delle cure.

In primo luogo, l'autorità garante ha esortato l'adozione di tecnologie avanzate, ai fini di garantire l'implementazione da parte delle strutture sanitarie sistemi di autenticazione a più fattori,

[186] ibidem

[187] si veda sul punto Garante per la Protezione dei Dati Personali, Provvedimento n. 10144184/2024, disponibile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10144184.

segmentazione delle reti e controllo degli accessi privilegiati per i propri dipendenti, nonché l'adozioni di sitemi di back- up costantemente aggiornati e regolamentati.

Successivamente, viene raccomandato alle strutture sanitarie di attribuire in modo preciso i compiti, individuando figure come il Responsabile della Protezione dei Dati (DPO**)** e altri referenti interni per la privacy. In questo modo si assicurare la presenza costante di una responsabile per la gestione dei dati personali.

In aggiunta, il Garante raccomanda programmi annuali di aggiornamento per tutti gli operatori sanitari, sensibilizzandoli sui rischi e sulle buone pratiche, poiché la formazione è uno strumento fondamentale per garantire la prevenzione da errori o negligenze.

Oltretutto si prescrive alle strutture sanitarie di fornire ai pazienti canali semplici e sicuri per esercitare i propri diritti, come quello di accesso, rettifica o cancellazione dei dati, anche tramite portali digitali[188].

Come accennato in precedenza, anche la gestione corretta del fascicolo sanitario, che include anche una corretta gestione del consenso, è punto chiave messo in luce nelle raccomandazioni del garante.

In sostanza, possiamo affermare con certezza, alla luce di quanto emerso dall'analisi della Relazione del Garante del 2024, indirizzata a tutte le strutture sanitarie pubbliche e private, che a protezione dei dati non può essere considerata più un semplice onere burocratico, bensì un dovere etico, in particolare in un contesto caratterizzato da una sempre più ampia e diffusa digitalizzazione[189].

Il rispetto della normativa sulla privacy costituisce un dovere etico, principalmente perché si pone come condizione necessaria per mantenere la fiducia dei pazienti. Difatti, Garantire la riservatezza non solo rispetta le leggi, ma tutela la dignità e l'autodeterminazione degli individui. Proprio per tali motivi è estremamente importante investire sulla formazione, in tecnologie avanzate che garantiscono maggiore sicurezza e in un governo responsabile, auspicando in un futuro in cui innovazione e tutela procedono di pari passo.

3.1 Accesso amministrativo agli atti nella ricerca sanitaria: tra interesse pubblico, digitalizzazione e protezione dei dati sensibili

Il quadro normativo relativo alla ricerca scientifica in ambito sanitario è reso complesso principalmente da due fattori. Da un lato, il Regolamento Generale sulla Protezione dei

[188]. L. Bolognini, S. Zipponi, Privacy e diritto dei dati sanitari, Giuffrè, Milano, 2024
[189] ibidem

Dati (GDPR) ha cercato di uniformare le regole in tutta l'UE, ma ha concesso agli Stati membri la possibilità di introdurre deroghe e norme nazionali specifiche per la ricerca, generando talvolta un quadro normativo frammentario, nonostante il tentativo di armonizzazione. Dall'altro lato, occorre tenere a mente che il processo di adeguamento al GDPR nel nostro ordinamento è stato lento e complicato. Del resto, anche l'attribuzione di numerosi compiti all'autorità garante per la protezione dei dati personali ha determinato un prolungamento del periodo di transizione. Di conseguenza, non dve sorprendere il fatto che il contesto attuale sia caratterizzato da incertezze che hanno generato dubbi e difficoltà pratiche anche per gli esperti del settore.

Nel seguente paragrafo si vuole tentare di fornire una panoramica su questo complesso mondo della ricerca biomedica, e sulle conseguenze derivanti dall'introduzione del GDPR in questo ambito.

La ricerca scientifica si articola in diverse fasi, che spaziano dalla ricerca di base all'applicazione clinica, e come esamineremo di seguito la protezione dei dati personali in questo contesto presenta sfide etiche e giuridiche uniche, e in costante evoluzione, richiedono disposizione specifiche per la loro regolamentazione.

La ricerca di base si svolge principalmente in laboratorio ed è orientata all'aumento della conoscenza di un fenomeno biologico, senza che vi sia un'immediata finalità pratica. I risultati della ricerca di base sono essenziali per garantire il passaggio alla successiva ricerca traslazionale, il cui scopo è trasferire i risultati ottenuti dal laboratorio al "letto del paziente" (*from bench to bedside*), al fine di sviluppare nuovi farmaci e trattamenti[190].

La ricerca biomedica è un'area di studio interdisciplinare, che si avvale di approcci integrati per cercare di comprendere i meccanismi fisiologici, patologici e l'efficacia dei farmaci. Al suo interno ritroviamo la ricerca epidemiologica che si occupa di studiare il nesso causale tra fattori di rischio e determinate condizioni di salute come malattie, disabilità o morte. É proprio grazie a questo tipo di ricerca che numerosi esperti del settore sono riusciti a individuare associazioni tra malattie e loro fattori di rischio molto

[190] AA.VV., Data protection e privacy, op. cit., p. 335 ss

importanti per la salute, comportando un importante contributo per la medicina in generale e in particolare per l'oncologia.

Nello svolgimento delle sue analisi la ricerca epidemiologica può avvalersi di dati raccolti in modo prospettico, ossia osservando i pazienti e monitorandoli nel tempo o retrospettivo, ossia utilizzando dati già esistenti, come quelli presenti nelle cartelle cliniche, senza intervenire direttamente sul paziente.

Questo tipo di approccio si differenzia nettamente dai cosiddetti studi di intervento, come per esempio le sperimentazioni cliniche, considerati talvolta più "invasivi", in quanto condotti su esseri umani per scoprire o verificare gli effetti di medicinali e trattamenti sperimentali, incluse eventuali reazioni avverse, al fine di accertarne la sicurezza e l'efficacia terapeutica.

Tuttavia, indipendentemente dalla sua natura la ricerca scientifica viene considerata ta dal GDPR un contesto specifico di trattamento dei dati, che richiede particolari cautele. Anche in questo ambito, vedremo come il bilanciamento tra le libertà individuali e la libertà di ricerca solleva questioni etiche e giuridiche complesse che richiedono l'impiego di regole specifiche e ben definite[191].

Da quanto appena detto emerge il carattere peculiare della ricerca scientifica, intesa come processo sistematico che applica il metodo scientifico all'osservazione di fenomeni. Questo metodo prevede la formulazione di ipotesi e la loro verifica per giungere a conclusioni valide.

È importante sottolineare come la ricerca scientifica, avvalendosi di un continuo scambio di informazioni e conoscenze, soprattutto quando prevede il coinvolgimento di soggetti residenti in diversi paesi membri dell'Unione Europea, è soggetta al Regolamneto Generale sulla protezione dei Dati, il quale riconosce la ricerca come un'attività di interesse pubblico e le concede una certa flessibilità, a patto che venga posta in essere all'interno di quadro normativo idoneo a garantire un'adeguata tutela e nel rispetto dei principi etici.

L'ambito della ricerca scientifica è soggetto ad un trattamento speciale all'interno del GDPR, con la previsione di alcune importanti deroghe rispetto ai principi generali di protezione dei dati, che abbiamo analizzato esaustivamente nel corso della trattazione.

[191] L. Bolognini, S. Zipponi, Privacy e diritto dei dati sanitari, cit.

Generalmente, i dati personali devono essere raccolti per scopi specifici e non possono essere trattati per finalità incompatibili con tali scopi[192]. Tuttavia, per la ricerca scientifica, il GDPR introduce una "presunzione di compatibilità". Questo significa che se i dati raccolti inizialmente per un determinato scopo, come ad esempio la cura medica, vengono successivamente impiegati per la ricerca scientifica, non è richiesta una base giuridica separata. Questa regola si applica solo nel caso in cui siano state adottate tutte le misure di salvaguardia richieste, secondo quanto previsto dall'articolo 89 del GDPR[193], e si basa sul presupposto che la ricerca sia condotta nell'interesse pubblico e nel rispetto dei principi etici.

In tale contesto si richiede che i titolari del trattamento valutino e gestiscano attentamente i rischi, che possono essere estremamente elevati, specialmente quando il trattamento viene effettuato nei confronti di dati genetici o relativi alla salute, evidenziando pertanto il ruolo fondamentale assunto dal principio di responsabilizzazione (accountability) in tale ambito.

Inoltre tra i principi generali in materia di trattamento dei dati personali, viene altresì stabilito che i dati personali devono essere conservati solo per il tempo necessario a raggiungere la finalità per la quale sono stati raccolti[194]. Tuttavia, il GDPR consente di conservare i dati per periodi di tempo superiori se il trattamento è finalizzato alla ricerca scientifica, all'archiviazione nel pubblico interesse o per fini statistici. Tale deroga consente ai dati raccolti con fine di ricerca di avere valoro a lungo termine, in quanto la loro conservazione è considerata essenziale per il progresso della conoscenza collettiva.

Fermi i principi di cui sopra, proprio nel campo della ricerca scientifica, vengono introdotte alcune ulteriori semplificazioni normativamente previste, al ricorrere di determinate condizioni, relative alla compressione dei diritti degli interessati, nei casi in cui gli stessi possano pregiudicare in qualche modo l'attività scientifica o comprometterla.

---

[192] Principio di limitazione delle finalità, secondo quando stabilito all'articolo 5, comma 1, lett b) del GDPR

[193] Il quale testualmente stabilisce: " Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo."

[194] Secondo quanto stabilito all'art. 5, comma 1, lett e) del GDPR

Con riferimento al diritto di informazione: nel caso in cui i dati non possono essere raccolti direttamente dagli interessati o si è in presenza di una oggettiva impossibilità alla somministrazione della informativa o la sua somministrazione può avere luogo solo con elevata difficoltà, arrecando pertanto pregiudizio all'attività di ricerca, tale informativa potrà essere omessa. Viceversa, nessuna eccezione all'omissione di informativa potrà esservi laddove i dati siano raccolti presso gli interessati.

Con riferimento ai diritti di accesso, rettifica, limitazione e opposizione: la loro compromissione è ammessa solo nei casi in cui il rispetto di tali diritti renda impossibile o pregiudichi il conseguimento della finalità specifica della ricerca.

L'art. 9.2 j del GDPR dunque pone la base giuridica specifica del trattamento dei dati sensibili per la ricerca scientifica ed in base all'art. 89.1 il diritto dell'Unione o la legge nazionale dovrà contemperare la finalità perseguita con il diritto alla protezione dei dati quale diritto fondamentale dell'interessato.

Tuttavia, perchè si possa parlare di trattamento di dati deve ricorrere una base giuridica del trattamento.

Il GDPR amplia il numero delle potenziali basi giuridiche su cui può essere effettuato il trattamento dei dati personali.

L'individuazione della base giuridica è importante per comprendere il numero e la portata dei diritti che devono essere garantiti agli interessati e l'utilizzo futuro degli stessi da parte del titolare del trattamento.

Il consenso è la base che rende lecito il trattamento dei dati e deve essere fornito liberamente ed inequivocabilmente, esso è presupposto fondamentale del diritto di libertà di autodeterminazione terapeutica. Si può affermare che con il GDPR si è andati sempre più verso una impostazione consenso-centrica fissando in un certo senso i requisiti di validità del consenso.

Certamente fondare la base giuridica legittimante la ricerca scientifica può comportare delle problematiche.

Il titolare del trattamento dovrà essere in grado di adempiere ad una serie di oneri amministrativi e documentali. Egli dovrà dimostrare che il consenso sia realmente informato ovvero che tutte le informazioni di cui all'art. 13 del ripetuto GDPR (se raccolte direttamente) o di cui all'art. 14 del medesimo GDPR (se raccolte presso terzi), siano state date all'interessato, che il consenso sia libero, ossia che l'interessato abbia potuto

compiere una scelta libera e consapevole e ciò soprattutto è reso più complesso nel caso in cui l'interessato non sia in buone condizioni di salute. Inoltre l'interessato dovrà essere edotto della circostanza che il consenso potrà in ogni momento essere ritirato senza giustificazioni. In tal caso tutti trattamenti effettuati prima della revoca resteranno leciti, ma tutte le attività svolte con i dati della persona interessata dovranno cessare, i dati dovranno essere immediatamente cancellati e dovrà cessare anche la loro conservazione, salvo che non ricorrano altre basi legali che ne legittimo la conservazione.

L'European Data Protection Board (EDP)[195] stabilisce infatti - nel rispetto dei principi generali di cui all'art. 5 e fatte salve le garanzie di cui all'art. 89, comma 1 - che in tali casi, in alternativa al consenso, il trattamento possa fondarsi su altre basi giuridiche. Le altre basi giuridiche rilevanti possono individuarsi nell'interesse pubblico rilevante (art. 6 comma 1 lett e), nell'interesse legittimo (art6 comma 1 lett f) o motivi di interesse pubblico nel settore della sanità pubblica. In tale ultimo caso,in base all'art. 9 comma 2 lett. j, il diritto "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". Per tutelare i diritti e le libertà dell'interessato in particolare è previsto il segreto professionale.

In definitiva, l'accesso amministrativo agli atti nella ricerca sanitaria si colloca al crocevia tra esigenze di trasparenza, tutela della salute pubblica e protezione dei dati personali. Il quadro normativo attuale, arricchito e complicato dall'impatto del GDPR, impone alle amministrazioni sanitarie e ai ricercatori un costante bilanciamento tra diritti fondamentali e interesse pubblico. La digitalizzazione dei dati e l'internazionalizzazione della ricerca accentuano la complessità del sistema, rendendo essenziale l'adozione di misure organizzative e giuridiche adeguate.

---

[195] Il Comitato europeo per la protezione dei dati (EDPB**)** è un organismo indipendente dell'Unione Europea, che riunisce, sotto la propria egida, le Autorità nazionali di controllo in materia di protezione dei dati personali dei Paesi appartenenti allo Spazio Economico Europeo, insieme al Garante europeo della protezione dei dati (EDPS**)**. Per approfondire ulteriormente sul funzionamento e sui compiti del Comitato: https://edpb.europa.eu/about-edpb/board_it

3.3.1 Sperimentazioni cliniche e diritto di accesso: tra obblighi di pubblicità e protezione dei dati personali

Le sperimentazioni cliniche (clinical trials) sono studi di ricerca condotti per testare la sicurezza e l'efficacia di nuovi farmaci.

La sperimentazione clinica viene generalmente promossa da una società farmaceutica (cd. sponsor o promotore).

Il promotore predispone dunque un protocollo ove dettaglia la progettazione, gli obiettivi e la metodologia di sperimentazione. Tale protocollo deve essere presentato alle competenti autorità del settore e pertanto all' EMA (Agenzia Europea per i Medicinali) e l'AIFA[196] (Agenzia Italiana del Farmaco), dopo aver ottenuto anche l'approvazione di un comitato etico.

Di regola, le sperimentazioni si svolgono in centri di sperimentazione, ossia strutture organizzate come ospedali o università che si prestano a tal fine. Tali attività sono eseguita dai medici che si occupano della raccolta di dati clinici e campioni biologici dei partecipanti, in conformità con quanto stabilito nella Dichiarazione di Helsinki[197] e le buone pratiche cliniche (GCP)[198].

Per garantire la conformità al protocollo, lo sponsor accede alle informazioni cliniche dei partecipanti tramite propri collaboratori, come i clinical study monitor o le Contract Research Organization (CRO), che esaminano la documentazione originale dei pazienti. Le informazioni vengono poi trasmesse al promotore su schede di raccolta dati, cartacee o elettroniche.

Infine, al termine dello studio, tutti i dati sono inseriti in un database centralizzato per il controllo, la validazione e l'elaborazione statistica, con l'obiettivo di documentare i risultati finali che saranno successivamente documentati in un rapporto ufficiale.

In questo processo la gestione dei dati personali è specificamente regolamentata:

---

[196] L'EMA (Agenzia Europea per i Medicinali) è l'ente dell'Unione Europea che valuta e monitora i medicinali per l'UE e il SEE, mentre l'AIFA (Agenzia Italiana del Farmaco) è l'ente pubblico italiano che regola i farmaci a uso umano in Italia,

[197] La Dichiarazione di Helsinki] fu sviluppata dalla Associazione Medica Mondiale[2] (AMM o WMA), come un insieme di principi etici riguardanti tutta la comunità medica, per ciò che concerne la sperimentazione umana. Prtanto viene considerate la pietra angolare dell'etica della ricerca umana, in https://it.wikipedia.org/wiki/Dichiarazione_di_Helsinki

[198] Le Good Clinical Practice (GCP**)** o linee guida di buona pratica clinica, recepite con D.M.D 15 luglio 1997, il cui obbiettivo è quello di definire gli standard di buona pratica clinica, che possono essere implementati anche dai governi dei singoli Paesi nelle legislazioni riguardanti gli studi clinici su soggetti umani

Titolari del trattamento: il promotore (sponsor) e il centro di sperimentazione sono generalmente considerati titolari autonomi del trattamento in quanto hanno responsabilità e finalità distinte. Essi tuttavia, possono divenire co-titolari (ai sensi dell'art. 26 del GDPR) qualora determinino congiuntamente le finalità e i mezzi del trattamento.

Persone autorizzate e responsabili del trattamento: i clinical study monitor, ossia i soggetti che lavorano con il promotore, anch'essi agiscono come soggetti autorizzati al trattamento (art. 29 GDPR).

Le CRO (Contract Research Organizationo), che sono soggetti indipendenti ed esterni, anch'esse vengono nominate responsabili del trattamento dal promotore (art. 28 GDPR).

In tema di adempimenti privacy è necessario precisare che il centro di sperimentazione, quale punto di contatto diretto con i pazienti, ha l'obbligo, come previsto dagli artt. 12 e 13 del GDPR, di garantire sin dal principio la trasparenza e pertanto deve fornire ai pazienti un'informatica completa ed esaustiva sul trattamento dei dati personali. Questa informatica contenuta in un apposito documento viene somministrata congiuntamente dai titolari autonomi (o co-titolari).

E' importante ricordare che questo documento informativo contiene anche il consenso informato alla partecipazione alla sperimentazione, consenso che non deve essere confuso con il consenso come base giuridica per il trattamento dei dati personali di cui all'art. 9, comma 2, lett. a, esso risponde a requisiti etici e costituisce un requisito imprescindibile per la partecipazione allo studio.

L'importanza della trasparenza nella ricerca clinica nella ricerca clinica è un principio sostenuto da numerosi enti autorevoli come AIFA, EMA e OMS, poiché la divulgazione dei dati delle sperimentazioni è fondamentale per diversi ordini di motivi. Difatti, la mancanza di trasparenza può comportare conseguenze negative come l'inefficienza della ricerca dovuta alla duplicazione degli studi, la distorsione delle decisioni regolatorie e l'eventualità di sottoporre i volontari a rischi inutili[199]. Per contro, la pubblicazione dei dati consentirebbe di aumentare l'efficienza nello sviluppo dei farmaci, accrescendo allo stesso tempo la fiducia dei cittadini nella scienza.

[199] AIFA, "Condivisione dei dati provenienti dalle sperimentazioni cliniche: l'importanza di un approccio globale", in https://www.aifa.gov.it/-/condivisione-dei-dati-provenienti-dalle-sperimentazioni-cliniche-l-importanza-di-un-approccio-globale, 23 agosto 2025

Il nuovo Regolamento europeo sulle sperimentazioni cliniche (*EU Regulation 536/2014 on Clinical Trials*)[200] segue questa direzione, rendendo obbligatoria la pubblicazione su una banca dati europea accessibile al pubblico, migliorando non solo la sicurezza, ma accrescendo anche la competitività nel settore della ricerca clinica. Tuttavia, per un efficacie condivisione dei dati, tale obbligo di pubblicazione non è di per sé sufficiente. È altresì necessari creare un portale centralizzato e un'organizzazione indipendente e non-profit al fine di facilitare l'accesso alle informazioni e il loro utilizzo. Il fine ultimo è quello assicurare un sempre maggiore efficienza nel procedimento di sviluppo dei farmaci, attraverso la condivisione e la piena accessibilità ai dati utili, garantendo un miglioramento della vita dei pazienti[201].

In sostanza, il sistema delle sperimentazioni enfatizza l'importanza di garantire un equilibrio tra trasparenza e protezione dei dati personali. Il diritto di accesso, in questo contesto, assume un ruolo centrale quale strumento di controllo e partecipazione, ma deve essere esercitato nel rispetto delle normative sulla riservatezza e delle specificità della ricerca scientifica. Il rispetto della normativa vigente in materia, le disposizioni del GDPR e il Regolamento (UE) 536/2014, e la sua corretta applicazione rappresentano i punti chiave per assicurare ai cittadini un accesso informato, proporzionato e funzionale agli interessi pubblici e individuali coinvolti.

È importante sottolineare, infine, come questo quadro normativo mira a garantire da un lato la trasparenza e l'efficienza della ricerca, e dall'altro la tutela dei diritti fondamentali dei soggetti coinvolti.

Difatti, la trasparenza se correttamente bilanciata con la riservatezza, costituisce un presupposto essenziale per promuovere la fiducia nella ricerca clinica e favorire il progresso scientifico nel rispetto della dignità umana.

3.3.2 Considerazioni Conclusive

[200] Rgolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE (1), consultabile in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L:2014:158:FULL&from=IT

[201] Per approfondire vedi anche: EMA, "Policy on pubblication of clinical data for medical products for human use", EMA/ 240815/2014, 2 ottobre 2015, in https://www.ema.europa.eu/docs/en_GB/document_library/Other/2014/10/WC500174796.pdf

Dal punto di vista amministrativo, il diritto di accesso ai dati sanitari si inserisce in un ambito particolarmente delicato, dove l'esigenza di trasparenza dell'azione pubblica deve costantemente confrontarsi con il dovere di protezione dei dati personali, specie quando si tratta di informazioni sensibili come quelle relative alla salute. L'accesso agli atti, inteso come strumento di controllo e partecipazione del cittadino, rappresenta una garanzia fondamentale per assicurare legalità e buon andamento dell'amministrazione, ma deve necessariamente essere esercitato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (GDPR e Codice Privacy).

L'amministrazione sanitaria, in qualità di titolare del trattamento, è chiamata a valutare caso per caso se l'istanza di accesso sia compatibile con i diritti e le libertà fondamentali dell'interessato, adottando misure di tutela adeguate e proporzionate. In particolare, nei casi di accesso civico generalizzato o accesso documentale ex L. 241/1990, assume rilievo il bilanciamento tra l'interesse conoscitivo e la riservatezza dei dati dei terzi, da compiere secondo i criteri indicati dalle autorità garanti e dalla giurisprudenza amministrativa[202].

Il Garante per la protezione dei dati personali ha innanzitutto ricordato che l'accesso civico generalizzato consente a chiunque di richiedere dati e documenti in possesso delle pubbliche amministrazioni che non siano già stati pubblicati, purché si rispettino i limiti atti a tutelare interessi giuridicamente rilevanti dei soggetti coinvolti. In particolare, il limite principale è costituito dalla tutela dei dati personali dei controinteressati: pertanto, l'amministrazione deve rifiutare l'accesso se tale rifiuto è necessario per evitare un pregiudizio concreto alla protezione dei dati. Senza dimenticare che l'accesso civico

[202] Sul punto si veda anche TAR Lazio, Roma, Sez. III Quater, sent. 10 febbraio 2023, n. 2297 : " Al fine dell'esercizio del diritto di accesso che abbia ad oggetto dati sensibili, è essenziale dimostrare non già un generico interesse alla tutela dei propri interessi giuridicamente rilevanti, ma la concreta necessità (e, dunque, la stretta indispensabilità) dell'utilizzazione della documentazione richiesta in uno specifico giudizio, atteso che, nel quadro del bilanciamento tra il diritto alla tutela della riservatezza ed il diritto all'esercizio del cosiddetto accesso difensivo, risulta necessario accertare l'effettiva sussistenza o meno del nesso di strumentalità esistente tra la documentazione oggetto dell'istanza di accesso e le censure formulate, con la conseguenza che l'onere della prova del suddetto nesso di strumentalità incombe, secondo il consueto criterio di riparto dell'onere della prova, su chi agisce; l'interesse difensivo all'accesso agli atti di gara va, dunque, verificato in concreto. È altresì necessario provare il collegamento tra la posizione giuridica soggettiva da tutelare e i documenti oggetto della richiesta di accesso". V. anche - Consiglio di Stato, Sez. V, 05/08/2020, n. 4930.

generalizzato è sempre escluso quando la legge vieta espressamente l'accesso o la divulgazione del documento richiesto.

La digitalizzazione dei servizi sanitari e la crescente interoperabilità tra banche dati pubbliche impongono, inoltre, una maggiore attenzione alle modalità di gestione delle richieste di accesso, anche alla luce dei principi di minimizzazione, integrità e sicurezza dei dati trattati. In tale contesto, l'amministrazione deve dotarsi di strumenti organizzativi e tecnologici adeguati, oltre che di linee guida operative chiare, per garantire un accesso effettivo ma non lesivo.

Inoltre il costante sviluppo della sanità digitale, che come abbiamo appena visto si avvale di strumenti come il Fascicolo sanitario, il dossier sanitario e la telemedicina, sta apportando un cambiamento significativo al tradizionale rapporto tra pazienti e sistema sanitario. Questi strumenti, sebbene garantiscono maggior efficienza e accessibilità, richiedno al contempo un quadro solido e una costante attenzione alla sicurezza e alla privacy. La sfida principale per gli operatori del settore rimane quella di integrare queste tecnologie avanzate in modo sicuro ed efficace, garantendo al contempo che i dati sensibili dei pazienti siano sempre protetti, pur incentivando un accesso alle cure più rapido ed efficiente per tutti.

In aggiunta, anche il Sistema delle sperimentazioni cliniche evidenzia l'importanza di garantire un costante equilibrio tra trasparenza e protezione dei dati personali. Del resto anche in questo ambito il diritto di accesso ricopre un ruolo fondamnetale come strumento di controllo e partecipazione, il quale deve essere necessariamnete esercitato in conformità con la normative in materia di riservatezza, tenendo conto delle specifità della ricerca scientifica. Ed è proprio attraverso il rispetto delle disposizioni del GDPR e del Regolamento (UE) 536/2014, che si assicura ai cittadini un accesso informato, proporzionato e funzionale agli interessi pubblici e individuali coinvolti, costituendo di fatto al trasparenza un presupposto fondamentale per favorire il progresso scientifico e la fiducia nella ricerca clinica nel rispetto dei diritti e delle libertà individuali[203].

[203] Fabio Maria Donelli e Mario Gabbrielli, *Emergenza sanitaria e responsabilità medica*, op cit.

Da ciò discende che nell'era digitale il diritto di accesso ai dati sanitari pone l'amministrazione di fronte alla sfida di conciliare trasparenza e protezione, partecipazione e responsabilità. Solo attraverso un'applicazione consapevole e ponderata delle norme sarà possibile garantire un accesso legittimo e rispettoso della dignità della persona, salvaguardando al contempo l'efficienza e l'imparzialità dell'azione amministrativa.

In conclusione, il diritto di accesso ai dati sanitari, è un aspetto fondamentale della tutela della privacy, che vede coesistere le disposizioni del GDPR con le specifiche normative nazionali. La gestione e il trattamento di questi dati di natura sensibile richiede l'adozione di misure proattive, come il registro delle attività di trattamento, oltre che il rispetto della normativa vigente in materia. Un ulteriore misura di garanzia è rappresentata dalla nomina di un DPO, che sebbene non sia sempre richiesta obbligatoriamente per i singoli professionisti, è essenziale per le organizzazioni che trattano dati su larga scala, assicurando conformità con il principio di trasparenza[204].

Conclusioni

In linea con le tendenze internazionali, l'Italia sta attraversando un profondo processo di innovazione nei servizi per cittadini e imprese, che si basa sull'uso delle tecnologie digitali. Questa evoluzione tecnologica sta avendo e continuerà ad avere un impatto significativo sulla trasparenza dell'azione amministrativa e, di conseguenza, sul diritto di accesso agli atti

L'analisi dell'evoluzione del diritto di accesso agli atti amministrativi dimostra come il concetto di trasparenza sia passato da un'idea di mera formalità a un pilastro sostanziale del rapporto tra cittadino e pubblica amministrazione. Questo percorso, segnato da normative chiave come la Legge n. 241 del 1990 e le successive modifiche, ha trovato nella digitalizzazione una nuova, complessa frontiera. In particolare, le recenti

[204] T. Casadei, S. Pietropaoli, Diritto e tecnologie informatiche, cit.. p. 69 e ss

introduzioni dell' accesso civico semplice e dell'accesso civico generalizzato hanno ampliato notevolmente il diritto dei cittadini di conoscere l'operato della pubblica amministrazione. Tuttavia, questo diritto non è illimitato. Sul piano teorico, esistono ancora aree dell'azione amministrativa che non possono essere oggetto di accesso, come le "mere informazioni" che non hanno ancora assunto la forma di un documento. Questo scenario potrebbe però mutare con l'avanzamento tecnologico, che potrebbe rendere accessibili anche questi dati in futuro

L'era digitale, pur offrendo strumenti senza precedenti per l'efficienza e la partecipazione, ha sollevato sfide inedite e di vasta portata, specialmente nella delicata intersezione tra trasparenza e protezione dei dati personali.

Una delle principali sfide emergenti è rappresentata dalla necessità di conciliare il diritto alla conoscenza con le tutele del GDPR. Questo equilibrio è particolarmente critico in settori sensibili come la sanità, dove la digitalizzazione dei dati, attraverso strumenti come il Fascicolo Sanitario Elettronico (FSE), richiede un'attenzione costante per garantire che la facilità di accesso non comprometta la privacy. La gestione dei dati sanitari impone l'adozione di misure proattive e il rispetto rigoroso di principi come la minimizzazione dei dati, la trasparenza e la sicurezza informatica, evidenziando il ruolo sempre più cruciale di figure professionali come il Responsabile della Protezione dei Dati (DPO).

Inoltre, il rapporto tra trasparenza e ricerca scientifica, soprattutto nel campo delle sperimentazioni cliniche, pone ulteriori interrogativi. Se da un lato il diritto di accesso può promuovere la fiducia e il controllo sulla ricerca, dall'altro deve fare i conti con la riservatezza delle informazioni scientifiche e la protezione dei dati dei partecipanti. La sfida consiste nel trovare un equilibrio che permetta di garantire la trasparenza funzionale all'interesse pubblico senza ledere i diritti individuali, come stabilito dal Regolamento (UE) 536/2014.

In conclusione, il diritto di accesso è oggi un istituto dinamico che si confronta con le continue trasformazioni tecnologiche e normative. La sua piena realizzazione dipende dalla capacità delle pubbliche amministrazioni di integrare in modo sicuro ed etico le tecnologie digitali, trasformando le sfide in opportunità. Solo così sarà possibile edificare

un'amministrazione che, pur operando in un contesto di crescente complessità, sappia coniugare innovazione, efficienza, trasparenza e tutela dei diritti fondamentali dei cittadini.

La trasformazione in atto segna un cambio di paradigma, passando dalla mera dematerializzazione dei documenti a un'integrazione strutturale delle tecnologie dell'informazione e della comunicazione (ICT) in ogni aspetto dell'azione pubblica. Questo percorso, sebbene complesso, mira a rendere il diritto di accesso un pilastro operativo e non solo formale, con ricadute positive sulla qualità dei servizi, sulla partecipazione dei cittadini e sul controllo democratico dell'operato statale
A livello generale, la pubblica amministrazione si trova ancora in una fase di transizione e adattamento al digitale. La vera e propria digitalizzazione dei processi richiede una completa reingegnerizzazione dell'agire amministrativo, che porterà a nuove e più definite modalità di accesso e trasparenza, probabilmente destinate a convergere in modo organico.

Questa spinta verso la digitalizzazione è ulteriormente rafforzata dal Piano Nazionale di Ripresa e Resilienza (PNRR), che la identifica come una delle aree di intervento prioritarie. Questo piano, insieme alle direttive europee, influenzerà profondamente l'esercizio del diritto di accesso. L'obiettivo non è solo modernizzare l'infrastruttura tecnologica, ma anche ripensare l'intera organizzazione amministrativa per renderla più efficiente e vicina ai cittadini.

Bibliografia

ALONGI, G., POMPEI, L., Diritto della privacy e della protezione dei dati personali, Tab edizioni, 2021.

BATTELLI, E., CUFFARO, T. (a cura di), Codice privacy e provvedimenti del garante per la protezione dei dati personali, Giuffrè, 2025.

BOLOGNINI, L., ZIPPONI, S., Privacy e diritto dei dati sanitari, Giuffrè, Torino, 2024.

CLEMENTE DI SAN LUCA, G., "Diritto di accesso e interesse pubblico", Jovene Editore, Napoli, 2006.

DELLA CANANEA, G., DUGATO, M., MARCHETTI, B., POLICE, A., RAMAJOLI, M., Manuale di Diritto Amministrativo, G. Giappichelli, Torino, 2021.

DONELLI, F. M., GABBRIELLI, M., Emergenza sanitaria e responsabilità medica, Maggioli Editore, Santarcangelo di Romagna, 2021.

FINOCCHIARO, G., Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, Zanichelli, 2017.

LEVI, F., L'attività conoscitiva della pubblica amministrazione, Giappichelli, Torino, 1967.

MACRÌ, I., Digitalizzazione. Innovazione e Sicurezza nella p.a., Walter Kluters, 2022.

MATTARELLA, B. G., SAVINO, M. (a cura di), L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto, Napoli, Editoriale Scientifica, 2018.

MELIS, G., Storia dell'amministrazione italiana, Bologna, il Mulino, 1996.
MIELE, T., "Il procedimento amministrativo e il diritto di accesso", G. Giappichelli Editore, Torino, 1995.

MINAZZI, F., Il codice dell'amministrazione digitale riformato, Giuffrè, Milano, 2017.
PIZZETTI, F., Privacy e il diritto europeo alla protezione dei dati personali, Torino, Giappichelli, 2019.

PONTI B., La trasparenza amministrativa dopo il d.lgs. 33/2013, Santarcangelo di Romagna, 2013.

PUBUSA, F., Diritto di accesso ed automazione, Giappichelli, Torino, 2006.

ROSSA, S., Contributo allo studio delle funzioni amministrative, Cedam, novembre 2021.

SANDULLI, A., Manuale di diritto amministrativo, Jovene Editore, Napoli, 1989.

SANTISEI, M., Coordinate ermeneutiche di diritto amministrativo, Giappichelli, Torino, 2021.

TORCHIA, L., Lo Stato digitale. Una introduzione, Bologna, il Mulino, 2023.

Articoli e Saggi in Riviste

BASSINI, M., "Il fattore umano nella protezione dei dati personali: tra formazione e responsabilità", in Federalismi.it, n. 5, 2020.

BARRA, F., "Il diritto d'accesso civico generalizzato (c.d. FOIA): paradigmi, modelli e percorsi applicativi", in Rivista italiana di informatica e diritto, 6, 1 (Giugno 2024), pp. 191–216.

CORRADO, A., "Il silenzio dell'amministrazione sull'istanza di accesso civico generalizzato: quale possibile tutela processuale", in federalismi.it, n. 5, 2017.

COSTANTINO, F., "Lampi. Nuove frontiere delle decisioni ammnistrative tra open e big data", Giuffrè, Milano, 2017.

DAGOSTINO, R., "La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà", in P.A. Persona e Amministrazione, vol. 14, n. 1, 2024.

D’ORLANDO, E., ORSONI, G., "La digitalizzazione e l'organizzazione della pubblica amministrazione", in Istituzioni del federalismo: rivista di studi giuridici e politici, XLIV, 2, 2023, pp. 279 ss.

ESPOSITO, V., DEL GROSSO, F., PASSANNANTI, G., "Il diritto sociale alla trasparenza tra diritto di accesso e accesso civico", in filodiritto.com.

GALETTA, D. U., "Accesso civico generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del Decreto FOIA; la trasparenza de 'la vita degli altri'?", in federalismi.it, n. 10, 2018.

LICIA, C., "La Protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale", 2023.

PORTO, P., "Il principio di trasparenza e il diritto di accesso in ambito sanitario", in Ratio Iuris (ISSN 2420-7888), 2025, p. 5 ss.

SANDULLI, A., "Il procedimento amministrativo e la trasparenza", in L'amministrazione pubblica italiana (a cura di S. CASSESE e C. FRANCHINI), Bologna, 1994, pp. 101 ss.

SARTOR, G., "Data breach e obblighi di notifica: il nuovo sistema di responsabilità", in Il diritto dell’informazione e dell’informatica, 2019.

ALBISSINI F. G., "Germania", in Mattarella, B. G., Savino, M. (a cura di), L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto, Napoli, Editoriale Scientifica, 2018.

CARROTTI, B., "Spagna", in Mattarella, B. G., Savino, M. (a cura di), L'accesso dei cittadini. Esperienze di informazione amministrativa a confronto, Napoli, Editoriale Scientifica, 2018.

Altri Documenti e Rapporti

ANZALONE, A., Macri, I., Siragusa, F., La nuova contabilità delle amministrazioni pubbliche, Milano, 2015.

CARROTTI, B. (a cura di), Le funzioni amministrative digitali. Intervista a Stefano Rossa, Osservatorio sullo Stato Digitale – IRPA, 2023.

CHIEFFI, G., Evoluzione normativa del diritto di accesso ai documenti ai documenti amministrativi, in dirittifuturo.it.

The Onlife Manifesto. Being a human in a hyperconnected Era, Springer, Heidelberg New York, 2015.

PATRONI GRIFFI F., Un'introduzione al testo unico sulla documentazione amministrativa: metodologia e procedure, in Comuni D'Italia 2001

Riferimenti normativi

Legge n. 816/1985

Legge n. 349/1986

Legge n. 801/1997: "Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato".

Decreto Ministero della Sanità 18 febbraio 1982: "Norme per la tutela sanitaria dell'attività sportiva agonistica".

Circolare del Ministero della Sanità n. 900 2/AG454/260: emanata il 19 dicembre 1986.

Legge n. 241/1990: "Nuove norme in materia di procedimento amministrativo e di diritti di accesso ai documenti amministrativi".

Decreto Legislativo n. 39/1993: "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche".

Legge n. 59/1997: "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa".

D.P.R. n. 513/1997.

D.P.R. n. 445/2000: "Testo unico sulla documentazione amministrativa".

Decreto Legislativo n. 196/2003: "Codice in materia di protezione dei dati personali".

Legge n. 15/2005: "Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241".

Legge n. 80/2005: ha attribuito la giurisdizione esclusiva in materia di accesso al giudice amministrativo.

D. Lgs. n. 82/2005: "Codice dell'Amministrazione Digitale".

D.P.R. n. 184/2006: "Regolamento sull'accesso ai documenti amministrativi".

Decreto-Legge n. 179/2012: "Ulteriori misure urgenti per la crescita del paese".

Decreto Legislativo n. 33/2013: "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".

Legge n. 24/2017: (Legge Gelli-Bianco) "Disposizioni in materia di sicurezza delle cure e della persona assistita, nonche' in materia di responsabilita' professionale degli esercenti le professioni sanitarie".

Decreto-Legge n. 34/2020: "Misure urgenti in materia di salute, sostegno al lavoro e all'economia".

Altre fonti

Agenzia per la Cybersicurezza Nazionale, Rapporto sulla sicurezza cibernetica in Italia, Roma, 2023.

Agenzia per l'Italia Digitale (AgID), Linee guida sulla continuità operativa nella Pubblica Amministrazione, 2020.

Garante per la Protezione dei Dati Personali, Linee guida sulla valutazione d'impatto relativa alla protezione dei dati (DPIA), 2018.

Garante per la Protezione dei Dati Personali, Provvedimento 7 marzo 2019, n. 55 – Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario.

Turati, F., Atti del Parlamento Italiano, Camera dei Deputati, sessione 1904-1908, 17 giugno 1908.

ENISA, Cybersecurity Threat Landscape 2023.

Giurisprudenza

Consiglio di Stato, Adunanza Plenaria, 5 settembre 2005, n. 5.

Consiglio di Stato, Sezione VI, 22 giugno 2020, n. 3891.

TAR Lazio, Roma, Sezione III Quater, 10 febbraio 2023, n. 2297.

TAR Lazio, Roma, Sezione II, 2 ottobre 2023, n. 14553.

TAR Sicilia-Palermo, Sezione I, 9 novembre 2005, n. 5000.

TAR, Potenza, Sezione I, 5 ottobre 2023, n. 565.

Sitografia

agenzia per l'Italia Digitale (AgID), Linee guida sulla continuità operativa nella Pubblica Amministrazione, 2020. Disponibile su: https://context.reverso.net/traduzione/italiano-inglese/non+specificato.

AIFA, "Condivisione dei dati provenienti dalle sperimentazioni cliniche: l'importanza di un approccio globale", 23 agosto 2025. Disponibile su: https://www.aifa.gov.it/-/condivisione-dei-dati-provenienti-dalle-sperimentazioni-cliniche-l-importanza-di-un-approccio-globale.

Comitato europeo per la protezione dei dati (EDPB), [Homepage]. Disponibile su:

https://edpb.europa.eu/about-edpb/board_it.

Garante per la Protezione dei Dati Personali, "Cybersecurity", 18 agosto 2025. Disponibile su: https://www.garanteprivacy.it/temi/cybersecurity.

Garante per la Protezione dei Dati Personali, Linee guida in materia di Dossier sanitario del 4 giugno 2015. Disponibile su:

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4084632.

Garante per la Protezione dei Dati Personali, Provvedimento 7 marzo 2019, n. 55 – Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario, [doc. web n. 9091942]. Disponibile su:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942.

Garante per la Protezione dei Dati Personali, Relazione annuale, presentata il 15 luglio 2024, Docweb n. 10148845. Disponibile su:

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10148845.

Garante per la Protezione dei Dati Personali, Provvedimento n. 10144184/2024. Disponibile su:

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10144184.

Articoli e Documenti Online

Ceresetti, G., Diritto di accesso e atti delle autorità sanitarie, pp. 267 ss. Disponibile su:

https://www.ildirittodelleconomia.it/wp-content/uploads/2022/03/12Ceresetti.pdf.

Chieffi, Gabriele, Evoluzione normativa del diritto di accesso ai documenti ai documenti amministrativi. Disponibile su: www.dirittifuturo.it.

Coppola, Salvatore, "Protezione dei dati sanitari, tutti i paletti del Garante Privacy", Agenda Digitale, 27 marzo 2019, consultato il 20 agosto 2025. Disponibile su: https://www.agendadigitale.eu/sicurezza/privacy/protezione-dei-dati-in-sanita-tutti-i-paletti-del-garante-privacy/.

Iacono, N., Ruiu, G., Open Government, a cura di Formez PA, Dipartimento della Funzione Pubblica, ottobre 2015. Disponibile all'indirizzo: https://egov.formez.it/sites/all/files/open_government.pdf.

Martini, Nadia, "Privacy e Sanità: Le priorità emergenti dalla Relazione del Garante", in Quotidiano Sanità, 25 luglio 2024. Disponibile su: https://www.quotidianosanita.it/lettere-al-direttore/articolo.php?articolo_id=131203.

Nannarone, Michele A., "Il bilanciamento tra il diritto di accesso e il diritto di riservatezza in sanità", in Diritto.it, 26 luglio 2023, consultato il 22 agosto 2025. Disponibile su: https://www.diritto.it/il-bilanciamento-tra-il-diritto-di-accesso-e-il-diritto-di-riservatezza-in-sanita.

Rampulla, F. C., Ricciardi, G. C., Venturi, A., Digitalizzazione delle amministrazioni e accesso a dati e documenti informatici sanitari, 24 Gennaio 2024, pp. 133 e ss. Disponibile su: www.federalismi.it.

"Marriot hotel: multa da 20,4 milioni di euro a seguito di data breach", in federprivacy.org, 16 agosto 2025. Disponibile su: https://www.federprivacy.org/informazione/societa/marriott-hotel-multa-da-20-4-milioni-di-euro-a-seguito-di-un-data-breach.

"Lo standard ISO/IEC 27001...", in Wikipedia. Disponibile su:

https://it.wikipedia.org/wiki/ISO/IEC_27001.

"L'indice di digitalizzazione...", in Commissione Europea. Disponibile su:

https://digital-strategy.ec.europa.eu/it/policies/desi.

https://www.wordreference.com/enit/unidentified, https://www.nextre.it/ict-cose/.

Regolamento (UE) n. 536/2014. Disponibile su:

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L:2014:158:FULL&from=IT.

"Policy on pubblication of clinical data for medical products for human use", EMA/240815/2014, 2 ottobre 2015. Disponibile su: https://www.ema.europa.eu/docs/en_GB/document_library/Other/2014/10/WC500174796.pdf.