



# UNIVERSITÀ DEGLI STUDI DI CASSINO E DEL LAZIO MERIDIONALE

Corso di Dottorato in

curriculum Istituzioni e Azienda

Ciclo XXXVI

**Dati, nuove tecnologie e Pubblica Amministrazione:  
nuove sfide e forme di tutela**

SSD: IUS 10

Coordinatore del Corso  
Chiar.ma Prof.ssa Rosella  
Tomassoni

Dottorando  
Benedetta Gargari

Supervisore  
Chiar.ma Prof.ssa Margherita  
Interlandi

Co-Supervisore  
Chiar.ma Prof.ssa Maria  
Alessandra Sandulli



# INDICE

## CAPITOLO 1

### LA PROTEZIONE DEI DATI NEL SISTEMA DELLE FONTI

1. Il passaggio dal diritto alla riservatezza alla *privacy* come diritto alla protezione dei dati personali.
2. Sul labile confine tra riservatezza e *privacy*.
3. L'influenza delle fonti del diritto dell'Unione europea e della CEDU nell'ordinamento nazionale nell'ambito della protezione dei dati personali.
4. Il ruolo della CEDU.
5. Il Regolamento europeo per la protezione dei dati personali e la lettura contestuale con il Codice della Privacy.

## CAPITOLO 2

### LA PUBBLICA AMMINISTRAZIONE NELL'ERA DEI DATI

1. *Artificial Intelligence Act* europeo, nuove prospettive per la Pubblica Amministrazione.
2. La stretta interconnessione tra protezione dei dati personali e sistemi di Intelligenza Artificiale
3. A quale *Authority* la competenza sull'IA?
4. Nuove tecnologie a servizio della Pubblica Amministrazione e decisioni automatizzate: l'IA applicata nel settore pubblico.
5. Il necessario bilanciamento tra trasparenza algoritmica e protezione dei dati personali.

## Capitolo 3

### **I DATI IN MANO PUBBLICA: TRA ORGANIZZAZIONE AMMINISTRATIVA E INFRASTRUTTURE STRATEGICHE**

1. Premessa: l'evoluzione tecnologica e i dati in mano pubblica, quali problemi?
2. *Big data* e *open data*: tra innovazione e criticità in un ordinamento democratico.
3. L'organizzazione amministrativa nella gestione dei dati pubblici: dal modello *Government as a platform* al Polo Strategico Nazionale
4. *Cloud* Nazionale: tra utopia e primi problemi applicativi

## Capitolo 4

### **Spunti conclusivi**

### **Bibliografia**

# CAPITOLO I

## LA PROTEZIONE DEI DATI NEL SISTEMA DELLE FONTI

**SOMMARIO:** **1.** Il passaggio dal diritto alla riservatezza alla privacy come diritto alla protezione dei dati personali. **2.** Sul labile confine tra riservatezza e privacy. **3.** L'influenza delle fonti del diritto dell'Unione Europea e della CEDU nell'ordinamento nazionale nell'ambito della protezione dei dati personali. **4.** Il ruolo della CEDU. **5.** Il Regolamento Europeo per la protezione dei dati personali e la lettura contestuale con il Codice della Privacy.

### **1. Il passaggio dal diritto alla riservatezza alla privacy come diritto alla protezione dei dati personali**

Ai fini di illustrare esaurientemente le questioni problematiche concernenti la protezione dei dati personali e le nuove sfide dell'Intelligenza Artificiale, si ritiene preminente partire dal principio svolgendo un'introduzione sui concetti di privacy, diritto alla riservatezza e protezione dei dati personali.

L'ambito di applicazione della privacy è ampio e ha assunto concretezza e dinamicità soprattutto con l'avvento delle nuove tecnologie.

Le origini, risalgono ai sistemi giuridici di common law. La nascita di un diritto alla privacy nei sistemi anglosassoni viene riferita a un discorso pronunciato nel 1766 da Lord Chatham nel Parlamento inglese in un dibattito sull'utilizzo delle garanzie, il quale affermava che *“il più povero degli uomini può, nella sua casetta lanciare una sfida opponendosi alle forze della corona. La casetta può essere anche fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, ma il re d'Inghilterra non può entrare.”* La metafora del discorso indica che c'è un confine, un limite che nessuno, (nel contesto dell'esempio neanche il re di Inghilterra) può superare. L'attenzione

al diritto alla privacy, nell'ordinamento italiano non arriva come nei sistemi giuridici di common law. In particolare, verso la fine dell'800, in America, nello specifico il 15 dicembre del 1890 nella rivista "*Harvard law review*" veniva pubblicato da Samuel Warren e Louis Brandeis un articolo in cui si iniziava a parlare di "*right to privacy*" inteso come diritto ad essere lasciati in pace, nell'accezione data precedentemente nel 1888 dal Giudice Thomas Cooley come "*right to be let alone*"<sup>1</sup> nel suo *Law of Tort*<sup>2</sup> un trattato sui fatti illeciti.

In quel periodo, i sistemi di common law ponevano l'attenzione già sulla tecnologia dell'informazione e della comunicazione con l'avvento della carta stampata, delle macchine rotative e si avvertiva l'esigenza di una tutela forte dell'individuo da un uso non corretto della tecnologia. Partendo dall'esegesi del concetto, in Italia si è iniziato a comprendere la necessità di una tutela forte del singolo con le prime divulgazioni mediante mezzi di comunicazione di massa di fatti e informazioni relative a persone famose<sup>3</sup>.

---

<sup>1</sup> Si legge nell'articolo: "*(...) Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the rooftops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.*"

<sup>2</sup> T. COOLEY, *A treatise on the Law of Torts or the Wrongs which arise independent of contracts*, 1888, University of Michigan Law School.; A. BALDASSARRE, *Privacy e costituzione: L'esperienza statunitense*, Roma, 1974; V. MAYER SCHONBERGER, *Delete: the virtue of forgetting in the digital age*, Princeton University Press 2009.

<sup>3</sup> Per un approfondimento sui sistemi di common law vedasi V. VARANO - V. BARSOTTI, *La tradizione giuridica occidentale, testo e materiali per un confronto civil law common law*, settima edizione, Giappichelli Editore, Torino, 2021; C. COLAPIETRO, *The impact of the information and technology revolution on constitutional rights with particular attention to personal data protection issues*, in M. BELOV (a cura di), *Information and Technology Revolution and its impact on State, Constitutionalism and Constitutional Law*, London, 2020.

Nel 1956, la Corte di cassazione<sup>4</sup> negava l'esistenza di un vero e proprio diritto alla riservatezza sostenendo esplicitamente che *“nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati in modo diverso i singoli diritti soggettivi della persona pertanto non è vietato comunicare vicende della vita altrui quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto.”*

Tuttavia, successivamente, si è avvertita l'esigenza di un cambio di orientamento e la Corte di cassazione<sup>5</sup> inizia a pensare alla riservatezza non tanto come diritto tipico ma come diritto assoluto di personalità inteso quale diritto erga omnes alla libertà di autodeterminazione del singolo.

Infatti, afferma che *“viola il diritto assoluto di personalità la divulgazione di notizie relative alla vita privata in assenza di un consenso quantomeno implicito e laddove non esista per la natura dell'attività svolta dalla persona e del fatto divulgato un preminente interesse pubblico alla conoscenza”*.

Un ulteriore passo della giurisprudenza verso una tutela forte è stato fatto dal 1975 in poi con un orientamento più consolidato e omogeneo<sup>6</sup> in cui viene riconosciuto che l'ordinamento tutela e riconosce l'interesse di tutti a che non siano resi noti fatti o avvenimenti di carattere riservato senza il consenso, in particolare con il noto caso *Soraya*<sup>7</sup>. La sentenza<sup>8</sup> è di particolare rilievo poiché ha espressamente affermato che *“il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente*

---

<sup>4</sup> Corte di cassazione, 22 dicembre 1956, n. 4487.

<sup>5</sup> Corte di cassazione, 20 aprile 1963, n. 990.

<sup>6</sup> Corte di cassazione, 5 aprile 1978 n. 1557, Corte di cassazione, 13 marzo 1985, n. 1968

<sup>7</sup> Corte di cassazione, 27 maggio 1975, n. 2129

<sup>8</sup> Il noto caso di cronaca era sorto tra l'imperatrice Soraya Esfandiary contro dei giornali che avevano pubblicato alcune fotografie che ritraevano la stessa all'interno della propria dimora con un uomo in atteggiamenti privati e intimi.

*apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti.*

Nel 1970 il diritto alla privacy ha il suo primo riconoscimento legislativo nello Statuto dei lavoratori<sup>9</sup> dove la privacy entra nell'ordinamento mediante una tutela speciale accordata al diritto della classe operaia<sup>10</sup>.

Ciò ha determinato un primo cambiamento culturale di un'epoca volta ad accogliere la consapevolezza del rischio di un abnorme uso delle informazioni personali come strumento di discriminazione politica dei lavoratori.

A questo punto, occorre analizzare il piano costituzionale in un ordinamento dove il legislatore costituente non aveva previsto esplicitamente una tutela forte del diritto alla riservatezza che nei paesi di common law si andava via via affermando e consolidando sempre di più.

Ebbene, ancora oggi, la Costituzione italiana non prevede espressamente un diritto alla riservatezza, inteso anche come diritto alla vita privata in quanto tale.

Nell'ordinamento italiano il passo più importante è stato compiuto nel momento in cui si è riconosciuto che l'articolo 2 della Costituzione<sup>11</sup> è una fattispecie aperta idonea a garantire una tutela anche a quei diritti che non sono espressamente tutelati in modo esplicito dalla Costituzione. L'articolo 2

---

<sup>9</sup> L'articolo 8 della Legge n. 300 del 1970 "Statuto dei lavoratori", prevede che *"al datore di lavoro ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro. È fatto divieto di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali dei lavoratori, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore"*

<sup>10</sup> Si veda S. RODOTÀ, *Riservatezza*, in Enciclopedia Italiana – VI Appendice 2000, treccani.it; S. RODOTÀ, *Tecnologia e diritto*, il Mulino, 2021; S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. CONTI, Editori Laterza, 2005; S. RODOTÀ, R. ZACCARIA, *Diritto dell'informazione e della comunicazione*, Padova, 2007; L. PALADIN, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in *La libertà d'informazione*, a cura di L. Paladin, Torino, 1979; M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Riv. studi. parl. pol. cost.*, 176/2012, 51 ss.; G. Busia, *Riservatezza (diritto alla)*, in *Dig. disc. pubbl.*, agg., 2000.

<sup>11</sup> *La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.*

infatti è una fattispecie in grado di garantire una protezione a nuovi diritti che emergono nei nuovi contesti sociali e politici in relazione anche ai nuovi cambiamenti in itinere che si verificano.

In altri termini, per il tramite dell'articolo 2 della Costituzione, il diritto alla riservatezza è stato ricondotto ai diritti della personalità<sup>12</sup>.

La Corte costituzionale, con la sentenza n. 38 del 12 aprile 1973 riconduce il diritto del singolo al proprio decoro, al proprio onore, alla propria rispettabilità, riservatezza, intimità e reputazione ai diritti inviolabili dell'uomo di cui all'articolo 2 della Costituzione affermati anche negli articoli 3 comma e 13 comma 1<sup>13</sup>.

## 2. Sul labile confine tra riservatezza e privacy

Una volta ritenuto possibile rinvenire una tutela del diritto alla riservatezza indirettamente nella Costituzione, occorre soffermarsi sulla distinzione tra diritto alla riservatezza e diritto alla privacy, spesso ritenute due nozioni coincidenti *tout court*.

Invero, l'accezione originaria della privacy quale riservatezza<sup>14</sup> si era rivelata non idonea a garantire una tutela forte rispetto ai cambiamenti dovuti alla società dell'informazione e della comunicazione elettronica. Infatti, per

---

<sup>12</sup> Sui diritti della personalità vedasi: A. TORRENTE – P. SCHLESINGER, *Manuale di diritto privato*, ventiseiesima edizione, Giuffrè Editore, luglio 2023; F. GAZZONI, *Manuale di diritto privato*, Edizioni scientifiche italiane, 2023.

<sup>13</sup> L'articolo 3 della Costituzione prevede che “*Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese.*” L'articolo 13 comma 1 prevede che “*La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'Autorità giudiziaria e nei soli casi e modi previsti dalla legge.*”

<sup>14</sup> G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), *I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Il Mulino, 2007.

comprendere a pieno la nozione di diritto alla protezione dei dati personali occorre soffermarsi sulle differenze concrete esistenti tra diritto alla privacy che ingloba la protezione dei dati personali e diritto alla riservatezza tout court.

Ciò in quanto, nonostante i due termini siano utilizzati indifferentemente occorre rilevare che tra i due non vi è una coincidenza estrema poiché il diritto alla privacy include il diritto alla riservatezza così come tutelato indirettamente dalla nostra Costituzione ma il diritto alla privacy è molto più ampio della riservatezza, lo ingloba ne costituisce l'essenza e il punto di partenza per arrivare a comprendere l'importanza non solo della sfera del singolo e dunque della privacy come diritto individuale ma anche il rapporto che il soggetto ha verso l'esterno nonché il controllo sulla circolazione dei propri dati.

In altri termini, si è spostata l'attenzione dalla tutela del singolo individuo come *ius excludendi alios* e quindi tutela nella sua sfera privata alla tutela del singolo nel contesto nuovo sociale, politico, influenzato fortemente dalle nuove tecnologie.

Con la diffusione delle tecnologie dell'informazione e della comunicazione diventa sempre più agevole la raccolta e la gestione delle banche dati che trattano i dati personali. Ebbene, superando la sfera privata si è arrivati a configurare il diritto alla protezione dei dati personali come uno strumento efficace e subordinato al fine di garantire la tutela della privacy.

Dunque, la riservatezza deve differenziarsi dalla privacy poiché riguarda il diritto all'intimità dei propri dati personali e nella sfera privata, tutto ciò deve essere salvaguardato da esterne intrusioni affinché si possa consentire al soggetto titolare del suo diritto alla vita privata di escludere gli altri e di essere tutelato nel proprio spazio privato.

La privacy ha un'estensione diversa poliedrica e più ampia. È la *longa manus* della riservatezza, riguarda sempre la tutela del singolo individuo ma non solo

nella sua sfera privata ma con un'estensione verso l'esterno nel contesto sociale. Essa attribuisce al soggetto il diritto di impedire che vengano divulgate informazioni personali nonché di controllare la circolazione dei dati e il trattamento degli stessi. Si estende fino al diritto alla protezione dei dati personali che diventa un diritto alla protezione contro ogni controllo illegittimo e ogni ingerenza altrui, e porta il soggetto ad una autodeterminazione decisionale del soggetto e l'esclusivo controllo sulla circolazione dei propri dati. In ragione di ciò, i caratteri che qualificano la privacy diventano l'autodeterminazione decisionale del soggetto e la sovranità sui propri dati<sup>15</sup>. In definitiva, come si vedrà nel prosieguo dell'analisi, l'introduzione delle tecnologie informatiche ha determinato un grande cambiamento nella tutela dei diritti della personalità. Nello specifico, l'introduzione dei calcolatori ha richiesto e continua oggi, in virtù del veloce progresso, a richiedere l'adozione di specifici meccanismi di tutela non più solo per salvaguardare la sfera privata delle persone ma soprattutto, oggi per rimuovere i rischi relativi al trattamento dei propri dati personali<sup>16</sup>. La rivoluzione digitale ha dunque determinato una modifica dell'oggetto del diritto alla riservatezza tout court, poiché l'ha riconsiderato all'interno del contesto più ampio della privacy alla luce del nuovo diritto al controllo sui propri dati<sup>17</sup>.

Oggi, si ritiene che il diritto alla privacy nella sua visione ampia comprensivo della riservatezza e del diritto alla protezione dei dati personali sia un diritto duttile e dinamico, idoneo a trasformarsi e adattarsi a sfide differenti.

Il diritto ad essere lasciati soli di fine Ottocento come difesa del proprio spazio dal quale poter escludere le intrusioni, diventa il postulato di una libertà di scelta in grado di garantire il diritto ad essere pienamente esponibile dove lo

---

<sup>15</sup> Vedasi, A. WESTIN, *Privacy and freedom*, Atheneum, n.y., 1967.

<sup>16</sup> Così G. PASCUZZI, *Il diritto dell'era digitale*, pag. 82 e ss, Il mulino 2020.

<sup>17</sup> Si veda A. MONTI – R. WACKS, *Protecting personal information, the right to privacy reconsidered*, 30 maggio 2019, Hart Pub Ltd.

sviluppo della tecnologia ha arricchito ancora di più la nozione di privacy arrivando a definirla come diritto all'autodeterminazione informativa<sup>18</sup>. Il controllo del proprio patrimonio di informazioni in cui la persona è esposta ininterrottamente ha richiesto uno strumentario forte di mezzi di tutela al fine di controllare le informazioni costituenti l'identità digitale nella sfera digitale.

### **3. L'influenza delle fonti del diritto dell'Unione europea e della CEDU nell'ordinamento nazionale nell'ambito della protezione dei dati personali.**

Alla luce dell'analisi svolta, per comprendere il sistema dinamico e in *itinere* delle fonti in materia di protezione dei dati personali, occorre analizzare in primo luogo i rapporti tra l'ordinamento europeo con l'ordinamento nazionale per poi analizzare successivamente la natura della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

A seguito degli effetti economici e politici derivanti dai due conflitti mondiali, si avvertì l'esigenza di intraprendere un processo di integrazione europea. Ebbene, sembrava indispensabile individuare un espediente politico per raggiungere un clima di intesa tra gli Stati<sup>19</sup>. L'integrazione dell'ordinamento

---

<sup>18</sup> Così G. CERRINA FERRONI, *Il Ruolo del Garante per la protezione dei dati personali, La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, Il Mulino, Bologna, 2023.

<sup>19</sup> In argomento si sono espressi numerosi autori, W.V. GERVEN, *The European Union a polity of States and Peoples*, Stanford University Press, California, 2005, p.7 e ss.; A.M. CALAMIA – V. VIGIAK, *Diritto dell'Unione Europea*, Giuffrè, Milano, 2018, p.5 e ss.; G.TESAURO, *Diritto dell'Unione Europea*, Cedam, Padova, 2012, p.1 e ss.; L. NEVILLE BROWN – T.KENNEDY, *The Court of Justice of the European Communities*, Sweet and Maxwell, London, 2000, p.2 e ss.; C. AMALFITANO- M. CONDINANZI, *Unione Europea, fonti, adattamento e rapporti tra ordinamenti*, Giappichelli Editore, Torino, 2015, p.1 e ss.; S. WEATHERILL, *Cases and Materials on EU Law*, Oxford University Press, New York, 2007, p.5; F. POCAR, *Diritto dell'Unione Europea*, Giuffrè Editore, Milano, 2010, p.7 e ss.; R. ADAM-A.TIZZANO, *Manuale di diritto dell'Unione Europea*, Giappichelli Editore, Torino, 2017, p.18 e ss.; U.DRAETTA, *Elementi di diritto dell'Unione Europea*, Giuffrè Editore, Milano, 2014, p.7 e ss.; N. BOSCHIERO - T. SCOVAZZI - C. PITEA – C. RAGNI, *International Courts and the Development of International Law – Essays in Honour of Tullio Treves*, Springer - Asser Press, UK, 2013; E. DI SALVATORE, *L'identità costituzionale dell'Unione Europea e degli Stati membri, il decentramento politico – istituzionale nel processo di integrazione*, Giappichelli Editore – Torino, 2008; G. NOLTE, *European and Us Constitutionalism*, Cambridge University Press, 2005.

italiano con l'ordinamento sovranazionale ha determinato una proliferazione di fonti<sup>20</sup>.

In ragione di ciò, si è arrivati a definire l'ordinamento quale “*ordinamento a tutela multilivello*”<sup>21</sup> che da un lato ha comportato maggiori garanzie per gli amministrati, dall'altro lato ha determinato una trasformazione radicale del ruolo dell'interprete. Occorre anticipare preliminarmente che, oggi, il rapporto tra i due ordinamenti è retto dal principio del primato del diritto europeo in virtù del quale, la norma interna in contrasto con il diritto dell'Unione Europea direttamente applicabile dovrà essere disapplicata sia dalla pubblica amministrazione che dal giudice nazionale. Per ripercorrere brevemente le tappe del processo di integrazione europea, occorre fare riferimento alla data del 9 maggio del 1950 quando il Ministro degli Esteri francese Robert Schuman, manifestava il suo interesse ad istituire una Comunità Europea del Carbone e dell'Acciaio attraverso una dichiarazione, nota come la Dichiarazione Schuman mediante l'aiuto di Jeane Monnet nella preparazione e redazione dei testi.

La Dichiarazione ebbe un ruolo particolarmente di rilievo nel processo di integrazione europea<sup>22</sup>, poiché individuava le origini e gli scopi di un percorso comune tra gli Stati e consentiva la partecipazione a tutti i paesi che in concreto decidevano di prendere parte<sup>23</sup>.

---

<sup>20</sup> In argomento si veda M.A. SANDULLI, *I Principi costituzionali e comunitari di giurisdizione amministrativa*, in *Il nuovo processo amministrativo*, a cura di M.A. SANDULLI, Giuffrè Editore, Milano, 2013, p. 29.

<sup>21</sup> Si veda in argomento, M. CARTABIA, *La tutela multilivello dei diritti fondamentali. Il cammino della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in [cortecostituzionale.it](http://cortecostituzionale.it), 2014.

<sup>22</sup> Il fine della Dichiarazione era quello di evitare ulteriori conflitti tra Francia e Repubblica Federale Tedesca concernenti lo sfruttamento di risorse quali il carbone e l'acciaio che, tradizionalmente, avevano rappresentato motivo di contrasto tra le due.

<sup>23</sup> In argomento si veda U.VILLANI, *Istituzioni di Diritto dell'Unione Europea*, Cacucci Editore, Bari, 2017, p. 4; vedasi A.CELOTTO, *L'Italia e l'Unione Europea*, in *Diritto Pubblico*, a cura di F. MODUGNO, Giappichelli Editore, Torino, 2015, p. 218.

Successivamente, il governo francese, decideva di convocare una conferenza intergovernativa volta all'elaborazione di un progetto per un futuro, eventuale, Trattato istitutivo per la Comunità che si sarebbe dovuta istituire.

Invero, il 18 aprile del 1951, gli Stati che avevano preso parte alla conferenza intergovernativa, decidevano di firmare a Parigi il Trattato istitutivo della Comunità europea del carbone e dell'acciaio (CECA), il quale entrava in vigore più di un anno dopo, ossia il 23 luglio del 1952 con una durata della Comunità cinquantennale<sup>24</sup>.

La CECA era dotata di personalità giuridica e aveva una struttura omogenea mediante un'Alta Autorità, un'Assemblea Comune, un Consiglio speciale dei Ministri e una Corte di Giustizia.

Successivamente, il 25 marzo 1957, venivano firmati a Roma sempre dagli stessi sei Stati firmatari della CECA, il Trattato istitutivo della Comunità economica europea (CEE) e il Trattato istitutivo della Comunità europea dell'energia atomica (CEEa o EURATOM) destinati ad entrare in vigore il primo Gennaio del 1958.

Tra gli obiettivi principali del Trattato istitutivo della Comunità economica europea, vi erano la creazione di un mercato comune europeo, un'unione doganale, la libera circolazione delle persone e la creazione di una politica agricola comune.

Tuttavia, il secondo Trattato aveva come scopo principale quello di contribuire alla formazione di industrie nucleari indipendenti con la determinazione di norme uniformi per proteggere i lavoratori<sup>25</sup>.

---

<sup>24</sup> Tra gli obiettivi principali della CECA è opportuno ricordare quello della creazione di un mercato comune dei prodotti carbosiderurgici nel rispetto di condizioni normali di concorrenza e trasparenza dei prezzi oltre che quello della libertà di circolazione dei prodotti e del libero accesso alle fonti di produzione. In sostanza, come emerge dal preambolo del Trattato CECA, si privilegiava un approccio funzionalista al tema dell'integrazione europea.

<sup>25</sup> In argomento vedasi per maggiori approfondimenti, M.P. CHITI, *Diritto Amministrativo Europeo*, Giuffrè Editore, Milano, 2011, p. 34 e ss.

In tale scenario, il momento storico centrale è rappresentato dal Trattato di Maastricht, firmato il 7 febbraio del 1992 dai rappresentanti dei governi dei dodici Paesi membri della CEE, entrava in vigore soltanto nel novembre del 1993. Inizialmente, tale Trattato, non sostituì le tre Comunità originarie (CECA, CEE ed EURATOM) ma le ricomprese istituendo forme di collaborazione tra gli Stati membri in materia di politica estera, sicurezza comune (istituendo la PESC), giustizia e affari interni (GAI)<sup>26</sup>.

Conosciuto anche come Trattato sull'Unione Europea, contiene 252 articoli con 17 protocolli e 31 dichiarazioni.

La sua rilevanza è innegabile anche per la creazione di una Moneta Unica, avendo delineato le condizioni necessarie per la sua adozione, quali l'andamento dell'inflazione e dei tassi di interesse.

Con l'istituzione dell'Unione Europea si modificarono anche gli obiettivi principali, non più solo economici, ma anche politici con una nuova visione anche ai diritti fondamentali tutelati dalla Convenzione Europea dei diritti dell'Uomo<sup>27</sup>.

Successivamente, nell'ottobre del 1997, veniva ratificato il Trattato di Amsterdam entrato in vigore nel 1999.

---

<sup>26</sup> Per un maggior approfondimento del tema si veda, C. KOENIG- A. HARATSCHB - M. BONINI, *Diritto Europeo*, Giuffrè Editore, 2000, p.4; U. VILLANI, *Istituzioni di diritto dell'Unione Europea*, cit., p. 18; G. STROZZI - R. MASTROIANNI, *Diritto dell'Unione Europea parte istituzionale*, Giappichelli Editore, Torino, 2013, p.11 e ss.; F. POLITI, *Temi di diritto dell'Unione Europea*, Giappichelli Editore, Torino, 2015, p.28; J.H. JANS – R. DE LANGE – S. PRECHAL – R.J.G.M. WIDDERSHOVEN, *Europeanisation of Public Law*, Europa Law Publishing, 2007.

<sup>27</sup> Sulla CEDU si vedano gli scritti di N. RONZITTI, *Introduzione al diritto internazionale*, Giappichelli Editore, Torino, 2013, p. 313; S. BARTOLE – P. DE SENA – V. ZAGREBELSKY *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2012; A. ROYER, *Le Conseil d'Europe*, Les essentiels Milan, 2009; C. ZANGHÌ, *Diritto delle organizzazioni internazionali*, Giappichelli Editore, Torino, 2013; M. ALLENA, *Art 6 CEDU, procedimento e processo amministrativo*, Editoriale Scientifica, Napoli, 2012; G. RAIMONDI, *Il consiglio d'europa e la convenzione europea dei diritti dell'uomo*, Editoriale Scientifica, Napoli, 2009; U. DRAETTA-M.F. MERAVIGLIA, *Il diritto delle organizzazioni internazionali, parte speciale*, Giuffrè Editore, Milano, 2011, p.359 e ss; *Convenzione Europea dei diritti dell'Uomo e delle libertà fondamentali* in [treccani.it](http://treccani.it) ; R. ROMBOLI, *La influenza della Cedu e della giurisprudenza della Corte Europea dei diritti umani nell'ordinamento Costituzionale italiano*, dicembre 2018, in [giurcost.org](http://giurcost.org); R. DICKMANN, *Corte Costituzionale e diritto internazionale nel sindacato delle leggi per contrasto con l'articolo 117 primo comma della Costituzione* in [federalismi.it](http://federalismi.it).

Esso, accentuava la connotazione politico-sociale dell'Unione, proclamando tra i suoi principi fondanti quelli di libertà, democrazia, rispetto dei diritti umani e dello stato di diritto.

Nella stessa ottica va letta l'emanazione della Carta dei diritti fondamentali dell'Unione Europea<sup>28</sup> tenutasi a Nizza, nel dicembre del 2000.

La Carta ha lo stesso valore giuridico dei Trattati nonostante inizialmente fosse considerata priva di efficacia giuridica vincolante<sup>29</sup>.

Infine, un elemento fondamentale per il processo di integrazione europea si raggiunse quando il primo dicembre del 2009 entrò in vigore il Trattato di Lisbona<sup>30</sup> firmato da tutti gli Stati membri dell'Unione Europea.

Venne istituito per modificare sia il Trattato sull'Unione Europea che il Trattato istitutivo della Comunità Europea al quale venne modificato il nome in «Trattato sul funzionamento dell'Unione Europea».

Entrambi costituiscono i Trattati su cui si fonda l'Unione Europea<sup>31</sup> considerati fonte primaria.

L'ordinamento giuridico dell'Unione Europea trova dunque le proprie fondamenta nei Trattati, nei principi generali del diritto e nella Carta Dei diritti

---

<sup>28</sup> Per approfondimenti sul tema si veda V. PICCONE- O. POLLICINO, *La carta dei diritti fondamentali dell'Unione Europea efficacia ed effettività*, Editoriale Scientifica, Napoli, 2018; R. MASTROIANNI- O. POLLICINO- S. ALLEGREZZA- F. PAPPALARDO- O. RAZZOLINI , *Carta dei diritti fondamentali dell'Unione Europea*, Giuffrè Editore, Milano.

<sup>29</sup> *Essa garantisce un insieme di diritti (civili, politici) dei cittadini europei ed è composta da 54 articoli e da un preambolo*, in [treccani.it](http://treccani.it)

<sup>30</sup> Vedasi M. FRAGOLA, *Il Trattato di Lisbona che modifica il trattato sull'Unione Europea e il Trattato della Comunità Europea, versione ragionata e sistematica per una consultazione coordinata degli articoli alla luce dei Protocolli e delle Dichiarazioni*, Giuffrè Editore, Milano, 2010; P. BILANCIA- M. D'AMICO, *La nuova Europa dopo il trattato di Lisbona*, Giuffrè Editore, Milano, 2009; E. CHITI – B.G. MATTARELLA, *Global Administrative Law and Eu Administrative Law, Relationship, Legal issues and Comparison*, Springer, 2011; S. R. BEDI, *The development of Human Rights Law by the Judges of the International Court of Justice – Studies in International Law*, Hart Publishing – Oxford – Portland Oregon, 2007; F. BIONDI, *Quale dialogo tra le Corti?*, in [Federalismi.it](http://Federalismi.it), 2019.

<sup>31</sup> Sul tema si vedano in particolare gli approfondimenti di G. PASQUALI, *Le novità del Trattato di Lisbona*, Edizioni Nuova Cultura, Roma, 2010; V.M. BRESCIA, *Le competenze dell'Unione Europea nel Trattato di Lisbona*, Edizioni scientifiche italiane, Roma, 2008; A. ADINOLFI, *I fondamenti del diritto dell'UE nella giurisprudenza della Corte di Giustizia: il rinvio pregiudiziale*, in *Il dir. un. eur.*, 2019; R. BIFULCO, *La Costituzione Italiana dopo il Trattato di Lisbona*, in *Riv. it. dir. pubbl. comunit.*, 2012; E. CANNIZZARO, *Sui rapporti tra sistemi processuali nazionali e diritto dell'Unione Europea*, in *Dir. un. eur.*, 2008.

fondamentali avente lo stesso valore giuridico dei Trattati. I due Trattati assumono pari valore sul piano giuridico ma sul piano funzionale il TFUE svolge un ruolo strumentale essendo volto ad integrare la disciplina generale stabilita nel TUE. Entrambi, possono essere sottoposti a procedure di revisione ordinaria o semplificata.

La prima ha un campo applicativo generale che comprende la riduzione nonché l'allargamento delle competenze dell'Unione Europea mentre la seconda è una procedura di revisione volta a modificare le singole disposizioni specifiche dei Trattati.

Occorre sottolineare che le norme dei Trattati oltre a vincolare gli Stati possono produrre un effetto diretto nell'ordinamento statale laddove siano sufficientemente chiare incondizionate e precise.

Tra le fonti secondarie o anche conosciute come fonti di diritto derivato invece, l'ordinamento dell'Unione Europea, rinviene i regolamenti, le direttive e le decisioni.

Con specifico riguardo ai regolamenti, essi sono atti a portata generale nel senso che i destinatari non sono individuabili a priori poiché sono rivolti a categorie di soggetti che sono determinati in astratto e non in concreto. Inoltre, essi sono obbligatori in tutti i loro elementi e sono direttamente applicabili in ciascuno Stato membro.

La caratteristica principale, infatti, è data dall'obbligatorietà integrale nel senso che il regolamento deve essere applicato in modo completo. Ebbene, gli Stati non possono andare ad escludere l'applicazione di alcune disposizioni contenute nel regolamento oppure limitarne l'applicazione poiché lo stesso produce i suoi effetti diretti senza che sia necessario un atto di recepimento interno come per le direttive. In altri termini si verifica un adattamento immediato e diretto. In ragione di ciò, il regolamento arriva ad assumere un ruolo di fonte del diritto anche nell'ordinamento nazionale dello Stato membro in cui è direttamente applicabile. Nel proseguio dell'analisi sarà possibile

verificare in concreto il recepimento diretto del GDPR nell'ordinamento nazionale analizzando anche la disciplina precedente interna che opera contestualmente ad esso nell'ordinamento nazionale.

Le Direttive invece hanno la caratteristica di vincolare gli Stati membri con riferimento al risultato da raggiungere, lasciandoli però liberi di individuare la forma e i mezzi idonei per conseguire quel determinato risultato vincolato.

Essa, non è dotata di efficacia diretta come i regolamenti ma può produrre effetti giuridici negli ordinamenti interni anche in mancanza di misure di attuazione da parte degli Stati membri laddove ricorrano determinati presupposti quali: la sufficiente precisione del contenuto normativo e la scadenza del termine per il recepimento della direttiva sul piano nazionale. Inoltre, tra gli atti vincolanti occorre dare atto delle decisioni, esse sono disciplinate dall'articolo 288, co. 4 TFUE il quale prevede che *“la decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi”*. Infine, le raccomandazioni e i pareri sono atti privi di forza vincolante che consistono in un invito allo Stato membro a tenere un comportamento per quanto riguarda la raccomandazione mentre il parere è un punto di vista dell'Unione con riferimento ad una determinata questione.

Con riferimento ai principi, il Trattato sul Funzionamento dell'Unione Europea prevede esplicitamente competenze esclusive<sup>32</sup> e competenze

---

<sup>32</sup> L'Articolo 2 del TFUE prevede che *“Quando i trattati attribuiscono all'Unione una competenza esclusiva in un determinato settore, solo l'Unione può legiferare e adottare atti giuridicamente vincolanti. Gli Stati membri possono farlo autonomamente solo se autorizzati dall'Unione oppure per dare attuazione agli atti dell'Unione. Quando i trattati attribuiscono all'Unione una competenza concorrente con quella degli Stati membri in un determinato settore, l'Unione e gli Stati membri possono legiferare e adottare atti giuridicamente vincolanti in tale settore. Gli Stati membri esercitano la loro competenza nella misura in cui l'Unione non ha esercitato la propria. Gli Stati membri esercitano nuovamente la loro competenza nella misura in cui l'Unione ha deciso di cessare di esercitare la propria. Gli Stati membri coordinano le loro politiche economiche e occupazionali secondo le modalità previste dal presente trattato, la definizione delle quali è di competenza dell'Unione. L'Unione ha competenza, conformemente alle disposizioni del trattato sull'Unione europea, per definire e attuare una politica estera e di sicurezza comune, compresa la definizione progressiva di una politica di difesa comune. In taluni settori e alle condizioni previste dai trattati,*

concorrenti tra ordinamenti alla luce dei principi di proporzionalità e sussidiarietà.

Secondo il principio di attribuzione, l'Unione Europea agisce nei limiti delle competenze che le sono attribuite dai Trattati.

L'Unione ha competenza esclusiva in determinati settori specifici individuati dall'articolo 3 del TFUE<sup>33</sup>.

Inoltre, l'articolo 4 individua le materie in cui essa ha una competenza concorrente con gli Stati Membri<sup>34</sup>.

Il richiamo ai principi di proporzionalità e sussidiarietà è espressamente effettuato dall'articolo 5 del TUE, il quale, chiarisce che in presenza di una competenza concorrente l'esercizio delle funzioni normative deve avvenire nel rispetto dei principi di proporzionalità e sussidiarietà<sup>35</sup>.

---

*L'Unione ha competenza per svolgere azioni intese a sostenere, coordinare o completare l'azione degli Stati membri, senza tuttavia sostituirsi alla loro competenza in tali settori. Gli atti giuridicamente vincolanti dell'Unione adottati in base a disposizioni dei trattati relative a tali settori non possono comportare un'armonizzazione delle disposizioni legislative e regolamentari degli Stati membri. La portata e le modalità d'esercizio delle competenze dell'Unione sono determinate dalle disposizioni dei trattati relative a ciascun settore.*"

<sup>33</sup> L'Articolo 3 del TFUE prevede che "L'Unione ha competenza esclusiva nei seguenti settori: a) unione doganale; b) definizione delle regole di concorrenza necessarie al funzionamento del mercato interno; c) politica monetaria per gli Stati membri la cui moneta è l'euro; conservazione delle risorse biologiche del mare nel quadro della politica comune della pesca; e) politica commerciale comune. L'Unione ha inoltre competenza esclusiva per la conclusione di accordi internazionali allorché tale conclusione è prevista in un atto legislativo dell'Unione o è necessaria per consentirle di esercitare le sue competenze a livello interno o nella misura in cui può incidere su norme comuni o modificarne la portata.

<sup>34</sup> Vedi l'articolo 4 del TFUE, il quale afferma che "L'Unione ha competenza concorrente con quella degli Stati membri quando i trattati le attribuiscono una competenza che non rientra nei settori di cui agli articoli 3 e 6. L'Unione ha una competenza concorrente con quella degli Stati membri nei principali seguenti settori: a) mercato interno; b) politica sociale, per quanto riguarda gli aspetti definiti nel presente trattato; c) coesione economica, sociale e territoriale; d) agricoltura e pesca, tranne la conservazione delle risorse biologiche del mare; e) ambiente; f) protezione dei consumatori; g) trasporti; h) reti transeuropee; i) energia; j) spazio di libertà, sicurezza e giustizia; k) problemi comuni di sicurezza in materia di sanità pubblica, per quanto riguarda gli aspetti definiti nel presente trattato. Nei settori della ricerca, dello sviluppo tecnologico e dello spazio, l'Unione ha competenza per condurre azioni, in particolare la definizione e l'attuazione di programmi, senza che l'esercizio di tale competenza possa avere per effetto di impedire agli Stati membri di esercitare la loro. Nei settori della cooperazione allo sviluppo e dell'aiuto umanitario, l'Unione ha competenza per condurre azioni e una politica comune, senza che l'esercizio di tale competenza possa avere per effetto di impedire agli Stati membri di esercitare la loro.

<sup>35</sup> Sul tema vedasi M.A. SANDULLI, *Principi e regole dell'azione amministrativa*, Giuffrè Francis Lefebvre, 2020, pp.107 e ss.

Nello specifico, nel rispetto di tali principi sopra menzionati, la funzione legislativa spetta in primo luogo allo Stato membro che si trova in una posizione di massima vicinanza ai cittadini come accade nel riparto di competenze tra Stato e Regioni laddove i Comuni sono in una posizione di vicinanza maggiore al cittadino.

Ebbene, il rispetto dei principi di sussidiarietà e proporzionalità evoca un ordinamento in cui nella peculiare ipotesi in cui lo Stato membro non è in grado di garantire i principi e gli obiettivi prefissati dell'azione, l'Unione Europea dovrà intervenire a sostenere lo Stato fissando gli obiettivi e regolamentando esclusivamente a livello europeo<sup>36</sup>.

Per comprendere l'essenza dei rapporti tra ordinamento europeo<sup>37</sup> e nazionale un ruolo fondamentale è stato svolto dalla Corte di Giustizia dell'Unione Europea (art. 19 TFUE), che esercita la funzione giurisdizionale in forza della quale garantisce il rispetto del diritto dell'Unione Europea nell'interpretazione e nell'applicazione dei Trattati da parte degli Stati membri<sup>38</sup>.

La Corte ha sede a Lussemburgo ed è formata da un giudice per ogni Stato membro, coadiuvata da avvocati generali indipendenti, imparziali, nominati dai governi nazionali con un mandato rinnovabile di sei anni.

Di rilievo è il fatto che il Tribunale e la Corte di Giustizia non si pongono sullo stesso piano in virtù delle diverse competenze stabilite dai Trattati e dal relativo Statuto della Corte di Giustizia.

---

<sup>36</sup> Per ulteriori approfondimenti si veda V. LOPILATO, *Manuale di diritto amministrativo*, parte generale, terza edizione, Giappichelli Editore, 2021, pp. 156 e ss.

<sup>37</sup> L'articolo 13 del TUE lascia intendere che l'Unione Europea dispone di un quadro istituzionale ben delineato dove «ciascuna istituzione agisce nei limiti delle attribuzioni che le sono conferite dai Trattati secondo le procedure, condizioni, finalità da essi previste».

<sup>38</sup> Tra gli scritti più rilevanti relative alla Corte di Giustizia vedasi T. BALLARINO, *Diritto dell'Unione Europea*, Cedam, Padova, 2010, p. 173; R. DEHOUSSE, *The European Court of Justice*, European Union Series, New York, 1998 ; G.D. BÛRCA-J.H.H. WEILER, *The European Court of Justice*, Oxford University Press, Oxford; G. CAGGIANO, *La Corte di Giustizia difende il principio del primato a fronte della ribellione delle corti costituzionali di Polonia, Ungheria e Romania*, in *Studi sull'integrazione europea*, Cacucci Editore, 2021, pp.473 e ss; si veda V. LOPILATO, *Manuale di diritto amministrativo*, parte generale, terza edizione, Giappichelli Editore, 2021, pp. 158 e ss.

Invero, il Tribunale nello specifico è competente in primo grado per l'annullamento degli atti dell'Unione (263 TFUE) se il ricorrente è una persona giuridica o fisica, è competente per il ricorso in carenza (265 TFUE), azione di risarcimento danni contro l'Unione (268 TFUE) e ai sensi dell'articolo 270 (TFUE) è competente in caso di controversie tra Unione e i suoi agenti.

Tuttavia, per alcune competenze attribuite al Tribunale vige un doppio grado di giudizio anche dinnanzi alla Corte di giustizia, mentre alcune competenze sono esclusive di essa.

Ebbene, la Corte ha competenza per l'annullamento degli atti dell'Unione ai sensi dell'articolo 262 del TFUE in forza del quale *«la Corte di Giustizia esercita un controllo di legittimità sugli atti legislativi delle istituzioni e sugli atti degli organismi dell'Unione destinati a produrre effetti giuridici nei confronti dei terzi»*.

In secondo luogo, tra le competenze della Corte occorre menzionare il ricorso in carenza (265 TFUE) esercitabile nei casi in cui, in violazione dei Trattati, *«il Parlamento Europeo, il Consiglio Europeo, il Consiglio, la Commissione o la Banca Centrale si astengono dal pronunciarsi»*.

Nei menzionati casi, le altre Istituzioni possono adire la Corte di Giustizia dell'Unione Europea al fine di far valere tale violazione.

Tra le competenze esclusive della Corte di Giustizia è anche quella relativa alle procedure d'infrazione sollevate nei confronti di Stati membri (artt. 258-260 TFUE), che può essere promossa sia dalla Commissione sia da uno Stato membro.

In origine la Corte di Giustizia era l'unica Istituzione dell'Unione Europea ad esercitare la funzione giurisdizionale.

La Corte di Giustizia, definita «*Guardiana dei Trattati*»<sup>39</sup>, garantisce ai sensi dell'articolo 267 TFUE l'uniforme interpretazione dei Trattati, assicurando altresì il rispetto della Carta dei Diritti Fondamentali dell'Unione Europea, avendo oggi, ai sensi del nuovo art 6 TUE lo stesso valore giuridico dei Trattati.

I Trattati istitutivi dell'Unione Europea hanno comportato dunque un trasferimento dei poteri sovrani dagli Stati membri alle Istituzioni Europee.

Gran parte degli Stati, ad esclusione dell'Italia e di pochi altri, diedero esecuzione a tali Trattati con norme costituzionali in modo da rendere conciliabile il trasferimento dei propri poteri con le rispettive Costituzioni<sup>40</sup>.

Ciononostante, in Italia la situazione fu molto diversa, poiché l'ordine di esecuzione dei Trattati si fece con legge ordinaria e non con legge costituzionale.

Di conseguenza, mancava una clausola esplicita di riconoscimento, ossia una giustificazione valida per garantire la prevalenza del diritto Europeo sulle fonti nazionali.

Per meglio comprendere l'incrinato rapporto tra ordinamento interno e ordinamento sovranazionale, si ritiene opportuno richiamare brevemente i concetti di dualismo e monismo – ovviamente riferiti all'ordinamento giuridico – come teorizzati da Hans Kelsen. Ebbene, occorre distinguere il sistema monista dal sistema dualista sin dalle origini.

Infatti, seguendo un approccio monista «*i due complessi di norme apparentemente diversi possono costituire un sistema unitario o perché un ordinamento può trovare nell'altro il fondamento della sua validità, oppure attraverso un'equiparazione tra i due ordinamenti*»<sup>41</sup>.

---

<sup>39</sup> Espressione utilizzata da G. GERIN, *La Corte di Giustizia delle Comunità Europee*, Cedam, Padova, 2010, p. 34.

<sup>40</sup> Si veda U. VILLANI, *Istituzioni di diritto dell'Unione Europea*, cit., p. 431.

<sup>41</sup> Afferma H. KELSEN, *Lineamenti di dottrina pura del diritto*, Piccola Biblioteca Einaudi, Torino, 1952, p.155.

Propendendo invece per un approccio dualista, gli ordinamenti giuridici devono essere considerati come autonomi e separati, dunque posti su due piani diversi.

L'approccio dualista di Kelsen secondo parte della dottrina<sup>42</sup> ha inciso profondamente nei rapporti tra ordinamenti determinando anche conseguenze sempre più concrete.

Ebbene, la produzione di effetti giuridici da parte dell'ordinamento sovranazionale nel contesto interno è stata la conseguenza di un'apertura dello Stato italiano verso l'ordinamento europeo determinato da una posizione sovraordinata in virtù del riconoscimento come sistema giuridico autonomo e separato.

#### **4. Il ruolo della CEDU**

Sul piano internazionale, appare opportuno analizzare la natura della Convenzione Europea dei diritti dell'Uomo e delle libertà fondamentali per poi verificare l'incidenza della stessa sul trattamento dei dati personali. La Convenzione, rileva soprattutto per il grande passo compiuto verso la tutela dei diritti fondamentali. Il Consiglio d'Europa<sup>43</sup> è un'organizzazione internazionale fondata il 5 maggio del 1949 con il Trattato di Londra. Ha sede a Strasburgo, non ha poteri normativi ed è costituito da un Comitato dei Ministri, dal Segretario Generale e da un'Assemblea Consultiva composta dai parlamentari degli Stati membri. L'Assemblea adotta raccomandazioni e risoluzioni. Ad oggi i membri sono 47, di cui 28 fanno parte anche dell'Unione Europea. Nonostante i diritti fondamentali, ricevessero già una

---

<sup>42</sup> Vedasi G. PALMISANO, *Il Sistema giuridico internazionale e l'ordinamento comunitario*, 2012, in *treccani.it*.

<sup>43</sup> La letteratura in materia è vastissima, A. ROYER, *Le Conseil d'Europe*, Les essentiel Milan, 2009; G. RAIMONDI, *Il consiglio d'europa e la convenzione europea dei diritti dell'uomo*, Editoriale Scientifica, Napoli, 2009; C. ZANGHÌ, *Diritto delle organizzazioni internazionali*, Giappichelli Editore, Torino, 2013; U. DRAETTA - M.F. MERAVIGLIA, *Il diritto delle organizzazioni internazionali, parte speciale*, Giuffrè Editore, Milano, 2011, p.359 e ss.

copertura costituzionale all'interno dei singoli ordinamenti, ad esempio in Italia, l'articolo 2 della Costituzione, fattispecie aperta, stabiliva che «*la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità*», nel 1950 venne adottata, da parte di tutti gli Stati membri del Consiglio d'Europa, la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali<sup>44</sup>.

È un Trattato internazionale e la sua essenza è rappresentata dalla tutela dei diritti e delle libertà fondamentali che si esplica attraverso l'individuazione di una «*soglia minima comune*» che vada a temperarsi con le garanzie costituzionali di ogni Stato membro<sup>45</sup>.

La Convenzione può essere analizzata individuando due parti connesse tra loro.

Una prima parte, di natura sostanziale, nella quale sono indicati tutti i diritti garantiti; nella seconda parte, avente natura processuale, vengono identificate le modalità di tutela di tali diritti<sup>46</sup>.

Tuttavia, nel tempo è stata modificata ed integrata attraverso la redazione di numerosi Protocolli<sup>47</sup>.

Come noto, il controllo giudiziario circa il rispetto della Convenzione è effettuato dalla Corte Europea dei diritti dell'uomo, avente sede a

---

<sup>44</sup> Si veda R. ROMBOLI, *La influenza della Cedu e della giurisprudenza della Corte Europea dei diritti umani nell'ordinamento Costituzionale italiano*, dicembre 2018, in giurcost.org; inoltre vedasi voce *Convenzione Europea dei diritti dell'Uomo e delle libertà fondamentali* in treccani.it ;

<sup>45</sup> In argomento V. LOPILATO, *Manuale di diritto amministrativo*, cit., p. 151; in particolare, l'Autore richiama (nella nota 73) la Corte Cost. N. 43/2017 ; C. COLAPIETRO - M. RUOTOLO, *Diritti e Libertà in Diritto Pubblico*, a cura di F. MODUGNO, cit, p. 641 e ss.

<sup>46</sup> Si veda N. RONZITTI, *Introduzione al diritto internazionale*, Giappichelli Editore, Torino, 2013, p. 313.

<sup>47</sup> In particolare, il Protocollo n.11 del 1998, poi modificato con il Protocollo n.14 del 2010, ha istituito una Corte unica stravolgendo il meccanismo di garanzia che precedentemente era affidato al Comitato dei Ministri del Consiglio d'Europa, alla Commissione e alla Corte Europea dei Diritti dell'Uomo.

Strasburgo<sup>48</sup>. Un'ulteriore differenza rispetto agli altri Trattati internazionali è data dalla previsione di un sistema oggettivo di tutela non basato sul principio di reciprocità, bensì in una duplice attitudine. Invero, al suo interno, la Convenzione Europea dei Diritti dell'Uomo e delle Libertà Fondamentali, contiene delle disposizioni ben precise relative alla possibilità di esperire ricorso alla Corte Europea dei Diritti dell'Uomo.

Difatti, ai sensi dell'art 33 della Convenzione, il ricorso può essere presentato da uno Stato membro contro un altro Stato membro, quest'ultimo, rubricato *ricorso interstatale* è ammesso nei casi in cui quest'ultimo abbia violato un diritto contenuto all'interno della Convenzione stessa. Inoltre, ai sensi dell'art 34 della Convenzione, il ricorso alla Corte Europea può essere proposto anche da «una persona fisica, un'organizzazione non governativa o gruppo di individui» contro lo Stato al quale appartiene, a patto che dimostri di essere «vittima di una violazione della Convenzione da parte dello Stato»<sup>49</sup>. Presupposto fondamentale, sia per il ricorso individuale che per il ricorso interstatale, è ai sensi dell'articolo 35 della Convenzione, «il previo esaurimento dei ricorsi interni». Infatti, il rapporto tra la Corte di Strasburgo e i giudici interni, è basato sul principio di sussidiarietà, ove spetta *in primis* alle istituzioni degli Stati membri la tutela dei diritti fondamentali, la Corte Edu potrà essere adita esclusivamente dopo l'esaurimento di tutte le vie di ricorso nazionale in un termine di sei mesi dall'adozione della decisione interna finale. Invero, la Cedu è nata proprio come “strumento *sussidiario di tutela*”<sup>50</sup>. Occorre sottolineare il fatto che la Corte Edu non è obbligata ad accettare tutti

---

<sup>48</sup> La Corte d'Europa è composta da 47 giudici eletti dall'Assemblea Parlamentare del Consiglio d'Europa con un mandato non rinnovabile di 9 anni. Nel 1998 vi è stata una riforma che ha modificato la precedente suddivisione; ad oggi si ha un Giudice unico il quale ha il compito di esaminare i ricorsi irricevibili, un Comitato di tre giudici che normalmente decide all'unanimità sulla ricevibilità del ricorso, la Camera di sette giudici e la Grande Camera di diciassette giudici la quale agisce solo in casi eccezionali.

<sup>49</sup> Così P.V. DASTOLI, *Corte Europea dei diritti dell'Uomo*, in [treccani.it](http://treccani.it)

<sup>50</sup> Espressione utilizzata da C. MASCIOTTA in *Il ricorso diretto a Strasburgo in deroga al principio del previo esaurimento, ex art 35 cedu : un possibile cortocircuito tra sistema costituzionale e convenzionale di tutela?* In [osservatoriosullefonti.it](http://osservatoriosullefonti.it), 2018.

i ricorsi che le vengono presentati, può respingere il ricorso non conforme alla disposizione in ogni stato del procedimento.<sup>51</sup> Per quanto riguarda l'esecuzione delle sentenze della Corte Edu, il riferimento è agli articoli 46 e 41 della Convenzione. L'art. 46 della Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali rubricato «*Forza vincolante ed esecuzione delle sentenze*», nel par. 1, afferma che «Le Alte Parti contraenti s'impegnano a conformarsi alle sentenze definitive della Corte per le controversie di cui sono parte» 41 della medesima, rubricato «*Equa soddisfazione*» in virtù del quale «*Se la Corte dichiara che vi è stata violazione della Convenzione o dei suoi Protocolli e se il diritto dell'Alta Parte contraente non permette se non in modo imperfetto di rimuovere le conseguenze di tale violazione, la Corte accorda, se del caso, un'equa soddisfazione alla parte lesa*»

Invero, la fase esecutiva sarebbe demandata alla libera discrezionalità degli Stati aderenti, bensì, negli ultimi tempi, la Corte Edu attraverso delle recenti pronunce, ha integrato il significato di queste norme. Nello specifico ha esplicitato che oltre a dover corrispondere l'equa soddisfazione alla parte lesa, nel rispetto dell'articolo 41, potrà essere richiesta inoltre l'adozione di misure generali o individuali sempre volte a far arrestare la violazione e le relative conseguenze. Nel capitolo seguente, si analizzerà dunque l'ipotesi in cui vengano richiesti interventi *ex novo* del legislatore come ad esempio l'ipotesi di riapertura dei processi, mettendo in luce il contenuto “variabile”<sup>52</sup> emerso

---

<sup>51</sup> La Corte non accoglie alcun ricorso inoltrato sulla base dell'articolo 34, se: è anonimo; oppure è essenzialmente identico a uno precedentemente esaminato dalla Corte o già sottoposto a un'altra istanza internazionale d'inchiesta o di risoluzione e non contiene fatti nuovi. La Corte dichiara irricevibile ogni ricorso individuale presentato ai sensi dell'articolo 34 se ritiene che: il ricorso è incompatibile con le disposizioni della Convenzione o dei suoi Protocolli, manifestamente infondato o abusivo; o il ricorrente non ha subito alcun pregiudizio importante, salvo che il rispetto dei diritti dell'uomo garantiti dalla Convenzione e dai suoi Protocolli esiga un esame del ricorso nel merito e a condizione di non rigettare per questo motivo alcun caso che non sia stato debitamente esaminato da un tribunale interno.

<sup>52</sup> Corte Cost. n.123 del 2017.

negli ultimi anni dell'obbligo di conformazione alle sentenze della Corte Edu previsto dall'articolo 46.

Sino alle due sentenze gemelle della Corte Costituzionale (nn. 348 e 349 del 2007) ,in Italia si era assistito ad una situazione controversa, in virtù del fatto che la Cedu era stata collocata tra le fonti ma nonostante questo mancava un appropriato fondamento costituzionale<sup>53</sup>.

Si procederà attraverso un'analisi sistematica di entrambe le sentenze, dove si evidenzierà il fatto che la Corte Costituzionale non ha riconosciuto l'effetto diretto alla Cedu e nonostante la sua natura di fonte internazionale pattizia, per via della modifica all'articolo 117 della Costituzione, si è pervenuti al superamento della teoria che considerava la Cedu legge ordinaria<sup>54</sup>. In particolare, si ritiene necessario prendere le mosse dal differente regime di incompatibilità tra le norme dell'ordinamento interno e quelle appartenenti al diritto dell'Unione Europea<sup>55</sup>, per poi passare all'analisi del rapporto tra le disposizioni interne dell'ordinamento italiano e la Cedu.

Invero, nelle note pronunce *Frontini*<sup>56</sup> e *Granital*<sup>57</sup> , la Corte Costituzionale, per giustificare *l'efficacia diretta* del diritto dell'Unione Europea nell'ordinamento nazionale , aveva fatto perno sull'articolo 11 della Costituzione nella parte in cui stabiliva che «*consente in condizioni di parità con gli altri Stati, le limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le Nazioni, promuove e favorisce le organizzazioni internazionali rivolte a tale scopo*».

---

<sup>53</sup> In argomento si veda F.A. BELLA, *Tra Procedimento e Processo, contributo allo studio delle tutele nei confronti della pubblica amministrazione*, cit., p.217ss; R.ROMBOLI, *la influenza della Cedu e della Giurisprudenza della Corte Europea dei diritti umani nell'ordinamento costituzionale italiano*, in giurcost.org

<sup>54</sup> M.ALLENA, *Art 6 CEDU, procedimento e processo amministrativo*, Editoriale Scientifica, Napoli, 2012, p.27.

<sup>55</sup> L'Unione Europea ha un ordinamento giuridico proprio autonomo e distinto, al quale l'Italia e gli altri Stati partecipano attraverso limitazioni della loro sovranità.

<sup>56</sup> Corte Cost. 8 giugno 1984 n. 170.

<sup>57</sup> Corte Cost. 27 dicembre 1973 n. 183.

Tale articolo, non può essere utilizzato allo stesso modo per attribuire un eventuale effetto diretto alla normativa CEDU nei confronti dell'ordinamento nazionale.

Difatti il primo comma dell'articolo 117<sup>58</sup> della Costituzione, dopo essere stato modificato dalla riforma del titolo V del 2001, ha confermato la concreta distinzione non solo formale, esistente tra i vincoli derivanti da obblighi internazionali e quelli derivanti dall'ordinamento eurounitario. In altri termini esplicita la differenza netta tra sistema Convenzionale ed ordinamento dell'Unione Europea.<sup>59</sup>

Difatti a differenza dell'ordinamento europeo, dalla sentenza n.348/2007 è emerso che *«la Convenzione Edu non crea un ordinamento giuridico sopranazionale e non produce di conseguenza norme direttamente applicabili negli Stati contraenti. Essa è configurabile come un trattato internazionale multilaterale da cui derivano “obblighi” per gli Stati contraenti»*.

Inoltre, nella sentenza gemella 349/2007 si è detto, che l'art. 11 della Costituzione non potrà essere preso in considerazione per la CEDU anche perché *«non è individuabile, con riferimento alle norme pattizie in esame alcuna limitazione della sovranità nazionale»*.

Dopo questo divieto, si è tentato di ancorarsi all'articolo 10 della Costituzione, seppur in questo caso sia emerso che l'articolo in questione, affermando che *«l'ordinamento giuridico italiano si conforma alle norme del diritto internazionale generalmente riconosciute e ne prevede l'adeguamento automatico.»* farebbe riferimento, come dice la sentenza 349 (par.6.1), esclusivamente alla consuetudine ed ai principi generali dell'ordinamento internazionale. Di conseguenza, non potrà essere applicato alla normativa

---

<sup>58</sup> Il primo comma dell'articolo 117 stabilisce che *“La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali.”*

<sup>59</sup> Vedasi G. SILVESTRI, *Le limitazioni della sovranità statale in favore dell'Unione Europea nella giurisprudenza costituzionale – il sistema delle fonti*, a cura di RICCARDO NEVOLA, in [cortecostituzionale.it](http://cortecostituzionale.it).

CEDU, trattandosi di normativa pattizia<sup>60</sup>. Il divieto di utilizzare l'articolo 10 della Costituzione come perno è rinvenibile anche nella sentenza 348, ove si esclude esplicitamente l'applicazione dell'articolo 10 ai trattati internazionali bilaterali e multilaterali<sup>61</sup>.

Nello specifico, attraverso le sentenze gemelle 348 e 349 del 2007, si è arrivati a considerare la CEDU come «*norma di rango sub costituzionale*»<sup>62</sup>. Il giudice a quo, ravvisando un contrasto tra una disposizione nazionale ed una della CEDU, avrà il dovere di provare a risolvere il contrasto in via interpretativa<sup>63</sup>, tuttavia, nel caso in cui la risoluzione del contrasto non sia di semplice soluzione per il giudice interno attraverso questa strada, occorre in questa sede ribadire che egli non potendo disapplicare la normativa interna contrastante con la CEDU, dovrà sollevare questione di legittimità costituzionale per violazione dell'articolo 117, primo comma della Costituzione, considerandola come norma interposta<sup>64</sup> tra la Costituzione e la legge ordinaria.

A questo punto, è importante specificare il compito della Consulta. Invero, quest'ultima dovrà verificare la conformità<sup>65</sup>, sia della normativa nazionale che della norma appartenente alla CEDU, a Costituzione, procedendo nel

---

<sup>60</sup> Si veda G. SILVESTRI, *le limitazioni della sovranità statale in favore dell'Unione Europea nella giurisprudenza costituzionale – il sistema delle fonti*, a cura di RICCARDO NEVOLA, in [cortecostituzionale.it](http://cortecostituzionale.it)

<sup>61</sup> In argomento si veda C. ZANGHÌ, *La Corte Costituzionale risolve un primo contrasto con la Corte Europea dei diritti dell'uomo ed interpreta l'articolo 117 della Costituzione: le sentenze n.348 e 349 del 2007*, in [giurcost.org](http://giurcost.org); C. COLAPIETRO M. RUOTOLO, *Diritti e Libertà* in *Diritto Pubblico*, a cura di F. MODUGNO, *cit.*, p.643.

<sup>62</sup> Si veda D.TEGA, *Le sentenze della Corte Costituzionale nn.348 e 349 del 2007: la CEDU da fonte ordinaria a fonte subcostituzionale del diritto*, in [forumcostituzionale.it](http://forumcostituzionale.it)

<sup>63</sup> il giudice nazionale potrà solo svolgere un attività ermeneutica di conformità rispetto alla normativa internazionale, ricordando in tale contesto che la competenza esclusiva ad interpretare le norme della CEDU appartiene alla Corte Edu

<sup>64</sup> In dottrina e giurisprudenza i contributi sono tantissimi, vedasi A.RUGGERI, *La Cedu alla ricerca di una nuova identità ( sentt. Nn. 348/2007 e 349/2007)*, in [forumcostituzionale.it](http://forumcostituzionale.it); R.DICKMANN, *Corte Costituzionale e diritto internazionale nel sindacato delle leggi per contrasto con l'articolo 117 primo comma della Costituzione* in [federalismi.it](http://federalismi.it); C.NAPOLI, *La nuova collocazione della CEDU nel sistema delle fonti e le conseguenti prospettive di dialogo tra le Corti*, in [forumcostituzionale.it](http://forumcostituzionale.it); G.PILI, *il nuovo smalto costituzionale della Cedu agli occhi della Consulta ( sentt. Nn. 348 e 349 del 2007 )* in [forumcostituzionale.it](http://forumcostituzionale.it); D.TEGA, *Le sentenze della Corte Costituzionale nn.348 e 349 del 2007: la CEDU da fonte ordinaria a fonte subcostituzionale del diritto* in [forumcostituzionale.it](http://forumcostituzionale.it)

<sup>65</sup> In argomento vedasi M.ALLENA, *art 6 CEDU, procedimento e processo amministrativo*, *cit.*, p.28.

senso di garantire la “*compatibilità della norma interposta con la Costituzione e la legittimità della norma censurata rispetto alla stessa norma interposta*”<sup>66</sup>.

In conclusione, occorre tenere sempre a mente che la normativa CEDU non acquista la medesima forza della Costituzione, bensì la va ad integrare, rimanendo ad essa subordinata.

La presenza di più fonti esterne a tutela dei diritti fondamentali ha predisposto come confermato anche dalla Corte Costituzionale<sup>67</sup>, un “*sistema di protezione multilivello*”<sup>68</sup> in mancanza di una effettiva adesione dell’Unione Europea alla CEDU. Sul piano internazionale, La Dichiarazione universale dei diritti umani è stata approvata e proclamata dall’Assemblea Generale delle Nazioni Unite nel 1948. L’articolo 12 prevede che “*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*”. Sulla base di questa previsione legislativa, il diritto alla privacy è stato riconosciuto come diritto fondamentale della persona e dopo soli due anni con l’approvazione della CEDU, viene riconosciuto il rispetto della vita privata e familiare nonché il rispetto del proprio domicilio e della propria corrispondenza<sup>69</sup>. Prima di

---

<sup>66</sup> Corte cost 348 del 2007 par.4.7

<sup>67</sup> La Consulta ha affermato in Corte Cost 80/2011 punto 5.2 che “ alla luce dell’art 6 TUE , dunque, la tutela dei diritti fondamentali nell’ambito dell’Unione europea deriva (o deriverà) da tre fonti distinte: in primo luogo, dalla Carta dei diritti fondamentali (cosiddetta Carta di Nizza), che l’Unione «riconosce» e che «ha lo stesso valore giuridico dei trattati»; in secondo luogo, dalla CEDU, come conseguenza dell’adesione ad essa dell’Unione; infine, dai «principi generali», che – secondo lo schema del previgente art. 6, paragrafo 2, del Trattato – comprendono i diritti sanciti dalla stessa CEDU e quelli risultanti dalle tradizioni costituzionali comuni agli Stati membri. Si tratta, dunque, di un sistema di protezione assai più complesso e articolato del precedente, nel quale ciascuna delle componenti è chiamata ad assolvere a una propria funzione. Il riconoscimento alla Carta di Nizza di un valore giuridico uguale a quello dei Trattati mira, in specie, a migliorare la tutela dei diritti fondamentali nell’ambito del sistema dell’Unione, ancorandola a un testo scritto, preciso e articolato.

<sup>68</sup> nello specifico vedasi V. LOPILATO, *Manuale di diritto amministrativo*, cit, p. 156; M.CARTABIA, *I diritti fondamentali in Europa dopo Lisbona: verso nuovi equilibri?*, in *Giorn.dir.amm.*,2010,p. 211 e ss.

<sup>69</sup> L’articolo 8 della CEDU prevede che: “*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di*

procedere alla trattazione del regolamento, occorre infine evidenziare l'importanza della Carta dei diritti fondamentali e dell'articolo 8<sup>70</sup>. Con il Trattato di Lisbona, tale disposizione ha assunto un'efficacia pari a quella dei trattati e da quel momento il diritto alla protezione dei dati personali è diventato un diritto fondamentale della persona. La Corte Europea dei diritti dell'Uomo, proprio per l'importanza dell'articolo 8 ha aggiornato la Case Law Guide<sup>71</sup> inserendo delle precise indicazioni per l'applicazione di tale disposizione mediante un'attenta analisi giurisprudenziale. Nello specifico, emerge nella guida che le garanzie che fornisce l'articolo 8 della CEDU sono volte ad assicurare lo sviluppo senza interferenze esterne della personalità di un soggetto nei suoi rapporti con gli altri.

## **5. Il Regolamento europeo per la protezione dei dati personali e la lettura contestuale con il Codice della Privacy**

A questo punto dell'analisi, dopo aver analizzato la natura delle fonti europee e internazionali nonché la loro incidenza nell'ordinamento interno secondo differenti modalità, occorre porre in luce l'importanza e il forte impatto che ha avuto nell'ordinamento italiano l'introduzione di un regolamento europeo in materia di trattamento dei dati personali.

La necessità di un regolamento in materia derivava dalla natura della fonte-regolamento, l'unica fonte secondaria idonea ad essere obbligatoria in tutti gli Stati membri ed immediatamente vincolante. Infatti, prima del regolamento, al fine di colmare alcune lacune presenti nella materia, venne adottata la

---

*un'autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.*"

<sup>70</sup> "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."

<sup>71</sup> Guide on article 8 of the European Convention on Human Rights. Right to respect.

Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali. Successivamente venne introdotta un'ulteriore direttiva sull'E-privacy 2002/58/CE sul trattamento dei dati personali alla luce delle nuove esigenze sorte in virtù dell'introduzione dei nuovi mezzi elettronici che però, nonostante sia attualmente in vigore, risultava inadeguata nella regolamentazione della disciplina specifica soprattutto oggi del marketing, e-commerce e servizi di instant messaging che all'epoca non esistevano.

In data 25 maggio 2018 è diventato operativo il Regolamento generale per la protezione dei dati personali (UE) 2016/679, General Data Protection Regulation o GDPR. Come si è visto, il regime previgente si basava su una Direttiva n. 95/46/CE, il cambio di strumento da parte del legislatore europeo ha visto la sua ratio nel voler frenare la confusione normativa in virtù di una direttiva che vincolava lo Stato solo per il risultato da perseguire. Il Regolamento è composto da 173 considerando e 99 articoli che devono essere letti congiuntamente.

Il Regolamento è riuscito ad adeguare la disciplina sul trattamento dei dati personali alle nuove forme di comunicazione, all'era digitale e alle nuove tecnologie.

L'obiettivo centrale è stato quello di fornire un livello molto elevato di protezione dei dati alle persone fisiche e di rimuovere gli ostacoli alla circolazione dei dati personali nel territorio dell'Unione Europea.

Con riferimento alla struttura, gli articoli 2 e 3 del GDPR<sup>72</sup> definiscono l'ambito territoriale e materiale di applicazione con riguardo al trattamento dei

---

<sup>72</sup> L'articolo 2 prevede che "1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. 2. Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico" d) effettuati dalle autorità competenti a fini di

dati sia automatizzato che manuale delle persone fisiche. L'articolo 3 stabilisce un'applicazione effettuata in base al principio della collocazione geografica dei soggetti interessati. Con specifico riguardo ai limiti, occorre rilevare che esso non si applica alle attività che non rientrano nell'ambito applicativo del diritto europeo come le attività relative alla sicurezza nazionale, attività di prevenzione, di indagine, di accertamento o perseguimento dei reati.

L'articolo 4<sup>73</sup> del Regolamento stabilisce le definizioni principali e in particolare individua i soggetti del trattamento, ossia l'interessato che è la persona fisica identificata o identificabile alla quale si riferiscono i dati personali, il titolare del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme

---

*prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. 3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98. 4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.”* L'articolo 3 prevede invece che “1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. (C22) 2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: (C23, C24) a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico. (C25)”

<sup>73</sup> Ai fini del presente regolamento s'intende per:”1) «dato personale»: 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; (C26, C27, C30) 2) «trattamento»: 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 (...)

ad altri determina la finalità e i mezzi del trattamento dei dati personali, il responsabile del trattamento invece è colui che tratta i dati per conto del titolare del trattamento. Il trattamento è ovviamente lecito solo se l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.

Con specifico riguardo ai principi, l'articolo 5 del GDPR<sup>74</sup> richiede in primo luogo il rispetto nel trattamento dei dati da parte del titolare e del responsabile dei principi di liceità, correttezza e trasparenza.

In secondo luogo richiede che i dati, in virtù del principio di minimizzazione siano adeguati, pertinenti e limitati al necessario rispetto alle finalità per le quali sono trattati, inoltre in virtù del principio di integrità e riservatezza, il regolamento prescrive che i dati siano trattati in maniera tale da garantire un'adeguata sicurezza dei dati personali compresa la protezione, mediante misure organizzative e tecniche adeguate.

Il Regolamento, è molto specifico nelle definizioni e proprio per questo consente a tutti di comprendere la ratio della disciplina. Il legislatore europeo ha voluto abbandonare la precedente disciplina presente nella direttiva basata su una distinzione tra la natura privata o pubblica dei soggetti che trattano i dati diventando invece soprattutto rilevante la finalità perseguita con il trattamento. Una modifica importante è stata effettuata con riguardo alla categoria dei dati sensibili e giudiziari. Il nuovo articolo 9 del Regolamento<sup>75</sup>

---

<sup>74</sup> L'articolo 5 si occupa dei principi applicabili al trattamento di dati personali.

<sup>75</sup> L'articolo 9 prevede che "1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (C51) 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52) a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un

oggi li definisce categorie particolari di dati personali mentre l'articolo 10 non fa più riferimento ai dati giudiziari bensì a dati personali relativi a condanne penali e reati. Un concetto particolarmente importante introdotto con il regolamento è il principio di *accountability*, tradotto nel nostro ordinamento come principio di responsabilizzazione dei titolari del trattamento dei dati personali. Tale principio è la struttura base su cui è stato costruito tutto l'impianto del Regolamento. L'*Accountability*<sup>76</sup> non è un concetto nuovo, è legato alla trasparenza, attiene all'obbligo di dover dare conto e rispondere per l'istituzione dei propri compiti. In altri termini, dimostrare che sono state messe in atto una serie di misure e contribuisce a migliorare l'efficacia e

---

*interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56) h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53) i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54) j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (C53) 4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. (C8, C10, C41, C45, C53).*

<sup>76</sup> Gli articoli letti in combinato disposto sono due nel considerando n. 85 e nell'articolo 5 paragrafo 2.

l'efficienza della funzione pubblica. Esso deve essere inteso come uno strumento di semplificazione normativa in cui si rimettono al titolare del trattamento una serie combinata di scelte di cui egli dovrà dare conto. Viene dunque affidato ai titolari il compito di decidere autonomamente le modalità, i limiti e le garanzie del trattamento dei dati personali nel rispetto sempre del regolamento e delle disposizioni interne. È importante che prima di procedere al trattamento dei dati vi sia un'analisi preventiva in modo da poterlo applicare e dimostrare di averlo fatto in un certo modo dunque una protezione dei dati sin dalla progettazione. In altri termini, si ritiene necessaria un'analisi preventiva da parte dei titolari in modo tale da rendere le proprie attività concrete e dimostrabili sin dal principio. I considerando 75 e 77 fanno riferimento espresso al tema del rischio, ossia il rischio inerente al trattamento, dunque un rischio di impatti negativi sulle libertà e sui diritti degli interessati tenendo conto anche delle misure che il titolare deve adottare per mitigare l'insorgenza dei rischi ai sensi degli articoli 35 e 36<sup>77</sup>. In definitiva, tra le novità più importanti di forme di tutela occorre quindi ricomprendere una specifica e rigorosa valutazione del rischio e in particolare su un eventuale o ipotetico impatto negativo del trattamento sui diritti e libertà delle persone fisiche, l'introduzione della figura nuova e peculiare del Responsabile della protezione dei dati conosciuto come Data protection officer, avente, tra gli altri il compito di assicurare una gestione corretta dei dati personali negli enti, e nelle imprese.

A questo punto occorre fare una breve riflessione sul fatto che nell'ordinamento nazionale è comunque presente il Codice in materia di protezione dei dati personali, D.Lgs. 196/2003 completamente riadattato alla luce dell'introduzione del Regolamento europeo. Infatti, al fine di armonizzare la disciplina interna alle previsioni regolamentari, il Codice della Privacy è

---

stato corretto con il D.lgs. 101/2018 per adeguarlo il più possibile alla normativa europea. Sul piano della struttura, il Codice, è organizzato in tre differenti parti dove la prima parte riguarda le disposizioni in generale relative soprattutto all'attuazione e all'armonizzazione con la normativa europea.

La seconda parte<sup>78</sup> è rivolta al trattamento in particolari ambiti specifici che richiedono delle disposizioni peculiari.

L'ultima parte invece riguarda la tutela dell'interessato e delle relative sanzioni previste.

Ciò che è importante è che in ogni trattamento si tenga conto contestualmente sia del Regolamento che del Codice della privacy in virtù della necessaria armonizzazione richiesta dalla normativa europea, non vi è il rischio di incontrare conflitti tra le due normative, in tale ipotesi il Regolamento prevale su quest'ultimo.

Con l'introduzione del Regolamento, non è più possibile esaminare autonomamente e separatamente la normativa nazionale dalla normativa europea in materia di trattamento dei dati personali. Essi operano in maniera congiunta e vanno dunque a costituire un sistema normativo complesso e dinamico.

In definitiva, il Garante per la protezione dei dati personali ha espressamente affermato nel parere sullo schema di decreto legislativo di adeguamento della normativa nazionale a quella europea che il trattamento dei dati personali deve avvenire secondo le norme di cui al regolamento (UE) 2016/679 le cui disposizioni costituiranno il primario regime interno in materia di protezione dei dati personali<sup>79</sup> e poi secondo le disposizioni del D.lgs 196/2003 come modificato dal legislatore nel 2018.

---

<sup>78</sup> “Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al Capo IX del Regolamento.”

<sup>79</sup> Vedasi il provvedimento n. 312 del 22 maggio 2018 del Garante per la protezione dei dati personali.

Infatti il nuovo codice revisionato nel 2018 alla luce del regolamento europeo prevede all'articolo 1 che nell'ordinamento italiano il trattamento dei dati personali avviene secondo le norme del regolamento e del codice nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

All'esito della presente disamina delle principali fonti in materia di protezione dei dati personali, occorre nel proseguo, analizzare l'impatto dei nuovi sistemi di Intelligenza artificiale nella protezione dei dati personali anche alla luce dell'approvando nuovo Regolamento sull'Intelligenza Artificiale<sup>80</sup>.

---

<sup>80</sup> Sul tema che verrà ampiamente approfondito in seguito vedasi i primi contributi di F. PIZZETTI (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018; M. C. CARROZZA, C. ODDO, S. ORVIETO, A. DI MININ, G. MONTEMAGNI, *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, n. 3, 2019, p. 245 e ss; C. CASONATO *Intelligenza Artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019, pp. 101-130. P.G CHIARA, *Sistemi intelligenti autonomi e responsabilità civile: stato dell'arte e prospettive nell'esperienza comunitaria*, in *Diritto ed economia dell'impresa*, n. 1, 2020; A. SIMONCINI *L'algoritmo incostituzionale: Intelligenza Artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n.1, 2019, pp. 69-71.; J. BURREL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & society*, 3, 2021; E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.*, n. 3, 2022, p. 1120.; D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Riv. it. inf. e dir.*, n. 2, 2022.

## CAPITOLO II

### LA PUBBLICA AMMINISTRAZIONE NELL'ERA DEI DATI

**SOMMARIO:** 1. *Artificial Intelligence Act* europeo, nuove prospettive per la Pubblica Amministrazione. 2. La stretta interconnessione tra protezione dei dati personali e sistemi di intelligenza artificiale. 3. A quale *authority* la competenza sull'IA? 4. Nuove tecnologie a servizio della Pubblica Amministrazione e decisioni automatizzate: l'IA applicata nel settore pubblico. 5. Il necessario bilanciamento tra trasparenza algoritmica e protezione dei dati personali.

#### **1. *Artificial Intelligence Act* europeo, nuove prospettive per la Pubblica Amministrazione.**

Nella disamina delle questioni giuridiche legate al trattamento dei dati personali nell'ambito del settore pubblico non può prescindere da un'attenta analisi del quadro regolatorio in tema di Intelligenza Artificiale.

Nello specifico, occorre muovere la presente analisi verso un settore particolarmente innovativo, quello dell'Intelligenza Artificiale, anche alla luce del nuovo strumento regolatorio ancora in fase di approvazione definitiva<sup>81</sup>.

A questo proposito, appare, in ogni caso, già possibile delineare alcune prime riflessioni. Occorre principiare sottolineando che la Commissione Europea<sup>82</sup> nel 21 aprile 2021 aveva redatto la prima proposta<sup>83</sup> di

---

<sup>81</sup> [https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf)

<sup>82</sup> La Commissione nelle premesse dell'atto (cfr. Point 2.2) precisa che «*the objectives of this proposal cannot be effectively achieved by Member States alone. Furthermore, an emerging patchwork of potentially divergent national rules will hamper the seamless circulation of products and services related to AI systems across the EU and will be ineffective in ensuring the safety and protection of fundamental rights and Union values across the different Member States. National approaches in addressing the problems will only create additional legal uncertainty and barriers, and will slow market uptake of AI*».

<sup>83</sup> Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (legge sull'Intelligenza Artificiale) e modifica alcuni atti dell'Unione: COM (2021) 206 del 21.4.2021.

Regolamento sull'Intelligenza Artificiale volta a stabilire regole armonizzate sull'Intelligenza Artificiale<sup>84</sup>.

La proposta è stata un elemento chiave della politica dell'Unione Europea volta alla promozione e allo sviluppo in tutto il mercato unico dell'Unione di un utilizzo dell'Intelligenza Artificiale rispettosa della certezza del diritto e della legalità<sup>85</sup>.

In particolare, l'obiettivo era quello di consentire uno sviluppo sostenibile delle nuove tecnologie e rispettoso dei diritti fondamentali delle persone, stimolando al tempo stesso lo sviluppo di tali tecnologie consentendo all'Europa di rivestire un ruolo strategico in tale ambito. Il legislatore europeo, nella relazione di accompagnamento al Regolamento ha stabilito che *“la proposta non pregiudica il Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (Direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio”*.

In seguito, il 14 giugno 2023, con l'approvazione della posizione del Parlamento Europeo con 499 voti a favore, 28 contrari e 93 astenuti, sono stati avviati i negoziati interistituzionali e il Parlamento Europeo approvava un testo con diversi emendamenti alla proposta della Commissione e dopo vari negoziati, il Parlamento e il Consiglio nella fase di trilogia, hanno raggiunto l'8 dicembre 2023 un accordo sul testo provvisorio “approvando”.

---

<sup>84</sup> Nel testo si legge che *“i) to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; ii) ensure legal certainty to facilitate investment and innovation in AI; iii) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; iv) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation”*.

<sup>85</sup>Vedasi <https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>

Il 2 febbraio 2024, gli Ambasciatori dei 27 paesi dell'Unione Europea del Coreper<sup>86</sup> hanno votato all'unanimità l'ultimo testo dell'*AI Act* approvando l'accordo raggiunto a dicembre nella fase di negoziazione<sup>87</sup>.

Successivamente, dopo aver ottenuto l'approvazione del COREPER e delle commissioni LIBE<sup>88</sup> e IMCO<sup>89</sup> del Parlamento dell'Unione Europea il 13 febbraio si è giunti a una fase prodromica alla finalizzazione dell'iter di approvazione, che è previsto per la primavera del 2024 con la votazione del Parlamento in sessione plenaria e la successiva approvazione del Consiglio<sup>90</sup>. Una volta approvato ufficialmente e formalmente dal Consiglio e dal Parlamento Europeo, il testo sarà il primo testo legislativo organico del mondo in materia di Intelligenza Artificiale<sup>91</sup>. Le linee di emendamento approvate in Parlamento hanno portato a nuovi risvolti soprattutto con riferimento alla protezione dei

---

<sup>86</sup> Coreper I is composed of each country's deputy permanent representatives. Its meetings are chaired by the deputy permanent representative of the country holding the presidency of the Council of the European Union. Coreper stands for the 'Committee of the Permanent Representatives of the Governments of the Member States to the European Union'. Its role and different formations is explained in article 240(1) of the Treaty on the Functioning of the EU. Coreper is the Council's main preparatory body. All items to be included into the Council's agenda (except for some agricultural matters) must first be examined by Coreper, unless the Council decides otherwise. It is not an EU decision-making body, and any agreement it reaches can be called into question by the Council, which alone has the power to make decisions. Coreper is composed of the 'permanent representatives' from each member state, who, in effect, are their country's ambassadors to the EU. They express the position of their government. The two configurations of Coreper (Coreper I and II) meet every week.

<sup>87</sup> <https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coreper-i/>

<sup>88</sup> Commissione per le libertà civili, la giustizia e gli affari interni

<sup>89</sup> La commissione IMCO è responsabile della supervisione e del controllo legislativo delle norme dell'UE sul mercato unico, tra cui quelle riguardanti il mercato unico digitale, le dogane e la protezione dei consumatori.

<sup>90</sup> *“Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (la "Carta"), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento. Il presente regolamento dovrebbe essere applicato conformemente ai valori dell'Unione sanciti dalla Carta agevolando la protezione delle persone fisiche, delle imprese, della democrazia e dello Stato di diritto e la protezione dell'ambiente, promuovendo nel contempo l'innovazione e l'occupazione e rendendo l'Unione un leader nell'adozione di un'IA affidabile.”*

<sup>91</sup> [https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf)

dati personali e alla tutela dei diritti fondamentali che nel proseguo si analizzeranno<sup>92</sup>.

Il 13 marzo 2024, il Parlamento ha approvato il nuovo regolamento sull'Intelligenza Artificiale<sup>93</sup> frutto dell'accordo raggiunto con 49 astensioni, 46 voti contrari e 523 voti favorevoli.

L'obiettivo principale da una preliminare lettura è rimasto quello della proposta ossia l'intento di proteggere i diritti fondamentali del cittadino in uno Stato di diritto rispettoso del principio democratico<sup>94</sup>. In particolare, tra le principali novità del nuovo regolamento, si è posta l'attenzione sui sistemi di identificazione e categorizzazione biometrica<sup>95</sup>.

---

<sup>92</sup> *“In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani. Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire regole comuni per i sistemi di IA ad alto rischio. Tali regole dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della dichiarazione europea sui diritti e i principi digitali per il decennio digitale e degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale”.*

<sup>93</sup> [https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf)

<sup>94</sup> *Nell'ultimo testo “Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA. Tali nozioni possono variare in relazione al contesto pertinente e possono includere la comprensione della corretta applicazione degli elementi tecnici durante la fase di sviluppo del sistema di IA, le misure da applicare durante il suo utilizzo, le modalità adeguate per interpretare l'output del sistema di IA e, nel caso delle persone interessate, le conoscenze necessarie per comprendere in che modo le decisioni adottate con l'assistenza dell'IA incideranno su di esse. Nel contesto dell'applicazione del presente regolamento, l'alfabetizzazione in materia di IA dovrebbe fornire a tutti i pertinenti attori della catena del valore dell'IA le conoscenze necessarie per garantire l'adeguata conformità e la sua corretta esecuzione. Inoltre, l'ampia attuazione delle misure di alfabetizzazione in materia di IA e l'introduzione di adeguate azioni di follow-up potrebbero contribuire a migliorare le condizioni di lavoro e, in ultima analisi, sostenere il consolidamento e il percorso di innovazione di un'IA affidabile nell'Unione.”*

<sup>95</sup> *La nozione di "dati biometrici" utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del regolamento (UE) 2016/679, all'articolo 3, punto 18, del regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche. (15) La nozione di "identificazione biometrica" di cui al presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una*

In particolare, si evince dal nuovo testo di recente emendato, che un divieto dovrebbe essere posto ai sistemi di “categorizzazione biometrica” basati sui dati biometrici di persone fisiche, quali il volto o le impronte digitali, per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona. Tale divieto non dovrebbe riguardare però l'etichettatura, il filtraggio o la categorizzazione legali dei set di dati biometrici acquisiti in linea con il diritto dell'Unione o nazionale in funzione dei dati biometrici, come la selezione di immagini in base al colore dei capelli o degli occhi, che possono essere utilizzati, ad esempio, nel settore delle attività di contrasto.

Essi, sono basati principalmente su una estrapolazione e registrazione di immagini facciali tramite la rete internet o sistemi di telecamere e incidono sulla sfera personale del singolo individuo espropriato del proprio diritto all'immagine.

---

*persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali. (...) La nozione di "categorizzazione biometrica" di cui al presente regolamento dovrebbe essere definita come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale, il che significa che l'elemento non può, per ragioni tecniche oggettive, essere utilizzato senza il servizio principale e che l'integrazione di tale caratteristica o funzionalità non rappresenta un mezzo per eludere l'applicabilità delle norme del presente regolamento. Ad esempio, i filtri che classificano le caratteristiche facciali o del corpo utilizzate sui mercati online potrebbero costituire una tale caratteristica accessoria, in quanto possono essere utilizzati solo in relazione al servizio principale che consiste nel vendere un prodotto consentendo al consumatore di visualizzare in anteprima il prodotto su se stesso e aiutarlo a prendere una decisione di acquisto. Anche i filtri utilizzati nei servizi di social network online che classificano le caratteristiche facciali o del corpo per consentire agli utenti di aggiungere o modificare immagini o video potrebbero essere considerati una caratteristica accessoria, in quanto tale filtro non può essere utilizzato senza il servizio principale dei servizi di social network consistente nella condivisione di contenuti online.”*

In altri termini, il nuovo regolamento ha posto un freno ai sistemi di intelligenza artificiale idonei a sfruttare la vulnerabilità dei soggetti mediante manipolazioni del comportamento umano. Dal nuovo “approvando testo” emerge che *“le tecniche di manipolazione basate sull'IA possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la scelta”*.

Ciò a cui occorre prestare particolarmente attenzione attiene al fatto che l'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA con l'obiettivo o l'effetto di distorcere materialmente il comportamento umano, *con il rischio di causare danni significativi, in particolare aventi effetti negativi sufficientemente importanti sulla salute fisica, psicologica o sugli interessi finanziari, sono particolarmente pericolosi e dovrebbero pertanto essere vietati*<sup>96</sup>.

Una deroga importante è prevista per le forze dell'ordine con riferimento ai sistemi di identificazione biometrica poiché, essi potranno farvi ricorso nelle ipotesi tassativamente previste dal regolamento e laddove vengano rispettate determinate garanzie procedurali quali l'uso limitato nel tempo e previa autorizzazione giudiziaria o amministrativa.

Ebbene, anche il regolamento sull'Intelligenza Artificiale, richiederà una ponderazione tra opposti interessi primari e valutazioni di impatto sui diritti fondamentali dell'individuo alla luce del rischio.

---

<sup>96</sup>Tali sistemi di IA impiegano componenti subliminali quali *stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli vanno al di là della percezione umana o altre tecniche manipolative o ingannevoli che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona senza che ne sia consapevole o, se ne è consapevole, senza che sia in grado di controllarle o resistervi o possa evitare l'inganno. Ciò potrebbe essere facilitato, ad esempio, da interfacce cervello-computer o dalla realtà virtuale, in quanto queste consentono un livello più elevato di controllo degli stimoli presentati alle persone, nella misura in cui possono distorcerne materialmente il comportamento in modo significativamente nocivo.*

Gli studiosi della materia parlano di una regolazione “*future proof*”<sup>97</sup> flessibile e aperta costantemente ad adattamenti; quindi, di primaria importanza sarà la redazione di norme di facile comprensione e di ampio respiro idonee ad adattarsi al cambiamento tecnologico con accentuata rapidità e mutevolezza costante.

Nei primi commenti<sup>98</sup> in dottrina, si è evidenziata l’importanza che l’utilizzo di tali sistemi sia rispettoso dell’uguaglianza di genere, delle diversità culturali, e della parità di accesso. Tali strumenti devono necessariamente restituire delle concrete elaborazioni dotate di livelli elevati di qualità e integrità in virtù di una garanzia di resilienza e resistenza nelle ipotesi di manomissione dei dati. L’*AI Act*, rispetto al Regolamento UE 2016/679 (GDPR)<sup>99</sup> è rivolto in primo luogo ai soggetti che utilizzano metodologie e processi automatizzati mediante Intelligenza Artificiale. La finalità primaria che l’Unione Europea si è promessa di raggiungere con questo nuovo regolamento è sicuramente quella di far sì che l’utilizzo di sistemi di Intelligenza Artificiale avvenga in sicurezza, trasparenza e in modo non discriminatorio<sup>100</sup>.

Nello specifico, nel primo considerando della proposta di regolamento già si faceva riferimento alla necessità di promuovere la diffusione di un’intelligenza

---

<sup>97</sup> Vedasi per un approfondimento F. LA VIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *Osservatorio sulle fonti*, n. 3, 2021, pp. 1163 ss; C. COLAPIETRO, *Gli algoritmi tra trasparenza e protezione dei dati personali*, 22 febbraio 2023, Osservatorio sulla Trasparenza, in [Federalismi.it](http://Federalismi.it); L. VIOLANTE, A. PAJNO, *Diritto e etica dell’Intelligenza Artificiale. Presentazione.*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3, 2019; F. PIZZETTI, (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018; E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.*, n. 3, 2022; D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell’Artificial Intelligence Act dell’Unione europea*, in *Riv. it. inf. e dir.*, n. 2, 2022.

<sup>98</sup> Vedasi, S. CAL, *Il quadro normativo vigente in materia di IA nella Pubblica Amministrazione (CAD, GDPR, IA ACT)* in *Intelligenza Artificiale per la pubblica amministrazione, Principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini giuridica, 2023, P. 75 e ss.

<sup>99</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

<sup>100</sup> Si veda, S. CAL, *Il quadro normativo vigente in materia di IA nella Pubblica Amministrazione (CAD, GDPR, IA ACT)* in *Intelligenza Artificiale per la pubblica amministrazione, Principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini giuridica, 2023, P. 65 e ss.

artificiale “*antropocentrica e affidabile al fine di garantire un livello elevato di protezione della salute, della sicurezza dei diritti fondamentali della democrazia dello stato di diritto nonché dell’ambiente proprio dagli effetti nocivi dei sistemi di intelligenza artificiale*”<sup>101</sup>. In particolare, all’articolo 4-bis, vengono enunciati i principi generali applicabili a tutti i sistemi di IA, al principio della sorveglianza umana (lett. a), al rispetto della normativa in materia di vita privata e protezione dei dati (lett. c) e al principio della trasparenza (lett. d) e a quello di non discriminazione (lett. e). Ciò detto, analizzando in concreto il testo, seppure non definitivo, occorre sottolineare l’importanza data al concetto di rischio<sup>102</sup>.

Infatti, nello specifico, per rischio, il nuovo regolamento intende la probabilità, il pericolo che dal sistema di intelligenza artificiale possa derivare un danno, o meglio una incertezza su una conseguenza possibile e avversa di un determinato evento per ciò che per l’essere umano è di rilievo<sup>103</sup>.

Nel Regolamento sull’Intelligenza Artificiale il pericolo quale conseguenza avversa è proprio il sistema di IA.

---

<sup>101</sup> “*Il presente regolamento contribuisce all’obiettivo di promuovere l’approccio antropocentrico europeo all’IA ed essere un leader mondiale nello sviluppo di un’IA sicura, affidabile ed etica.*”

<sup>102</sup> Già l’articolo 22 del GDPR prevede che “L’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione:a) sia necessaria per la conclusione o l’esecuzione di un contratto tra l’interessato e un titolare del trattamento;b) sia autorizzata dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato;c) si basi sul consenso esplicito dell’interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, almeno il diritto di ottenere l’intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all’articolo 9, paragrafo 1, a meno che non sia d’applicazione l’articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato.

<sup>103</sup> Per un approfondimento vedasi A. ALAIMO, *Il Regolamento sull’Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico? Focus Lavoro, persona, tecnologia*, 18 ottobre 2023, in [Federalismi.it](#); C. NOVELLI, *L’artificial Intelligence Act Europeo: alcune questioni di implementazione*, 24 gennaio 2024 in [Federalismi.it](#); T. AVEN, *Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation*, in *European Journal of Operational Research*, 253, n. 1, 2016.

Di conseguenza, il nuovo regolamento, ha suddiviso i potenziali rischi in macrocategorie nel rispetto del principio di precauzione al fine di prevedere, evitare e controllare il rischio.

Sulla base di un bilanciamento preventivo, rischi minori richiedono una cautela minore rispetto a un rischio alto o intollerabile al quale è precluso l'utilizzo.

Il rischio è considerato inaccettabile laddove i sistemi di Intelligenza Artificiale vengono utilizzati per manipolazione psicologica del comportamento umano, categorizzazione sulla base di sesso, genere, etnia, o orientamento politico, categorizzazione biometrica, in tali casi, il regolamento ha previsto una tutela forte e pregnante di divieto di utilizzo o comunque fortemente limitati salvo delle deroghe eccezionali.

Nei sistemi di rischio considerato “alto” invece, il regolamento<sup>104</sup> fa rientrare quei sistemi applicati alla sicurezza, al trasporto, all'amministrazione della giustizia e alla sicurezza pubblica e alla gestione dell'immigrazione.

In tale ipotesi, le tutele sono state ponderate in modo meno stringente rispetto ai sistemi catalogati come di rischio “inaccettabile” ma comunque, il

---

<sup>104</sup> Nel testo del Regolamento si legge che “*Il sistema di gestione dei rischi dovrebbe essere costituito da un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio. Tale processo dovrebbe mirare a individuare e attenuare i rischi pertinenti dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali. Il sistema di gestione dei rischi dovrebbe essere periodicamente riesaminato e aggiornato per garantirne l'efficacia costante, nonché la giustificazione e la documentazione delle eventuali decisioni e azioni significative adottate a norma del presente regolamento. Tale processo dovrebbe garantire che il fornitore individui rischi o impatti negativi e attui misure di attenuazione per i rischi noti e ragionevolmente prevedibili dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali alla luce della loro finalità prevista e del loro uso improprio ragionevolmente prevedibile, compresi gli eventuali rischi derivanti dall'interazione tra il sistema di IA e l'ambiente in cui opera. Il sistema di gestione dei rischi dovrebbe adottare le misure di gestione dei rischi più appropriate alla luce dello stato dell'arte in materia di IA. Nell'individuare le misure di gestione dei rischi più appropriate, il fornitore dovrebbe documentare e spiegare le scelte effettuate e, se del caso, coinvolgere esperti e portatori di interessi esterni. Nell'individuare l'uso improprio ragionevolmente prevedibile dei sistemi di IA ad alto rischio, il fornitore dovrebbe contemplare gli usi di sistemi di IA che, pur non essendo direttamente coperti dalla finalità prevista e considerati nelle istruzioni per l'uso, si può ragionevolmente prevedere derivino da un comportamento umano facilmente prevedibile nel contesto delle caratteristiche e dell'uso specifici di un determinato sistema di IA.*”

regolamento richiede degli standard molto elevati di trasparenza, affidabilità e sicurezza.

In ragione di ciò, è richiesto un sistema di gestione del rischio continuo, un controllo dei dati utilizzati, una valutazione di impatto sui diritti fondamentali e un ulteriore monitoraggio con una supervisione umana<sup>105</sup>.

Infine, il regolamento ha predisposto delle implicazioni normative diverse a seconda che il rischio sia limitato o minimo. Il rischio è limitato nel caso di sistemi come *chatbot* o *deepfakes* o sistemi di intelligenza artificiale formulati per interagire con esseri umani. In tal caso sono richiesti degli obblighi di trasparenza al fine di informare sull'interazione con sistemi di intelligenza artificiale. Invece se il rischio è considerato minimo, sono previsti minimi obblighi di trasparenza come il rispetto di codici di condotta per le aziende. In definitiva, si è riflettuto sul fatto che *“in un’ottica guidata dai valori europei e dalla tutela dei diritti fondamentali, l’Artificial Intelligence Act identifica diversi livelli di rischio nell’utilizzo di tali tecnologie, prevedendo limiti all’implementazione di tecnologie algoritmiche nel settore pubblico e privato”*<sup>106</sup>.

Tra le ultime novità, è emerso che *“sebbene l’approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un’IA affidabile del 2019 elaborati dall’AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l’AI HLEG ha elaborato sette principi etici non vincolanti per l’IA che sono intesi a contribuire a garantire che l’IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati,*

---

<sup>105</sup> Vedasi per un maggiore approfondimento A. SIMONCINI, M. G. LOSANO, *“La lunga marcia dell’informatica nelle istituzioni italiane, in il diritto dell’amministrazione pubblica digitale”* a cura di R. Cavallo Perin e Diana Urania Galetta, 2020, Giappichelli Editore, Introduzione.

<sup>106</sup> Sul tema è di recente intervenuta G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali. L’analisi di Ginevra Cerina Feroni (Garante Privacy) intervento* disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.

*trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. Fatti salvi i requisiti giuridicamente vincolanti del presente regolamento e di qualsiasi altro diritto dell'Unione applicabile, tali orientamenti contribuiscono all'elaborazione di un'IA coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione. Secondo gli orientamenti dell'AI HLEG con "intervento e sorveglianza umani" si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani."*

Il Regolamento deve essere sottoposto alla verifica finale dei giuristi – linguisti ed essere approvato definitivamente dal Consiglio.

Successivamente, entrerà in vigore venti giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea e si inizierà ad applicare 24 mesi dopo l'entrata in vigore salvo alcune deroghe<sup>107</sup>.

## **2. La stretta interconnessione tra protezione dei dati personali e sistemi di Intelligenza Artificiale**

Nell'ordinamento democratico, un principio cardine è il principio di trasparenza<sup>108</sup> e come si avrà modo di analizzare nel proseguio sarà un

---

<sup>107</sup> [https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf)

<sup>108</sup> Su tale principio che verrà richiamato spesso nel capitolo, per approfondimenti vedasi A. CORRADO *Il principio di trasparenza*, in M. A. SANDULLI, (a cura di), *Principi e regole dell'azione amministrativa*, Giuffrè Editore, Milano, 2023; A. CORRADO *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018; F. MERLONI, *La trasparenza amministrativa*, Milano, Giuffrè, 2008; M.R. SPASIANO, *I principi di pubblicità. Trasparenza e imparzialità*, in *Codice dell'azione amministrativa*, (a cura di) M. A. SANDULLI, Milano, 2017; C. COLAPIETRO – A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, a cura di C. COLAPIETRO – L. CALIFANO, Editoriale Scientifica, Napoli, 2014, pp. 117 e ss; M. A. SANDULLI – L. DROGHINI, *La trasparenza amministrativa nel FOIA italiano. Il principio della conoscibilità generalizzata e la sua difficile attuazione*, in *Federalismi.it*, 2020; M. A. SANDULLI, *Voce Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, IV aggiorn., Milano, 2000; V. FANTI, *La trasparenza*

principio cardine anche per la nuova società tecnologica. Infatti, i sistemi di intelligenza artificiale, soprattutto quelli di intelligenza artificiale *generativa*, devono garantire il rispetto del principio di conoscenza, conoscibilità, trasparenza con un temperamento dei diritti fondamentali tra questi anche il diritto alla protezione dei dati personali. Emerge infatti dall'ultimo testo *“In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani.”* Nello specifico, i fornitori dei sistemi di AI, sono chiamati ex ante a progettare i sistemi in modo che il fornitore stesso o l'utente sia in grado di informare *“in modo tempestivo, chiaro e comprensibile la persona fisica esposta ad un sistema AI”* del fatto di stare interagendo con tale sistema. Ebbene, occorre sottolineare come nel passaggio da una società prettamente digitale a una società oggi – quasi – algoritmica, i sistemi di Intelligenza Artificiale siano diventati lo strumento cardine di supporto dell'esercizio della funzione pubblica e nel controllo dell'attività amministrativa proprio per questo il regolamento sull'Intelligenza Artificiale è il primo tentativo concreto di disciplina a livello organico dell'Intelligenza Artificiale in termini politici,

---

*amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte Costituzionale (n. 20/2019), in federalismi.it, n. 5, 2020; P. CANAPARO, La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni, in Federalismi.it, 2014; A. SIMONATI, La ricerca in materia di trasparenza amministrativa: stato dell'arte e prospettive future, in Dir. amm., 2018; C. COLAPIETRO – C. SANTARELLI, Accesso civico, in Libro dell'Anno del Diritto 2014, in Treccani.it.*

assiologici e regolatori<sup>109</sup>. Alla luce delle disposizioni analizzate, appare evidente come il quadro regolatorio di riferimento in tema di dati personali si stia arricchendo di fonti normative. In ragione di ciò, appare oggi impensabile immaginare la regolazione delle nuove tecnologie prescindendo dalla protezione dei dati personali. Nel precedente capitolo, si è evidenziato che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati sia divenuto il fulcro fondante la tutela del dato personale. La principale definizione di dato personale è rinvenibile nel Regolamento generale per la protezione dei dati personali (UE) 2016/679, General Data Protection Regulation<sup>110</sup> all'articolo 4, comma 1, n.1 il quale prevede che per dato personale deve intendersi *“qualsiasi informazione riguardante una persona fisica identificata o identificabile”*. La protezione dei dati, alla luce delle nuove realtà tecnologiche sta andando sempre di più verso la ricerca di regolamenti settoriali e specifici stante l'esigenza di forme di tutela forti e compatibili con il nuovo contesto sociale – economico. Infatti, sono stati adottati e ancora sono in via di attuazione, ulteriori regolamenti relativi alla politica europea del digitale e tutti accomunati dall'esigenza di *“riequilibrare il rapporto tra Stato e mercato, persona e tecnica, libertà e innovazione”*<sup>111</sup>.

È vero che il GDPR pone l'accento sul trattamento dei dati mentre il nuovo regolamento sull'IA si focalizza principalmente sulle nuove tecnologie da utilizzare per effettuare il trattamento ma è anche vero che essi possono essere

---

<sup>109</sup> Vedasi G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali*. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.

<sup>110</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

<sup>111</sup> Vedasi P. STANZIONE, *Il potere dell'innovazione e la solitudine digitale la protezione dei dati a tutela della persona*, Relazione annuale sull'attività svolta dal Garante per la protezione dei dati personali, Presidente Pasquale Stanzone, 2022.

considerati in una visione di complementarità nonostante, secondo alcuni, rischiano oggi e nel futuro digitale di condurre ad un eccesso di regolamentazione su alcuni fronti comuni<sup>112</sup>. Infatti, il nuovo regolamento, determinerà una sovrapposizione normativa soprattutto nei sistemi di Intelligenza Artificiale ad alto rischio dove sono soprattutto dati personali ad essere trattati e in quel caso il GDPR prevarrebbe sul nuovo regolamento avendo esso una portata generale<sup>113</sup>.

Il regolamento sull'IA ricalca il GDPR soprattutto nel voler predisporre una tutela mediante un approccio “umano – centrico” concentrandosi entrambi sulle finalità del trattamento, su un approccio *by design* e su un approccio volto a identificare i rischi per i diritti fondamentali. Nonostante le similitudini e la complementarità tra i due regolamenti, la criticità principale riguarda un coordinamento sul piano non teorico ma concreto di applicazione coerente dei principi e delle regole. Infatti, già il GDPR all'articolo 25<sup>114</sup> sulla *privacy by design* fa comprendere l'esigenza di un'integrazione tra regolamenti coordinata alla luce di un'integrazione della tutela dei diritti fondamentali nelle nuove tecnologie. Re-interpretando l'articolo 25 del GDPR alla luce dei

---

<sup>112</sup> Sul tema, merita approfondire la visione di G. CERRINA FERONI, Intelligenza Artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.

<sup>113</sup> Come si è avuto modo di approfondire, ne sono un esempio di sistemi ad alto rischio l'identificazione biometrica, l'istruzione, la sanità, l'immigrazione e le prestazioni assistenziali.

<sup>114</sup> L'articolo 25 del Regolamento prevede la “*Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)*” stabilendo che “1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. 3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.”

sistemi di intelligenza artificiale, è ragionevole interpretarlo nella necessità di proteggere e tutelare i dati personali sin dalla progettazione dei sistemi di Intelligenza Artificiale. Secondo Autorevole Dottrina, l'articolo 25 del GDPR inserisce i diritti costituzionali fondamentali nella dimensione digitale anche grazie all'interpretazione del Considerando 78<sup>115</sup> che ha valore interpretativo e consente di esplicitare il fatto che «*lo sviluppo, la progettazione, la selezione e l'utilizzo di applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati*» In altri termini, il GDPR ha già enunciato principi volti a tener conto del nuovo contesto tecnologico e algoritmico, dunque il nuovo regolamento sull'IA non dovrà diventare una mera “superfetazione” di norme bensì dovrà tenersi conto che in ogni procedura automatizzata vengono trattati dati personali e in ragione di ciò ogni si auspica un concreto raccordo con i principi del GDPR proprio per non entrarvi in conflitto ma al fine di mantenere una complementarietà nonché una implementazione normativa in settori non concretamente aggiornati nel GDPR.

In questo senso il nuovo regolamento sull'IA può concretamente apportare un apporto positivo al trattamento dei dati personali. In altri termini, il nuovo approccio basato sul rischio è positivo al fine di una tutela dei dati personali

---

<sup>115</sup> Il Considerando 78 prevede che “ (78) *La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita..Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.*”

laddove vi sia un corretto raccordo con i parametri delineati già nel 2019 dal GDPR.

### **3. A quale *Authority* la competenza sull'IA?**

Ulteriore problema di fondo ancora non risolto ma che ha sollevato delle perplessità è il fatto che nel regolamento non risulta ancora definito a chi verrà attribuita la competenza di autorità di controllo sul piano nazionale nei sistemi di intelligenza artificiale incaricata di sorvegliare<sup>116</sup> l'applicazione Regolamento sull'Intelligenza Artificiale proprio come fa il Garante con il GDPR nonché di agevolare lo sviluppo di sistemi di IA innovativi.

Orbene, la questione circa l'individuazione dell'autorità competente idonea a gestire e coordinare il nuovo settore rimane una questione aperta.

Infatti, rimettere ad ogni stato membro la decisione di costituire plurime autorità di controllo può portare a una confusione di controlli e di competenze. Ci si è interrogati sui problemi che potrebbe determinare l'introduzione di un'agenzia di controllo di tipo governativo. Ciò che rileva è che la vigilanza sull'applicazione del regolamento deve passare ad un'autorità neutrale, indipendente proprio dal potere politico libera di agire in condizioni di autonomia dal Governo responsabile anche dell'enforcement del regolamento nel rispetto dei diritti fondamentali e della democrazia che abbia sempre una pronta visione della tutela e del trattamento dei dati personali<sup>117</sup>.

---

<sup>116</sup> l'art. 59 dell'AI Act, le autorità nazionali competenti dovranno disporre di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di intelligenza artificiale, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti.

<sup>117</sup> Vedasi A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'Intelligenza Artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, pp. 87 ss; P. OTRANTO, *Riflessioni in tema di decisione amministrativa, Intelligenza Artificiale e legalità*, in *Federalismi.it*, n. 7, 2021; E. FALLETTI, *La formazione delle black box: garanzie della privacy e tutela antidiscriminatoria*, in M. D'AMICO, B. LIBERALI, ANTONIO P. MIRAS, E. C. RAFFIOTTA, S. ROMBOLI, G. M. TERUEL LOZANO (a cura di), *Europa, società aperta. Problemi attuali e prospettive future*, ESI, Napoli, 2022; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 11 agosto 2018, n. 101*, Bologna, 2017; A.D. SELBST,

È evidente che la caratteristica principale delle Autorità Amministrative Indipendenti sia quella di essere indipendente dagli altri poteri dello Stato, tuttavia, l'indipendenza dal potere economico e politico non è da sola sufficiente a racchiudere in sé il ruolo delle Autorità anche al fine di comprenderne concretamente l'esigenza di un'Autorità che vigili sui nuovi sistemi di IA.

Occorre dunque partire dalla ratio dell'istituzione delle Autorità e soffermarsi su un punto non sempre chiaro ma ben delineato e di fondamentale importanza.

Le Autorità amministrative indipendenti sono state istituite al fine di attuare gli obiettivi predisposti dal diritto dell'Unione Europea previsti dai Trattati e dalle fonti di diritto derivato (analizzate nel primo capitolo del presente contributo).

Tra i principali pilastri e valori fondanti dell'Unione europea vi sono appunto quelli previsti dagli articoli 2 e 3 del TUE<sup>118</sup>. Le missioni affidate alle autorità sono la ratio giustificatrice della loro indipendenza<sup>119</sup>.

---

J.POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 2017; G. FINOCCHIARO, F. PAOLUCCI, O. POLLICINO, *Intelligenza artificiale e diritti individuali al perimetro ancora incerto*, in *Il Sole 24 ore*, 16 giugno 2023.

<sup>118</sup> L'articolo 2 prevede che *“L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini.”* Mentre l'articolo 3 prevede che *“L'Unione si prefigge di promuovere la pace, i suoi valori e il benessere dei suoi popoli. L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima. 3. L'Unione instaura un mercato interno. Si adopera per lo sviluppo sostenibile dell'Europa, basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico. L'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociali, la parità tra donne e uomini, la solidarietà tra le generazioni e la tutela dei diritti del minore. Essa promuove la coesione economica, sociale e territoriale, e la solidarietà tra gli Stati membri. Essa rispetta la ricchezza della sua diversità culturale e linguistica e vigila sulla salvaguardia e sullo sviluppo del patrimonio culturale europeo. L'Unione istituisce un'unione economica e monetaria la cui moneta è l'euro. Nelle relazioni con il resto del mondo l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione*

Nell'ordinamento interno, il ruolo di il Garante per la protezione dei dati personali la prima autorità indipendente che vigila sul rispetto del Regolamento e ha la missione di tutelare il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata. Ciò che ha il Garante per la protezione dei dati personali rispetto alle altre autorità previste nel nostro ordinamento è che trattasi di un'autorità indipendente che ha una espressa previsione costituzionale a livello europeo rinvenibile nell'articolo 8 della Carta dei diritti fondamentali dove è espressamente previsto che *“Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

La tutela del dato personale, dunque è divenuta la preconditione per il godimento di ulteriori libertà fondamentali soprattutto nell'ordinamento democratico. L'importanza dell'istituzione di autorità indipendenti dal potere politico di controllo non osta neanche al principio democratico poiché, come affermato dalla Corte di Giustizia<sup>120</sup>, comunque regolano nel rispetto del

---

*dei suoi cittadini. Contribuisce alla pace, alla sicurezza, allo sviluppo sostenibile della Terra, alla solidarietà e al rispetto reciproco tra i popoli, al commercio libero ed equo, all'eliminazione della povertà e alla tutela dei diritti umani, in particolare dei diritti del minore, e alla rigorosa osservanza e allo sviluppo del diritto internazionale, in particolare al rispetto dei principi della Carta delle Nazioni Unite. 6. L'Unione persegue i suoi obiettivi con i mezzi appropriati, in ragione delle competenze che le sono attribuite nei trattati.”*

<sup>119</sup> Per un approfondimento vedasi il contributo di G. PITRUZZELLA, Le autorità amministrative indipendenti: bilancio e prospettive, in *Il ruolo del Garante per la protezione dei dati personali, la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di Ginevra Cerrina Feroni, Il Mulino, 2024; G.P. CIRILLO – R. CHIEPPA, *Le Autorità amministrative indipendenti*, in G. Santaniello, *Trattato di diritto amministrativo*, vol. 41. Padova, Cedam, 2010; G. P. ALPA – A. CATRICALA', *Diritto dei consumatori*, Bologna, Il Mulino, 2016.

<sup>120</sup> Corte di giustizia c-718/18 Commissione Europea c. Repubblica federale di Germania

principio di legalità, sono sottoposte al sindacato del giudice e i loro componenti sono comunque nominati dal governo<sup>121</sup>.

In ragione dell'analisi svolta, le ragioni che portano a riconsiderare il ruolo del Garante come autorità di controllo non solo della protezione dei dati personali ma anche come nuova autorità che vigila sul rispetto dei sistemi di intelligenza artificiale sono plurime anche a discapito di chi ritiene sia più sistematico individuare un'autorità ad hoc.

il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD) con un parere congiunto<sup>122</sup> hanno raccomandato l'affidamento della funzione e delle responsabilità di autorità di controllo in materia di IA alle autorità nazionali già competenti per la protezione dei dati.

Ciò in quanto esse già applicano il GDPR per quanto riguarda i sistemi di IA che interessano i dati personali e dunque hanno maturato *“conoscenze in materia di tecnologie basate sull'IA, di dati e di sistemi di elaborazione degli stessi nonché di diritti fondamentali, e di competenze nella valutazione dei rischi che le nuove tecnologie comportano per questi diritti fondamentali.”* Inoltre, se i sistemi di IA si basano sul trattamento di dati personali o li trattano, le disposizioni dell'AI Act sono direttamente interconnesse con il quadro giuridico per la protezione dei dati. *“La designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe un approccio normativo più armonizzato, favorirebbe un'interpretazione coerente delle disposizioni in materia di trattamento dei dati ed eviterebbe contraddizioni nella loro applicazione nei diversi Stati membri. Inoltre, le parti interessate della catena di valore dell'IA trarrebbero beneficio*

---

<sup>121</sup> Ancora G. PITRUZZELLA, Le autorità amministrative indipendenti: bilancio e prospettive, in *Il ruolo del Garante per la protezione dei dati personali, la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di Ginevra Cerrina Feroni, Il Mulino, 2024, p. 27 e ss; G. AMATO, *Autorità semi – indipendenti e autorità di garanzia*, in *Riv. trim. dir. pub.*, 1997.

<sup>122</sup> Parere 5 del 2021 sulla proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale 18 giugno 2021.

*dall'esistenza di un punto di contatto unico per tutte le operazioni di trattamento dei dati personali che rientrano nell'ambito di applicazione dell'AI Act<sup>123</sup>.*

Un ulteriore profilo a favore dell'istituzione del Garante come l'autorità incaricata di sorvegliare l'applicazione dell'AI Act e di istituire spazi di sperimentazione normativa per agevolare lo sviluppo e le prove di sistemi di IA innovativi prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio risiede nel fatto che il Garante sia già dotato di un Dipartimento di Intelligenza artificiale, che potrebbe costituire il nucleo originario di una struttura più articolata al fine di orientarne lo sviluppo attraverso la lente della privacy<sup>124</sup>.

Al fine della presente analisi, è possibile rinvenire un'applicazione concreta dei principi sopra espressi da parte del Garante sul tema dell'intelligenza artificiale.

Ebbene, il Garante Privacy ha avviato una istruttoria, l'8 marzo del 2024 nei confronti di OpenAI in virtù del lancio di un nuovo sistema di intelligenza artificiale denominato "Sora"<sup>125</sup>. Con specifico riguardo alle implicazioni dell'utilizzo di tale nuovo sistema di intelligenza artificiale sul trattamento dei dati personali, il Garante privacy ha chiesto ad OpenAI di fornire alcuni chiarimenti.

In primo luogo, ha chiesto di chiarire le modalità di addestramento dell'algoritmo nonché di specificare i dati raccolti ed elaborati per addestrarlo, specialmente se si tratti di dati personali, inoltre ha chiesto se tra questi vi siano anche particolari categorie di dati (convinzioni religiose, filosofiche,

---

<sup>123</sup> Punto 48 del parere congiunto 5 2021 edpb.

<sup>124</sup> Sul tema si è espresso D. FULCO, Autorità nazionale per l'IA: perché deve essere il Garante privacy in <https://www.agendadigitale.eu/sicurezza/privacy/autorita-nazionale-per-lia-perche-deve-essere-il-garante-privacy/>

<sup>125</sup> Nella definizione su <https://openai.com/sora> è possibile definire il programma come *"Sora is able to generate complex scenes with multiple characters, specific types of motion, and accurate details of the subject and background. The model understands not only what the user has asked for in the prompt, but also how those things exist in the physical world."*

opinioni politiche, dati genetici, salute, vita sessuale) nonché quali siano le fonti utilizzate.

L'analisi di tale provvedimento fa comprendere quanto, il Garante per la protezione dei dati personali sia l'autorità, ad oggi, più preparata sui nuovi sistemi di IA.

Invero, anche alla luce dell'istruttoria in itinere, occorre rilevare che l'addestramento di algoritmi di intelligenza artificiale richiede una raccolta ingente di dati e molto spesso si tratta di dati personali al fine di garantire prestazioni più efficienti da parte dei sistemi di intelligenza artificiale. Tutto ciò entra in collisione con il principio di minimizzazione secondo cui, i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

In definitiva, occorre sottolineare che oggi, nell'Unione Europea, gli sviluppatori, o chi fornisce o implementa tali tecnologie nuove, non potrà più ignorare il forte impatto della protezione dei dati personali sulla materia e dunque, una intersezione<sup>126</sup> tra la regolazione dell'Intelligenza Artificiale con il GDPR.

Con tale regolamento, il legislatore europeo ha dato avvio alla regolamentazione di un settore peculiare relativo al rapporto tra nuove tecnologie e protezione dei dati personali che sino a poco tempo fa era stato lasciato esclusivamente all'autoregolazione mentre sulla scorta del GDPR, il legislatore europeo ha iniziato a tutelare tale peculiare settore su più fronti.

In particolare, per completare la disamina del quadro regolatorio in materia di dati utilizzati in contesti diversi, successivamente al Regolamento europeo per la protezione dei dati personali, lo strumento regolatorio è stato utilizzato per disciplinare il funzionamento di uno Spazio comune europeo dei dati, esso è

---

<sup>126</sup> Così G. CERRINA FERONI, *Le stagioni del Garante. La privacy e il cambiamento del Paese*, G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali*, il Mulino 2024, pp. 59 e ss. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.

denominato “*Data Governance Act*”<sup>127</sup> attuato dal 24 settembre 2023 volto a definire le regole e le condizioni che l’Europa ha adottato sul *data sharing*. In particolare, la finalità di tale Regolamento è principalmente quella di disciplinare in concreto il riutilizzo dei dati pubblici e implementare i servizi di intermediazione di dati. Il *Data Governance Act* è volto principalmente a regolamentare l’economia digitale in tutte le sue articolazioni sia nel settore pubblico che privato in cui vengono in considerazione dati e strumenti di intelligenza artificiale connessi ad essi.

Inoltre, al fine di garantire una concorrenza leale nel mercato digitale dell’Unione Europea, è stato introdotto il Regolamento denominato “*Digital Markets Act*”<sup>128</sup> applicabile dal 6 marzo 2024.

La ratio dello stesso è quella di individuare le società *gatekeeper* al fine di garantire degli strumenti di tutela a terze parti contro eventuali preferenze di posizionamento o asimmetrie informative. Infine, sempre con il fine di disciplinare il funzionamento di una politica europea del digitale è stato previsto il “*Digital Service Act*”<sup>129</sup> applicabile dal 17 febbraio 2024 con la finalità di definire in concreto i contenuti digitali illegali introducendo degli strumenti nuovi al servizio degli utenti per effettuare delle segnalazioni in caso di contenuti che promuovono la violenza, discriminazione o incitamento all’odio. Nello specifico, le piattaforme dovranno effettuare delle valutazioni di impatto dei rischi sistemici relativi ad eventuali effetti negativi per l’esercizio dei diritti fondamentali al rispetto della vita privata e familiare e alla libertà di espressione e di informazione, del diritto alla non discriminazione e dei diritti del minore, sanciti rispettivamente dagli articoli 7, 11, 21 e 24 della Carta.

---

<sup>127</sup> Regolamento 2022/868 del 30 maggio 2022

<sup>128</sup> Regolamento 2022/1828 del 14 settembre 2022

<sup>129</sup> Regolamento 2022/2065 del 19 ottobre 2022

Tali iniziative regolamentari nuove hanno lo scopo principale di facilitare in primo luogo la disponibilità e la condivisione dei dati con la finalità di sfruttarne il loro potenziale garantendo dei benefici anche per le imprese europee.

L'aumento dei dati disponibili ha richiesto sin da subito nuove regolamentazioni settoriali e così facendo, l'Unione Europea, sulla scorta del successo del GDPR mira a diventare regolatore globale sull'impiego dei dati grazie al “*Digital Package*” nuovo strumento attraverso cui si arriva a disciplinare il valore secondario dei dati<sup>130</sup> e dunque l'interesse dei dati personali e non personali per la collettività nonché l'utilizzo che se ne può fare mediante i nuovi sistemi di Intelligenza artificiale<sup>131</sup>.

#### **4. Nuove tecnologie a servizio della Pubblica Amministrazione e decisioni automatizzate: L'IA applicata nel settore pubblico.**

Come si è avuto modo di anticipare, la digitalizzazione ha caratterizzato la società odierna portando ad un utilizzo di nuove tecnologie e di sistemi di intelligenza artificiale. L'evoluzione dei sistemi di intelligenza artificiale in grado di raccogliere, confrontare e rielaborare quantità indefinite di dati, ha avuto un forte impatto anche sulle tecnologie adoperate dalle pubbliche amministrazioni. L'amministrazione digitale utilizza tecnologie informatiche nell'organizzazione e nello svolgimento dell'attività amministrativa, si esprime attraverso dati in formato digitale applicando algoritmi per

---

<sup>130</sup> Il valore originario dei dati è tutelato dal GDPR mentre il valore secondario è tutelato dai nuovi strumenti regolatori.

<sup>131</sup> Sul tema si vedano i contributi di G. D'ACQUISTO, *Trattamento dei dati personali e processo decisionale automatizzato nella PA, in Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 203 e ss; A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*. in *Il diritto dell'amministrazione pubblica digitale*, a cura di R. Cavallo Perin e D. U. Galetta, Giappichelli Editore, 2020, p. 21 e ss.

automatizzare parte delle procedure amministrative e dei processi decisionali al fine di assicurare maggiore efficienza<sup>132</sup>.

In ragione di ciò, si è riconosciuto in capo alle pubbliche amministrazioni la possibilità di utilizzare nuove nonché evolute soluzioni tecnologiche in grado di sostituirsi all'attività umana anche nella gestione del procedimento amministrativo<sup>133</sup>

In realtà, già nel 1979 si iniziava a fare i conti con il possibile utilizzo di tecnologie come strumento efficiente e funzionale al servizio offerto dalla sfera pubblica<sup>134</sup>.

L'utilizzo dell'intelligenza artificiale ha avuto un serio impatto nella struttura della pubblica amministrazione nonché negli strumenti da essa utilizzati.

La ragione principale deve rinvenirsi in primo luogo nell'effetto che hanno tali strumenti nel velocizzare varie tipologie di processi sia sotto il profilo dell'organizzazione che sotto il profilo dell'attività. Parte della dottrina, ha iniziato a parlare ben presto di "Amministrazione 4.0"<sup>135</sup> caratterizzata da un *"alto grado di automazione e di interconnessione che sta esercitando un impatto importante sull'essere umano stesso e sul suo modo di essere, oltre che sul suo ambiente di riferimento"*<sup>136</sup>.

---

<sup>132</sup> Sul tema A. CORRADO, *La Trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, 22 febbraio 2023, in [Federalismi.it](http://Federalismi.it).

<sup>133</sup> Sul tema vedasi T. COCCHI, *La partecipazione procedimentale*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 134 e ss; A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 174 e ss.

<sup>134</sup> M.S. Giannini, *Rapporto sui principali problemi dell'Amministrazione dello Stato*, 16 novembre 1979.

<sup>135</sup> Vedasi sul tema D.U. GALETTA – J. G. CORVÀLAN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi*, 3/2019;

<sup>136</sup> «nel XX secolo, l'evoluzione delle tecnologie dell'informazione e della comunicazione (ICT) ha modellato una combinazione asimmetrica fra tre paradigmi della Pubblica Amministrazione: la Pubblica Amministrazione 1.0, che corrisponde al classico modello di Pubblica Amministrazione del diciannovesimo secolo, caratterizzato dall'utilizzo di carta, stampa e macchina da scrivere. La Pubblica Amministrazione 2.0, che incorpora computer, processori di testo, stampante e fax. La Pubblica Amministrazione 3.0 verso cui, nel XXI secolo, il settore pubblico ha iniziato a migrare

La legge 241 del 1990 sul procedimento amministrativo prevede all'articolo 3-bis che *“le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati.*

Tra i vantaggi espliciti principali, vengono alla luce esigenze di celerità, semplificazione e efficienza dell'azione amministrativa<sup>137</sup>. Tuttavia, ci si è interrogati sulle conseguenze derivanti dall'utilizzo dell'intelligenza artificiale nel settore pubblico e sul se, in concreto, possa essere in grado di far sì che venga perseguito l'interesse pubblico primario<sup>138</sup>.

Invero, si è sottolineata l'importanza di ricercare delle garanzie e delle tutele forti al fine di riconoscere un nuovo potere amministrativo “algoritmico” soggetto tuttavia agli stessi vincoli del potere amministrativo tradizionale.

Al fine di evitare delle compressioni dei diritti degli amministrati, parte della dottrina ha ipotizzato di aggiornare le teorizzazioni dei principi cardine del diritto amministrativo al fine di rinvenire delle tutele forti alla pari del procedimento amministrativo non algoritmico<sup>139</sup>.

Il procedimento amministrativo, inteso come la *“sequenza di atti e operazioni che si realizzano in vista di un certo risultato di diritto amministrativo”*<sup>140</sup>, consente di ricondurre il potere pubblico in uno standard di razionalità procedurale facendo sì che gli interessati al processo di formazione della decisione pubblica possano partecipare.

---

*grazie all'uso di internet, dei portali digitali, delle applicazioni mobili e dei social network. Attualmente la Pubblica Amministrazione si trova, tuttavia, già in una quarta fase di evoluzione. Questa quarta fase è collegata alla c.d. Quarta Rivoluzione Industriale”.*

<sup>137</sup> Si veda M. A. SANDULLI, *Il Giudizio amministrativo, Principi e regole*, Editoriale Scientifica Napoli, 2024; V. LOPILATO, *Manuale di diritto amministrativo*, II, III ed., Torino, 2023; P. CHIRULLI, *La partecipazione al procedimento*, in *Principi e regole dell'azione amministrativa*, a cura di M. A. SANDULLI, Milano, 2023; M. SPASIANO, *Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto*, in *Dir. dell'Econ.*, 2022, 30.

<sup>138</sup> Vedasi T. COCCHI, *La partecipazione procedimentale*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 136 e ss.

<sup>139</sup> L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023.

<sup>140</sup> Così A. M. Sandulli, *Manuale di diritto amministrativo*, Napoli, 1969, 373.

Ebbene, la partecipazione al procedimento persegue plurime finalità ed è disciplinata dalla legge 241 del 1990<sup>141</sup>. Gli istituti di partecipazione consentono il rispetto del principio democratico nonché garantiscono l'introduzione di interessi che l'amministrazione valuterà nel bilanciamento poiché se essa viene garantita all'interessato, il provvedimento finale sarà la sintesi degli interessi in gioco e correttamente bilanciati.

Occorre dunque concretamente interrogarsi sul se l'utilizzo delle nuove tecnologie nel pubblico settore, possa determinare un dequotamento sostanziale delle garanzie del procedimento amministrativo stabilite nella legge 241 del 1990 nonché il principio di buona amministrazione previsto dall'articolo 41 della Carta dei diritti Fondamentali<sup>142</sup>.

Nello specifico, in giurisprudenza e dottrina si suole parlare di legalità algoritmica<sup>143</sup> per indicare l'utilizzo delle tecnologie, algoritmi e soluzioni di intelligenza artificiale nel rispetto e in conformità con i principi della Costituzione nonché della legge sul procedimento amministrativo. Ciò in quanto, l'utilizzo di tali sistemi richiede sempre di più un temperamento forte tra l'efficientamento dell'amministrazione 4.0<sup>144</sup> con il principio di

---

<sup>142</sup> L'articolo 41 prevede che *“Ogni individuo ha diritto a che le questioni che lo riguardano siano trattate in modo imparziale, equo ed entro un termine ragionevole dalle istituzioni e dagli organi dell'Unione. Tale diritto comprende in particolare:– il diritto di ogni individuo di essere ascoltato prima che nei suoi confronti venga adottato un provvedimento individuale che gli rechi pregiudizio,– il diritto di ogni individuo di accedere al fascicolo che lo riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale,– l'obbligo per l'amministrazione di motivare le proprie decisioni. Ogni individuo ha diritto al risarcimento da parte della Comunità dei danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni conformemente ai principi generali comuni agli ordinamenti degli Stati membri. Ogni individuo può rivolgersi alle istituzioni dell'Unione in una delle lingue del trattato e deve ricevere una risposta nella stessa lingua.*

<sup>143</sup> Sul tema si veda E. CARLONI, I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo, in *Dir. amm.*, 2, 2020, 281; U. ALLEGRETTI, Democrazia partecipativa, in *Enc. dir.*, Annali, V, Milano, 2011; A. G. OROFINO – G. GALLONE, L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione, in *Giur. it.*, 7, 2020, 1738 ss; S. TRANQUILLI, Rapporto pubblico – privato nell'adozione della decisione amministrativa “robotica”, in *Dir. soc.*, 2, 2020, 281 ss; A. ALEMANNI, Unpacking the principle of openness in EU Law. Transparency, participation and democracy, in *Eur. Law Rev.*, 2014.

<sup>144</sup> Vedasi E. CARLONI, Tendenze recenti e nuovi principi della digitalizzazione pubblica, in *Giornale Dir. Amm.*, n.2, 2015.; E. CARLONI, La qualità delle informazioni pubbliche, l'esperienza italiana nella prospettiva comparata, in *Rivista trimestrale di diritto pubblico*, 2009; S. CASSESE, che cosa resta

buona amministrazione previsto dall'articolo 41 della Carta dei diritti fondamentali dell'Unione Europea.

Parte della dottrina<sup>145</sup> ha evidenziato che l'automazione del procedimento amministrativo può esplicarsi secondo differenti modalità.

In primo luogo, l'automazione del procedimento può definirsi “completa” in tutti i suoi elementi quando l'intermediazione del “funzionario” persona fisica non è dirimente per lo svolgimento delle funzioni ma è sostituita in toto dai sistemi di intelligenza artificiale che sostituiscono integralmente l'attività del funzionario.

In secondo luogo, è possibile rinvenire un'attività mediana in cui l'intermediazione del funzionario “persona fisica” è richiesta, ma non per l'intero svolgimento della procedura, bensì per un ridotto apporto al fine di compiere le attività istruttorie mediante un'interazione con i sistemi di intelligenza artificiale per controllare o revisionare i risultati prodotti dalla macchina.

Infine, è possibile che vi siano delle ipotesi di “*machine learning*” basate interamente su sistemi di intelligenza artificiale, di autoapprendimento.

La giurisprudenza amministrativa<sup>146</sup> in mancanza di una normativa puntuale per il procedimento amministrativo algoritmico ha individuato, anche e soprattutto alla luce del GDPR, il rispetto di alcuni principi fondamentali da parte delle amministrazioni pubbliche in presenza di decisioni automatizzate<sup>147</sup>.

---

dell'amministrazione pubblica?, in Riv. trim. dir. pub., n. 1, 2019.; P. COSTANZO, La democrazia digitale. Precauzioni per l'uso, in Diritto pubblico, 1, 2019.

<sup>145</sup> Vedasi D.U. GALETTA, Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT), in Diritto dell'Amministrazione pubblica digitale, Giappichelli, 2020; D.U. GALETTA – J. G. CORVALÀN, Intelligenza Artificiale per una Pubblica Amministrazione 4.0 potenzialità, rischi e sfide della rivoluzione tecnologica in atto, in federalismi.it 6 febbraio 2019.

<sup>146</sup> Cons. Stato 13 dicembre 2019 n. 8472.

<sup>147</sup> Vedasi F. FAINI, Trasparenza, apertura e controllo democratico dell'amministrazione pubblica, in Cib. dir., 2014;

In una prima fase, il TAR Lazio<sup>148</sup> ha preferito ritenere che *“le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l’attività cognitiva, acquisitiva e di giudizio che solo un’istruttoria affidata ad un funzionario persona fisica è in grado di svolgere e che pertanto, al fine di assicurare l’osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento deve seguitare ad essere il dominus del procedimento stesso, all’uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt’oggi un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell’attività dell’uomo.”*

Secondo il giudice di primo grado dunque, l’attività del funzionario pubblico non può essere in alcun modo sostituita dalla tecnologia e dalle decisioni automatizzate.

Successivamente, il Consiglio di Stato<sup>149</sup>, ha individuato alcune condizioni e principi per giustificare il procedimento amministrativo svolto mediante procedure automatizzate con l’uso di algoritmi.

In primo luogo, il giudice amministrativo ha affermato che il principio di buon andamento dell’azione amministrativa previsto dall’articolo 97 della Costituzione è ampiamente rispettato se la pubblica amministrazione si avvale di strumenti tecnologici innovativi e che un elevato livello di digitalizzazione dell’amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti. In ragione di ciò, il Consiglio di Stato ha ritenuto che l’utilizzo di tali strumenti favorisca anche un’accelerazione

---

<sup>148</sup> TAR Lazio Roma, 27 giugno 2016, n. 806; TAR Lazio Roma, 11 luglio 2018 n. 9224; TAR Lazio Roma 27 maggio 2019 n. 6606; TAR Lazio Roma, 13 settembre 2019 n. 10964.

<sup>149</sup> Cons. Stato, Sez. VI, 8 aprile 2019, n. 2270.

dell'iter procedimentale ponendo però un limite a tale utilizzo alle sole attività vincolate poiché nelle operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza o dolo del funzionario determina una maggiore garanzia di imparzialità della decisione automatizzata.

Il giudice di secondo grado, nella decisione ha poi stabilito il doveroso rispetto della cosiddetta "regola algoritmica"<sup>150</sup> delineandone le caratteristiche.

Nello specifico ha sottolineato l'importanza che essa assuma una valenza giuridica e amministrativa, anche se viene declinata in forma matematica e, come tale, deve soggiacere ai principi generali dell'attività amministrativa, quali quelli di pubblicità e trasparenza (art. 1 l. 241/90), di ragionevolezza, di proporzionalità. Inoltre, non può lasciare spazi applicativi discrezionali bensì dovrà prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili. Ciò in quanto la discrezionalità amministrativa, deve rinvenirsi al momento dell'elaborazione dello strumento digitale.

In ragione di ciò, l'amministrazione dovrà svolgere *ex ante* un bilanciamento degli interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo. Infine, la regola algoritmica deve contemplare la possibilità che sia il giudice a "*dover svolgere, per la prima volta sul piano 'umano', valutazioni e accertamenti fatti direttamente in via automatica*", con la conseguenza che la decisione robotizzata "*impone al giudice di valutare la correttezza del processo automatizzato in tutte le sue componenti*".

---

<sup>150</sup> Si veda E. BELISARIO – F. RICCIULLI, Legalità algoritmica e vizi procedimentali, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 159 e ss.

Il giudice amministrativo, alla luce di questi criteri dovrà valutare la correttezza del processo informatico tenendo conto della validità, della correttezza del processo informatico dei dati inseriti e di tutte le sue componenti intrinseche. Inoltre, il giudice amministrativo dovrà poter sindacare la logicità e ragionevolezza della “regola algoritmica”<sup>151</sup>.

Dopo aver affermato questi importanti principi, il Consiglio di Stato<sup>152</sup>, nel 2019 torna sul tema integrando la precedente pronuncia delineando tre principi fondamentali da tenere in considerazione in presenza di decisioni automatizzate mediante l’utilizzo di algoritmi. In primo luogo, il principio di conoscibilità dell’algoritmo, in secondo luogo il principio di non discriminazione algoritmica, in terzo luogo il principio di non esclusività della decisione algoritmica. Tali principi trovano il loro fondamento nel voler rafforzare le garanzie procedurali stabilite nella legge 241 del 1990 alla luce delle nuove tecnologie, come quella di garantire la trasparenza e la conoscibilità nonché la comprensibilità degli strumenti utilizzati.

Secondo il principio di conoscibilità ogni soggetto ha il diritto di conoscere l’esistenza di processi decisionali automatizzati che lo riguardano e di ricevere, in base al principio di comprensibilità, indicazioni sulle logiche utilizzate.

Il principio di non esclusività della decisione algoritmica, che deriva dall’articolo 22 del GDPR<sup>153</sup>, laddove una decisione automatizzata procuri effetti giuridici su una persona, questa ha diritto a che tale decisione non sia basata esclusivamente sulla procedura automatizzata.

---

<sup>151</sup>A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 175 e ss; M. INTERLANDI – L. TOMASSI, *La decisione amministrativa algoritmica*, in *Approfondimenti di diritto amministrativo*, a cura di A. Contieri, Editoriale Scientifica, 2020.

<sup>152</sup> Cons. Stato 13 dicembre 2019 n. 8472.

<sup>153</sup> “Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione”

Infine, secondo il principio di non discriminazione algoritmica desunto dal considerando 71 del Regolamento<sup>154</sup> il titolare del trattamento deve utilizzare delle procedure appropriate per la profilazione al fine di garantire l'esattezza dei dati e di minimizzare il rischio di errori ciò in virtù anche degli articoli 13 e seguenti del Regolamento europeo.

Parte della dottrina<sup>155</sup> ritiene che l'utilizzo delle nuove tecnologie anche in presenza di attività discrezionale possa determinare una perdita del potere

---

<sup>154</sup> Il Considerando 71 prevede che “L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti.. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.”

<sup>155</sup> Si veda G. FERRARI, *L'uso degli algoritmi nella attività amministrativa discrezionale*, in *Il diritto degli affari*, 2020, I.

decisionale essendo l'attività discrezionale espressione di azione e pensiero dell'uomo<sup>156</sup>.

È evidente, la stretta connessione con i principi del Regolamento europeo, in particolare, il principio di non esclusività algoritmica che trae le sue radici, come si è visto dall'articolo 22 gdpr, attiene proprio all'importanza dell'intermediazione umana nelle procedure automatizzate secondo il modello del “*human in the loop*” che richiede un'interazione proattiva tra macchina e essere umano.

È proprio il GDPR che prevede che in presenza di un processo decisionale automatizzato, l'interessato ha il diritto di non essere sottoposto ad una decisione basata solo ed esclusivamente sul trattamento automatizzato.

Ad oggi, si ritiene di primaria importanza la dimensione umana nell'era dell'intelligenza artificiale poiché è vero che l'uomo non può più fare a meno delle tecnologie nel nuovo contesto sociale ma è anche vero che la macchina necessita del sostentamento dell'essere umano, delle capacità cognitive dell'uomo e in particolare dei suoi dati, motore dell'Intelligenza artificiale<sup>157</sup>.

La finalità di introdurre delle “regole algoritmiche” racchiuse nel “principio di conoscibilità, non esclusività e non discriminazione algoritmica da parte della giurisprudenza amministrativa ispirata dal GDPR, deve dunque rinvenirsi nella necessità concreta di assicurare una protezione agli amministrati destinatari dell'attività amministrativa automatizzata poiché si è ritenuto che i principi e le

regole<sup>158</sup> dell'azione amministrativa non fossero sufficienti nel contesto attuale a garantirla in un ottica di trasparenza e conoscibilità.

---

<sup>156</sup> Sul tema, A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 175 e ss.

<sup>157</sup> Così di recente G. CERRINA FERONI, *La dimensione umana nell'era dei dati e delle intelligenze artificiali in occasione del convegno “Il diritto e le nuove dimensioni dell'essere*. In ricordo di Antonio Palma, Fondazione Cesifin 11 marzo 2024.

<sup>158</sup> M.A. SANDULLI, usa espressione nel testo *Principi e regole dell'azione amministrativa*, a cura di M.A. SANDULLI Milano, Giuffrè 2023.

Il legame tra la normativa sulla protezione dei dati personali prevista dal GDPR e i sistemi algoritmici è in particolar modo evidente negli strumenti di tutela messi a disposizione dell'interessato dal Regolamento ogni volta in cui subisce un trattamento. In particolare, occorre soffermarsi sugli articoli 13<sup>159</sup>, 14<sup>160</sup> e 15 del GDPR<sup>161</sup> che consentono di comprendere l'essenza stessa della

---

<sup>159</sup> L'articolo 13 prevede che *“In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) 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 e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. (1)2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.”*

<sup>160</sup> L'articolo 14 prevede che *“1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni: a) 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) le categorie di dati personali in questione; 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 destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. 2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti*

---

informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. 4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2. 5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

<sup>161</sup> L'articolo 15 del regolamento si occupa del diritto di accesso e prevede che "1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. 3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del

trasparenza algoritmica in attesa di una normativa interna di settore. Tali articoli, pongono in evidenza l'importanza di dare effettività concreta alla conoscibilità e comprensibilità.

Ebbene, in particolare il titolare del trattamento in caso di raccolta presso l'interessato di dati che lo riguardano fornisce una serie di informazioni oltre a rendere nota l'esistenza di un processo decisionale automatizzato compresa la profilazione nonché deve consentire la conoscibilità della "logica utilizzata dalla macchina" nel trattamento.

La comprensibilità della logica algoritmica prevista dall'articolo 14, come si è analizzato al principio, è stato preso in considerazione dalla giurisprudenza amministrativa come esempio concreto per costruire la regola algoritmica e consentire di rendere edotti gli interessati della logica sottostante alla decisione.

Un principio importante che merita di essere analizzato per comprendere se possa essere considerato uno strumento di tutela dell'interessato è il diritto di accesso previsto dall'articolo 15 del GDPR che prevede il diritto di ricevere una copia personale dei dati oggetto di trattamento nonché l'indicazione del periodo di conservazione.

La dottrina ha identificato i principi di legalità algoritmica come una macro categoria di garanzie procedurali "rafforzate"<sup>162</sup>.

In definitiva, ciò che rileva, al fine di assicurare le garanzie procedurali "tipiche", è che occorre prevedere sempre una interlocuzione istruttoria con il responsabile del procedimento e l'accesso partecipativo. Il responsabile del

---

*trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.*

<sup>162</sup> Vedasi F. NASSUATO, *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedurali*, in Ceridap, 2022.

procedimento<sup>163</sup> assume un ruolo diverso ma sempre centrale, di conduzione di tutto l'iter procedimentale quale garante di una gestione spersonalizzata del procedimento. L'apporto collaborativo e di intermediazione del responsabile diventa necessaria per legittimare democraticamente la decisione amministrativa automatizzata, soprattutto laddove il responsabile, avrà un rapporto collaborativo e partecipativo con il privato consentendogli una partecipazione all'azione amministrativa automatizzata piena.

Mentre il procedimento "tradizionale" amministrativo è caratterizzato da una suddivisione in fase dell'iniziativa, istruttoria e decisoria, nel procedimento automatizzato c'è una compressione della suddivisione in fasi e per questo la fase di apertura del contraddittorio avverrà tra il momento in cui viene adottata la decisione automatizzata per il tramite dell'algoritmo e la trasformazione da parte del responsabile del procedimento in provvedimento finale. In tal modo, i principi di conoscibilità e non esclusività saranno rispettati, in modo tale che l'interessato potrà partecipare confermando le determinazioni della macchina o correggerla, tutto ciò consente di favorire una integrazione dell'algoritmo indispensabile per le prerogative dell'interessato nell'attività amministrativa.

La dottrina ha avviato un tentativo di identificazione dei vizi del provvedimento in presenza di una violazione della legalità algoritmica<sup>164</sup>.

---

<sup>163</sup> L'articolo 5 della legge 241 del 1990 prevede che "1. Il dirigente di ciascuna unità organizzativa provvede ad assegnare a sé o altro dipendente addetto all'unità la responsabilità dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento nonché, eventualmente, dell'adozione del provvedimento finale. 2. Fino a quando non sia effettuata l'assegnazione di cui al comma 1, è considerato responsabile del singolo procedimento il funzionario preposto alla unità organizzativa determinata a norma del comma 1 dell'articolo 4.3. L'unità organizzativa competente, il domicilio digitale e il nominativo del responsabile del procedimento sono comunicati ai soggetti di cui all'articolo 7 e, a richiesta, a chiunque vi abbia interesse."

<sup>164</sup> Si veda C. TASSO, Attori, processi, meriti e responsabilità nell'utilizzo di algoritmi di Intelligenza Artificiale: Il caso del Machine Learning, in L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale, a cura di Roberto Cavallo Perin, Università degli studi di Torino, 2020, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino, pp 19 e ss; E. BELISARIO – F. RICCIULLI, *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 159 e ss.

In particolare, gli algoritmi, se vengono utilizzati nel procedimento amministrativo, devono essere programmati per rispettare le norme al fine di non incorrere in una violazione di legge.

Nel contesto algoritmico, l'eccesso di potere, invece, laddove l'amministrazione faccia un cattivo uso del potere assegnatogli come nell'ipotesi di delega incontrollata in cui l'amministrazione decide di delegare una decisione determinante a un sistema algoritmico senza una supervisione umana oppure laddove l'amministrazione vada a manipolare al fine di favorire un determinato risultato, l'algoritmo.

Di conseguenza, l'algoritmo potrebbe arrivare a generare delle decisioni sproporzionate determinando un'incertezza sistemica in assenza di una normativa idonea a controllare i vizi procedimentali.

Orbene, ciò determinerà non solo violazioni della normativa interna ma ad oggi anche del contesto europeo come il GDPR poiché è inevitabile in presenza di vizi procedimentali legati al procedimento algoritmico incorrere anche in violazioni del trattamento dei dati personali come in caso di mancata trasparenza, oppure del nuovo regolamento sull'AI.

In conclusione, importante è un costante aggiornamento delle garanzie partecipative che deve procedere sulla stessa strada dell'innovazione tecnologica adeguandosi alle peculiarità dei nuovi sistemi. È evidente l'esigenza di individuare delle garanzie idonee per il cittadino rispetto all'esercizio del potere pubblico anche in un'ottica "algoritmica".

Necessario sarà un intervento concreto del legislatore al fine di mantenere intatta la separazione dei poteri e assicurare la certezza del diritto, delineando le coordinate per garantire la trasparenza nonché la partecipazione anche nei procedimenti automatizzati proprio come ha agito per il procedimento amministrativo tradizionale mediante la legge 241 del 1990. L'applicazione delle regole del procedimento amministrativo al procedimento algoritmico non consente di tutelare tutti quei diritti fondamentali che richiedono una tutela

forte alla luce delle nuove tecnologie e sarebbe anche non idonea rispetto al nuovo scopo da perseguire.

È evidente che non è abbastanza l'approccio volto a sopperire ad una lacuna normativa in mancanza di un tempestivo adeguamento al contesto tecnologico del giudice amministrativo nella creazione delle regole algoritmiche sino a qui delineate.

Allo stato degli atti, il giudice amministrativo ha avuto un ruolo importante, ma oggi è fondamentale nel rispetto della certezza del diritto e della legalità un concreto intervento del legislatore, al fine di evitare un “*creazionismo giurisprudenziale*”<sup>165</sup>.

Il potere giudiziario è sempre più spesso chiamato a intervenire in ausilio della legislazione.

Oltre al principio di separazione dei poteri ciò che viene dequotato è anche la soggezione dei giudici alla legge e ciò determina una forte incertezza giuridica nonché una disomogeneità applicativa.

Si auspica un intervento del legislatore volto a delineare il perimetro di una regolamentazione sul procedimento amministrativo automatizzato rispettosa della trasparenza e a garanzia della partecipazione dell'interessato.

## **5. Il necessario bilanciamento tra trasparenza algoritmica e protezione dei dati personali.**

Con l'arretramento della centralità del funzionario “umano” e con l'avanzata verso i sistemi automatizzati, si è visto come è diventato necessario sempre di

---

<sup>165</sup> Per un approfondimento vedasi F. PATRONI GRIFFI, *Il giudice amministrativo oggi: ruolo, etica, responsabilità*, Relazione introduttiva al Primo congresso nazionale dei Magistrati amministrativi, Palazzo Spada, 7-8 giugno 2019, in [www.giustizia-amministrativa.it](http://www.giustizia-amministrativa.it); A. TRAVI, *Eccesso di potere giurisdizionale e diniego della giurisdizione dei giudici speciali al vaglio delle Sezioni Unite della Cassazione*, intervento al Seminario di Studi tenutosi presso la Corte di Cassazione di Roma, 21 settembre 2017; C. MEOLI, *Il declino della legge statale*, in *Libro dell'anno del Diritto*, Roma, 2013.

più un ripensamento delle garanzie procedurali dell'individuo nel rapporto con il potere pubblico<sup>166</sup>.

In realtà ciò che occorre effettuare al fine di comprendere le forme di tutela effettive dei dati nel sistema attuale è comprendere se la maggiore autonomia acquisita da parte della macchina anche nel settore pubblico, stia portando il sistema a preferire un sistema in cui si vuole privilegiare l'efficienza della tecnologia a discapito dell'essere umano oppure, se il sistema sia comunque in grado anche a fronte dell'evoluzione tecnologica di tener conto dell'importanza di mantenere l'essere umano al centro del sistema tenendo conto sicuramente dell'importanza di una interrelazione – uomo macchina ma non dimenticando la protezione dei diritti fondamentali.

Ebbene, la ricerca di una regolamentazione sistemica sia dal punto di vista della protezione dei dati personali come si è visto nel GDPR che nel nuovo approvato regolamento su AI va in entrambi i casi verso una strada in cui l'uomo non sia mai subordinato, scavalcato, dall'algoritmo e dall'Intelligenza artificiale<sup>167</sup>. Nella normativa analizzata è emersa l'importanza di strumenti a servizio dell'uomo in cui non c'è una sostituzione ma un rapporto di interrelazione tra macchina e uomo, per migliorarsi a vicenda e garantire i principi fondamentali quali la trasparenza l'affidabilità la non discriminazione la riservatezza e il principio democratico.

In ragione di ciò, occorre porre in luce il ruolo attribuito alla trasparenza. Secondo alcuni autori, da un lato, essa potrebbe essere vista come la retta via verso una governance migliore dell'algoritmo, dall'altro lato, deve anche essa essere in grado di adattarsi a dei sistemi in continua evoluzione.

---

<sup>166</sup> Si veda P. CARROZZA, *Governo e amministrazione*, in *Diritto costituzionale comparato*, a cura di P. Carrozza, A. Di Giovine e G.F. Ferrari, Laterza, Roma – Bari, 2017.

<sup>167</sup> Si veda, P. STANZIONE, *L'uomo e le macchine: una visione antropocentrica dell'Intelligenza Artificiale*, in *AI Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il mulino, 2022.

È ovvio che le procedure automatizzate entrano in crisi con la trasparenza soprattutto dal punto di vista della comprensione di tutto l'iter procedurale seguito.

Nello specifico, la questione che investe il ruolo della trasparenza riguarda in particolare, il tema della conoscibilità del software utilizzato con la richiesta del codice sorgente.

La dottrina<sup>168</sup>, si è interrogata sulla concreta necessità imprescindibile di conoscenza del codice sorgente e sulla sua conseguente opacità.

Il codice sorgente di un software è il testo di un algoritmo di calcolo scritto secondo un linguaggio cosiddetto di “programmazione” idoneo a definire tutto il flusso di esecuzione del programma.

Orbene, da un lato, la possibilità concreta di conoscere il modo in cui l'algoritmo opera e “pensa” potrebbe secondo alcuni garantire il diritto della persona ad essere assoggettato a decisioni motivate e conformi alla legge seppur incidenti sulla sua sfera giuridica, dall'altro, comporta la delicata questione relativa al fatto che il codice di programmazione che si vuole conoscere potrebbe essere oggetto di un diritto tutelato come opera dell'ingegno o dal diritto d'autore.

Il giudice amministrativo<sup>169</sup> ha concesso anche in passato l'ostensione al codice sorgente ritenendo non sussistenti le ragioni di tutela della riservatezza anche laddove l'amministrazione riteneva che mediante l'accesso al codice sorgente il pericolo è quello di decriptare e gestire i dati inseriti nel programma con un problema di trattamento dei dati personali.

Indagare il funzionamento dell'algoritmo ha la finalità di verificare e comprendere dall'interno le decisioni prese in autonomia dalla macchina al fine di contemperarle con i diritti garantiti dalla Costituzione.

---

<sup>168</sup> Vedasi, A. CORRADO, *La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, in Osservatorio sulla trasparenza in Federalismi, 22 febbraio 2023.

<sup>169</sup> TAR Lazio, Sez. III Bis, 22 marzo 2017, n.3769.

Si è avuto modo di esporre che i dati sono il motore delle procedure automatizzate, poiché le nutrono e dunque la frequente ricerca di una tutela rafforzata per il funzionamento degli algoritmi sia nel settore pubblico che nel settore privato richiede di tener conto della protezione dei dati personali e non personali.

La garanzia per l'interessato circa la trasparenza dell'algoritmo, gli consente di indagare sul motivo che ha portato a una decisione e di rispondere a garanzie costituzionali in ambito sia giudiziario che amministrativo ai sensi dell'articolo 3 della legge 241 del 1990 nonché articolo 111 della Costituzione.

Gli algoritmi sono diventati uno strumento necessario per l'uomo nelle decisioni in ambito tecnologico.

Tale contesto, come si è anticipato e come si avrà modo di esporre nel successivo capitolo relativo al fenomeno dei Big data e degli Open data, è caratterizzato da una quantità di dati in continuo aumento nonché dalla presenza di macchine dotate di una forte potenzialità di calcolo a costi sempre ridotti.

Tuttavia, ciò che occorre rilevare è che non si può immaginare la presenza di sole macchine senza la supervisione dell'essere umano.

Ebbene, esercitare un controllo di supervisione sulla decisione automatizzata indirizza la progettazione dell'algoritmo verso un insieme di valori più compatibili con i diritti costituzionalmente garantiti<sup>170</sup>.

Nel capitolo successivo si analizzerà condivisione dei dati tra pubbliche amministrazione e le problematiche di riferimento cercando di comprendere le conseguenze giuridiche e le forme di tutela.

In definitiva, sarà necessario un contemperamento, soprattutto nel settore pubblico, tra l'approccio giuridico e l'approccio tecnologico alla protezione

---

<sup>170</sup> Sul tema, M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Editoriale Scientifica 2023.

dei dati personali<sup>171</sup> cercando soluzioni concrete idonee a tutelare gli interessati e ridefinendo i parametri della legalità algoritmica. La condivisione dei dati tra pubbliche amministrazioni è considerata il punto di partenza per la strategia europea sui dati laddove avverrà nel rispetto delle norme in materia di protezione dei dati personali. In altri termini, protezione e condivisione dei dati sembrano porsi in conflitto ma in un'ottica vincente dovranno essere riconciliati soprattutto nel settore pubblico dove le amministrazioni potranno sviluppare politiche e strategie migliori sia a livello locale che centralizzato auspicando di arrivare ad una governance trasparente, informata e con servizi pubblici garantiti più efficienti<sup>172</sup>.

Le tecniche di intelligenza artificiale, sono diventate uno strumento irrinunciabile per il supporto di ogni sistema che preveda un processo di analisi e acquisizione completa di informazioni.

Tuttavia, a prescindere dalla loro indubbia utilità, evidente è il fatto che le nuove tecniche debbano essere utilizzate con oculatezza e in conformità con la normativa eurounitaria e nazionale di ogni singolo stato membro al fine di evitare di intraprendere un comportamento scorretto per una mancata, o meglio non completa sperimentazione<sup>173</sup>.

---

<sup>171</sup> Vedasi, G. D'ACQUISTO, in *Intelligenza artificiale, sicurezza nazionale e difesa*, in AI Anthology Profili giuridici, economici e sociali dell'Intelligenza Artificiale, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il Mulino, 2022, pp 309 e ss; N. RANGONE, *Intelligenza Artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli, con prefazione di M. Clarich, Giappichelli, 2022.

<sup>172</sup> Così G. D'ACQUISTO, *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p.204 e ss.

<sup>173</sup> Così M. PANDOLFI, in *Intelligenza artificiale, sicurezza nazionale e difesa*, in AI Anthology Profili giuridici, economici e sociali dell'Intelligenza Artificiale, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il Mulino, 2022. pp 513 e ss.

## CAPITOLO III

# I DATI IN MANO PUBBLICA: TRA ORGANIZZAZIONE AMMINISTRATIVA E INFRASTRUTTURE STRATEGICHE

SOMMARIO: **1.** Premessa: L'evoluzione tecnologica e i dati in mano pubblica, quali problemi? **2.** Big Data e Open Data: tra innovazione e criticità in un ordinamento democratico. **3.** L'organizzazione amministrativa nella gestione dei dati pubblici: dal modello Government as a platform al Polo strategico Nazionale. **4.** Cloud nazionale: tra utopia e primi problemi applicativi.

### **1. Premessa: l'evoluzione tecnologica e i dati in mano pubblica, quali problemi?**

Per comprendere al meglio le conseguenze derivanti dalla sostituzione degli archivi tradizionali – quale unico strumento di conservazione delle informazioni nella mano pubblica – con i nuovi strumenti offerti dalle nuove tecnologie della comunicazione e informazione anche nel contesto pubblico, occorre principiare la presente analisi dal verificare in concreto, come e con quali strumenti, l'evoluzione tecnologica, abbia determinato una rimodulazione della modalità di gestione dei dati per le pubbliche amministrazioni.

Ebbene, per mezzo di tale “riadattamento sistematico” alla luce del nuovo contesto economico e sociale, l'amministrazione è arrivata a conoscere

fenomeni come la catalogazione, indicizzazione, strutturazione dei dati contenuti in archivi digitali<sup>174</sup>.

In particolare, le informazioni detenute dalla pubblica amministrazione sono passate dall'assumere una veste statica ad una veste dinamica in virtù dei nuovi strumenti offerti dalla tecnologia dell'informazione e della comunicazione che ha consentito il passaggio da cataloghi di informazioni e dati detenuti in meri supporti cartacei e archivi a banche dati digitali<sup>175</sup>.

Occorre rilevare che i dati per essere detenuti in forma digitale devono essere ricordati, o meglio, memorizzati su strumenti di supporto materiale idonei a detenerli. Le pubbliche amministrazioni necessitano di strumenti di supporto specifici e idonei a ricomprendere un numero complesso di dati.

Infatti, le banche dati delle pubbliche amministrazioni hanno una struttura differente per mezzo del quale, vi sono dei *data center* specifici e organizzati deputati alla memorizzazione dei dati con la funzione di accentrare in un unico luogo la conservazione dei dati stessi<sup>176</sup>.

Sin dalle prime implementazioni di tali sistemi di c.d cloud nazionale da parte delle pubbliche amministrazioni per i trattamenti svolti nel settore pubblico, si è arrivati sin da subito a parlare di principio del *cloud first*, secondo cui la pubblica amministrazione deve piano piano convertirsi alla tecnologia del

---

<sup>174</sup> Sul tema si veda F. DI PORTO, *Opacità algoritmica e trasparenza delle decisioni amministrative*, in *L'amministrazione pubblica con i Big Data: Da Torino un dibattito sull'intelligenza artificiale*, a cura di Roberto Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli studi di Torino; L. TORCHIA, *Lo stato digitale una introduzione*, Il Mulino, 2023, pp. 17 e ss.; B. BOSCHETTI, *La transizione della pubblica amministrazione*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli con prefazione di M. Clarich, Giappichelli, 2022, p. 3 e ss.

<sup>175</sup> L'articolo 1 comma 2 della Direttiva 96/9/CE sulla tutela giuridica delle banche dati recepito dal legislatore all'articolo 1, comma 1, n. 9, della Legge 22 aprile 1941, n. 633 prevede che "*Per banca dati si intende una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo*".

<sup>176</sup> Sul tema vedasi il contributo di F. CARDARELLI, *Le banche dati pubbliche: una definizione*, in *Il diritto dell'informatica*, 2022, volume 18, p.321 e ss.

cloud, il quale sta arrivando ad assurgere a criterio regolativo essenziale della transizione digitale nella pubblica amministrazione<sup>177</sup>.

In particolare, i sistemi di cloud richiedono come si analizzerà nel proseguio, una struttura radicata nel territorio con un centro caratterizzato da uno standard alto di qualità, sicurezza e indipendenza per i dati detenuti dalla pubblica amministrazione, soprattutto al fine di ottimizzare sempre di più i sistemi e proteggerli da minacce informatiche<sup>178</sup>.

Occorre dunque svolgere un'analisi evolutiva e articolata della digitalizzazione dell'azione pubblica tentando di comprendere i fenomeni di *Big Data* e *Open Data* nella nuova dimensione tecnologica al fine di comprendere i nuovi strumenti utilizzati dalla pubblica amministrazione nonché le prospettive future e le criticità. Ebbene, la digitalizzazione dell'attività delle amministrazioni pubbliche, ha determinato una trasmissione continua e a tratti intermittente di dati anche di ingenti dimensioni relativi a un patrimonio prezioso di conoscenze che ha richiesto e continua a richiedere delle tutele forti. L'ordinamento nazionale, allo stato attuale, è in grado di abbracciare un nuovo sistema al fine di realizzare una digitalizzazione anche del settore pubblico e di implementare gli strumenti rispetto al passato ma non si può tenere nell'ombra la criticità più grande derivante dal fatto che il flusso di dati personali del privato trasmessi inevitabilmente alle pubbliche amministrazioni a fini conoscitivi, conservativi, manipolativi, anche alla luce di un trattamento bilanciato, proporzionato e trasparente può determinare delle conseguenze pregiudizievoli e indesiderate sulla sfera personale del privato

---

<sup>177</sup> Si veda A. SORO, *Dati e democrazia*, in *Il ruolo del garante per la protezione dei dati personali, La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. CERRINA FERONI, 2024, p. 94 e ss.

<sup>178</sup> Si veda S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021; L. TORCHIA, *Lo Stato digitale e i nuovi stati digitali*, in *Lo Stato digitale una introduzione*, Il Mulino Itinerari, 2023.

proprio alla luce dei volumi ingenti di dati personali che diventano “incontrollabili” nella loro duttilità e velocità<sup>179</sup>.

Le nuove tecnologie consentono ormai l’utilizzo di dati personali da parte delle amministrazioni pubbliche e delle imprese private per lo svolgimento di ogni attività. Occorre dunque considerare che tale evoluzione tecnologica va di pari passo con l’esigenza primaria di efficaci misure di attuazione al fine di creare un clima idoneo a garantire lo sviluppo concreto di un’economia digitale del mercato interno garantito da un sistema di fiducia del cittadino nell’amministrazione con un controllo concreto sulla circolazione dei propri dati per rafforzare la certezza e la conoscenza circa l’utilizzabilità e il circuito di trasferimento del proprio dato<sup>180</sup>.

È proprio l’Anac con deliberazione del 20 dicembre 2017 n. 1301 ha individuato i problemi di un’acquisizione di documenti e dati indiscriminata immaginando in concreto nel nuovo scenario un regime condizionato solo dall’effettività e dal bisogno di conoscenza del dato per il perseguimento di finalità pubbliche per evitare di mettere a repentaglio la tutela del dato del soggetto coinvolto in decisioni amministrative.

In altri termini, il fulcro principale si è spostato dal problema del “come viene acquisito il dato” al come possa essere svolta una “corretta diffusione”. Invero, una pubblicazione di dati su siti web istituzionali non prevista dalla legge determina una nuova “vulnerabilità” della sfera personale del soggetto interessato. In ragione di ciò, il Regolamento generale per la protezione dei dati personali (UE) 2016/679, General Data Protection Regulation<sup>181</sup> richiede

---

<sup>179</sup> Sul tema si veda S. TOSCHEI, *I trattamenti in ambito pubblico nell’era della digitalizzazione e della trasparenza*, in *Innovazione tecnologica e valore della persona*, L. CALIFANO E C. COLAPIETRO, Editoriale scientifica, p.433 e ss, 2020.

<sup>180</sup> Così S. TOSCHEI, *I trattamenti in ambito pubblico nell’era della digitalizzazione e della trasparenza*, in *Innovazione tecnologica e valore della persona*, L. CALIFANO E C. COLAPIETRO, Editoriale scientifica, p. 437, 2017.

<sup>181</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera

un monitoraggio costante e penetrante sull'esercizio da parte delle pubbliche amministrazioni del potere di pubblicazione in modo corretto e sulla gestione equilibrata dell'accesso<sup>182</sup>.

In definitiva, secondo autorevole Dottrina<sup>183</sup>, il pregiudizio ricollegato alla diffusione illecita e indiscriminata dei dati, diventa un vulnus non emendabile e dunque, di conseguenza, l'illecito trattamento dei dati da parte delle pubbliche amministrazioni non può in alcun modo trovare una tutela nel solo ristoro economico del danno subito.

Il Garante per la protezione dei dati personali, congiuntamente all'Anac, mediante linee guida condivise delinea di pari passo con l'evoluzione tecnologica il perimetro per un esercizio bilanciato dello strumento della diffusione dei dati e della condivisione con le amministrazioni al fine di assicurare in virtù dell'attuazione del Regolamento europeo e del principio cardine di *accountability*, una tutela effettiva della sfera personale dell'individuo laddove non sia necessario a nessuna finalità l'ostensione dei dati<sup>184</sup>.

---

circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

<sup>182</sup> Vedasi S. TOSCHEI, *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*, in *Innovazione tecnologica e valore della persona*, L. CALIFANO E C. COLAPIETRO, Editoriale scientifica,

<sup>183</sup> Si veda R. CAVALLO PERIN, *Pubblica amministrazione e data analysis*, in *L'amministrazione pubblica con i Big Data: Da Torino un dibattito sull'intelligenza artificiale*, a cura di Roberto Cavallo Perin, Università di Torino, 2021.

<sup>184</sup> Sul rapporto tra riservatezza e trasparenza vedasi *ex multis* A. CORRADO, *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018; M.A. SANDULLI – L. DROGHINI, *La trasparenza amministrativa nel FOIA italiano. Il principio della conoscibilità generalizzata e la sua difficile attuazione*, in *Federalismi.it*, 2020; P. CANAPARO, *La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni*, in *Federalismi.it*, 2020.

## ***2. Big Data e Open Data: tra innovazione e criticità in un ordinamento democratico.***

A questo punto dell'analisi, occorre verificare in concreto le implicazioni positive e negative derivanti da una particolare tipologia, o meglio, macrocategoria di dati in mano pubblica conosciuti come *Big Data*<sup>185</sup>.

La nostra era è connotata da una datizzazione della realtà in cui ogni fenomeno, ogni evento, è convertito in dato e divenuto calcolabile<sup>186</sup>.

Le nuove tecnologie hanno consentito un aumento esponenziale<sup>187</sup> di quantità di dati prodotti rispetto al passato.

Al fine di comprenderne il perché dell'utilizzo nonché l'uso diffuso del termine, appare opportuno soffermarsi sulla definizione.

Ebbene, con la definizione di *Big Data* si individuano una serie di dati estesi caratterizzati da volume, varietà intesa come strutture di dati eterogenee, velocità<sup>188</sup> e variabilità<sup>189</sup>. Oggi, il riferimento è anche la qualità del dato nonché la sua capacità concreta di trasformarsi mediante la propria elaborazione<sup>190</sup>.

---

<sup>185</sup> Sulle nozioni di Big Data vedasi M. DELMASTRO – A. NICITA, *Big Data, come stanno cambiando il nostro mondo*, Bologna, Il Mulino, 2019; G. PASCUZZI, *Big Data*, in *Il diritto dell'era digitale*, Il mulino, p.265 e ss, 2020; R. KITCHIN, G. MCARDLE, *What Makes Big Data? Exploring the Ontological Characteristics of 26 Datasets*, in *Big Data & Society*, 1, 2016, p. 1 ss; V. MAYER-SCHONBERGER, K.N. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, trad. it. a cura di R. Merlini, Garzanti, Milano, 2013; S. LEONELLI, *La ricerca scientifica nell'era dei Big Data*, Meltemi, Milano, 2018; A. MANTELETO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 1, 2012; R. MORO VISCONTI, *Valutazione dei Big data e impatto su innovazione e digital branding*, in *Il Diritto industriale*, 1, 2016; J. SHKABATUR, *The Global Commons of Data*, in *Stanford Technology Law Review*, 22, 2019; G. AZZONE – F. CAIO, *In un mare di dati. Quali dati per le politiche, quali politiche per i dati*, Milano, Mondadori, 2020.

<sup>186</sup> Sul tema, P. FALLETTA, *La riforma delle amministrazioni pubbliche, tra piattaforme interoperabili e atti amministrativi digitali*, in *Federalismi.it*, 27 dicembre 2023.

<sup>187</sup> Si veda anche V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2019, p. 32.

<sup>188</sup> Rapidità nella creazione, trasmissione, archiviazione visualizzazione.

<sup>189</sup> Vedasi G. PASCUZZI, *Big Data*, in *Il diritto dell'era digitale*, Il mulino, p.265 e ss, 2020.

<sup>190</sup> Si veda L. TORCHIA, *Lo Stato digitale una introduzione*, il Mulino, 2023 p. 17 e ss.

La ragione principale dell'introduzione dei *Big Data* è da rinvenirsi nell'evoluzione tecnologica che ha determinato l'esigenza di introdurre dei nuovi sistemi di raccolta di dati. Tale evoluzione, ha prodotto inoltre dei nuovi aspetti di relazioni introducendo l'esigenza di nuove regole. In particolare, essa ha determinato una trasformazione delle abitudini individuali determinando una asimmetria tra il tempo veloce di cambiamento e il tempo di reazione da parte della società e del potere pubblico determinando un fenomeno difficilmente controllabile nel tempo<sup>191</sup>.

È vero che la finalità primaria è stata quella di ottenere un'analisi di dati efficiente ed economica e conforme all'evoluzione tecnologica e ai nuovi strumenti a disposizione ma non si può nascondere il fatto che la diffusione di strumenti innovativi ha aumentato la disponibilità dei dati a disposizione ma dall'altro lato ha compromesso alcuni equilibri sociali ed economici che si erano sedimentati nel tempo.

La possibilità di utilizzare Internet come la sola piattaforma ha condotto ad un fenomeno di aggregazione di dati che già esisteva ma che con le nuove tecnologie si è rivelato sempre più incontrollabile e diffuso.

Ebbene, già nell'epoca precedente all'introduzione dei Big Data si è passati dalla gestione di dati non aventi alcuna struttura ad una gestione efficiente di dati più strutturati e dunque organizzati sulla base di regole predefinite mediante l'utilizzo iniziale di database relazionali<sup>192</sup> secondo una struttura che descrive le loro caratteristiche e interrelazioni. Ciò in quanto, il precedente sistema non era più idoneo a gestire con efficienza il bisogno di un'analisi di dati di ampio volume e a volte non strutturati. La peculiarità - che spesso porta ad una mancata comprensione del problema - della rivoluzione dei *Big Data* ha investito non tanto il solo volume formale del dato, quanto plurimi ordini di aspetti.

---

<sup>191</sup> Vedasi L. TORCHIA, *Lo Stato digitale*, Il Mulino, pp. 21 e ss, 2023.

<sup>192</sup> La struttura del dato è utilizzata mediante un database di relazioni.

I *Big Data*<sup>193</sup> sono masse di dati fruibili mediante software specifici in grado di estrapolare il valore conoscitivo che l'insieme dei dati e non il singolo dato considerato in sé per sé è in grado di esprimere verso l'esterno. Alcuni<sup>194</sup>, in dottrina fanno riferimento a un “*data lake*” in virtù dell'ampiezza, dove ciò che rileva è l'insieme dei dati che portano a un risultato e non il volume considerato sul piano sostanziale del singolo.

Occorre evidenziare gli impatti che ha avuto nella crescita sul piano tecnologico.

In primo luogo, l'utilizzo dei Big Data è stato determinato dalla velocità di calcolo dei microprocessori, alla grande capacità delle schede di memoria e alla *data analytics* mediante la quale, l'analisi del dato viene effettuata al fine di comprendere, visualizzare, quantificare e interpretare il grande numero di dati<sup>195</sup>, in altri termini, l'avvento di tale tipologia di dati ha reso doverosa un'analisi nuova, con tecniche e metodologie specifiche volti appunto ad estrarre conoscenza del dato e reinterpretarla nell'insieme arrivando ad una rimodulazione dei modi e delle tecniche di gestione dei dati da parte anche delle amministrazioni.

L'estensione del fenomeno dei *Big Data* ha consentito alle pubbliche amministrazioni di analizzare in tempo reale volumi di dati provenienti da imprese, privati o aziende mediante la tecnica dell'analisi per mezzo di incrocio di dati rendendo, o meglio, “promettendo di rendere” veloci ed efficaci le modalità con cui si diffonde e acquisisce conoscenza.

---

<sup>193</sup> L'Agid nel Piano triennale per l'informatica nella Pubblica Amministrazione 2017 -2019 li ha definiti come un insieme di dati da memorizzare e/o elaborare di dimensioni così grandi, e/o con una varietà di formati così elevata, e/o con una velocità di crescita così alta da richiedere l'uso di software non convenzionali.

<sup>194</sup> Vedasi G. CARULLO, *Dati, banche dati, blockchain e interoperabilità dei sistemi informatici*, in Il diritto dell'amministrazione pubblica digitale, a cura di R. Cavallo Perin – D. U. Galetta, Giappichelli Editore, Torino, 2020 p. 197 e ss.

<sup>195</sup> Si veda G. RACCA, *La digitalizzazione dei contratti pubblici: adeguatezza delle pubbliche amministrazioni e qualificazione delle imprese*, in Il diritto dell'amministrazione pubblica digitale, a cura di R. Cavallo Perin – D. U. Galetta, Giappichelli Editore, Torino, 2020 p. 321 e ss; G. PASCUZZI, *Big Data*, in *Il diritto dell'era digitale*, Il mulino, p.265 e ss, 2020.

La rivoluzione<sup>196</sup> vera e propria dei Big Data è strettamente connessa con il significato intrinseco di Open data.

Le due nozioni non devono essere considerate dei sinonimi, bensì sono concetti distinti che si completano a vicenda.

Infatti, mediante un'analisi è possibile rinvenire un set di dati "open" non qualificabile come "big data" nonché un insieme agglomerato di big data non accessibili e aperti.

Con specifico riguardo al settore pubblico, il vasto numero di dati che vengono processati viene racchiuso nell'ambito della categoria dei *Big Data*.

Ai fini della presente analisi, incentrata sul ruolo dei Big Data nel contesto pubblico, occorre analizzarne anche le eventuali criticità future nonché delle prime riflessioni.

In primo luogo, una criticità che porta a riflettere è il fatto che i *Big data* sono costituiti principalmente da singoli dati personali che richiedono una tutela particolarmente stringente con specifico riguardo al loro trattamento sia individuale che nella "massa" in virtù del Regolamento generale per la protezione dei dati personali e del Codice della Privacy.

Prima di analizzare la predisposizione dei Big Data ad essere "*Open Data*" nonché il significato racchiuso anche in tale definizione, occorre fare una premessa ponendo in luce il fatto che l'apertura dei dati soprattutto nel settore pubblico nonostante alcuni crismi di criticità è stata determinante ai fini dello sviluppo economico poiché le nuove tecniche "*open*" hanno come scopo

---

<sup>196</sup> Di rilievo, è il fatto che l'Autorità Garante della Concorrenza e del Mercato insieme al Garante per la protezione dei dati personali e all'Autorità per le garanzie nelle comunicazioni hanno pubblicato un'*indagine conoscitiva sui Big Data* al fine di sottolineare la necessità di una normativa volta a garantire la trasparenza nell'utilizzo delle informazioni nonché di esplicitare il significato di "*estrazione di conoscenza*" contenitore delle micro categorie di elaborazione, raccolta quale generazione, acquisizione e memorizzazione nonché interpretazione dei dati.

primario il contenimento dei costi, un utilizzo intelligente del digitale nel settore pubblico, nonché un miglioramento dei servizi forniti<sup>197</sup>.

Il termine Open data<sup>198</sup>, trae la sua origine dall'esperienza statunitense e descrive un modo di essere "aperto" dei dati e accessibile<sup>199</sup> in diversi contesti e per plurime finalità.

In particolare, è un'impostazione che prevede un'apertura della pubblica amministrazione al cittadino, in virtù del principio di trasparenza<sup>200</sup>.

Sul piano normativo, il d.lgs. 82/2005 (Codice dell'Amministrazione Digitale) ha delineato una definizione giuridica degli stessi all'articolo 1, comma 1, lett. 1 ter stabilendo che sono da ricomprendere nella categoria di dati di tipo aperto *"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*

---

<sup>197</sup> Si veda U. PAGALLO, *Big data open data e black box society*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, p. 49 e ss, Università degli studi di Torino, 2021.

<sup>198</sup> Il portale dati.gov.it alimenta il Portale europeo dei dati e contiene il catalogo nazionale dei dati rilasciati in formato aperto dalle pubbliche amministrazioni italiane, attraverso cui, l'Agid promuove la valorizzazione delle informazioni sul piano nazionale.

<sup>199</sup> Vedasi G. CARULLO, *Dati, banche dati, blockchain e interoperabilità dei sistemi informatici*, in *Il diritto dell'amministrazione pubblica digitale*, a cura di R. Cavallo Perin – D. U. Galetta, Giappichelli Editore, Torino, 2020 p. 194 e ss.

<sup>200</sup> Si veda A. CORRADO, *Il principio di trasparenza*, in M. A. SANDULLI, (a cura di), *Principi e regole dell'azione amministrativa*, Giuffrè Editore, Milano, 2023; A. CORRADO *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018; M.R. SPASIANO, *I principi di pubblicità. Trasparenza e imparzialità*, in *Codice dell'azione amministrativa*, (a cura di) M. A. SANDULLI, Milano, 2017; C. COLAPIETRO – A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, a cura di C. COLAPIETRO – L. CALIFANO, Editoriale Scientifica, Napoli, 2014, pp. 117 e ss; M. A. SANDULLI, *Voce Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, IV aggiorn., Milano, 2000; V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte Costituzionale (n. 20/2019)*, in *federalismi.it*, n. 5, 2020; P. CANAPARO, *La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni*, in *Federalismi.it*, 2014; A. SIMONATI, *La ricerca in materia di trasparenza amministrativa: stato dell'arte e prospettive future*, in *Dir. amm.*, 2018.

da parte di programmi per elaboratori e sono provvisti dei relativi metadati;  
3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36.”

La presente analisi, non può non soffermarsi sul tema della *data quality*<sup>201</sup> poiché se le pubbliche amministrazioni fanno uso di dati, i cittadini, devono poter fare affidamento sulla qualità delle informazioni a cui hanno accesso<sup>202</sup> anche e soprattutto in virtù del principio democratico. Il problema nasce sul piano delle modalità idonee ad assicurare una qualità dal punto di vista solo oggettivo del dato poiché è evidente che ciò che viene a mancare è lo schermo umano nella formazione, trattamento e accesso al dato rilevante. In ragione di ciò, si è passati da un regime di garanzia di qualità soggettivo del processo conoscitivo del dato a una qualità meramente oggettiva dove viene a mancare il prius logico dato dalla partecipazione umana. Inoltre, occorre rilevare che il dato “open” utilizzato dalle pubbliche amministrazioni mediante sistemi informativi interoperabili di altre pubbliche amministrazioni, laddove sia un dato di “cattiva qualità”, va a generare e produrre diverse tipologie di errori che si riflettono anche sul piano dei costi e produce inefficienze determinando una cattiva qualità dei servizi oltre che una disparità di trattamento.

Nell'ordinamento nazionale non c'è un espresso riferimento al tema, tuttavia, si avverte l'esigenza sempre più forte di caratterizzare il sistema di garanzia da

---

<sup>201</sup> Vedasi E. CARLONI, *Qualità dei dati, big data e amministrazione pubblica*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino; E. CARLONI, v, in B. Ponti (a cura di), *il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, Rimini, 2008.

<sup>202</sup> Sul tema, S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino, 1973; L. CALIFANO – C. COLAPIETRO, *Innovazione tecnologica e valore della persona, il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, 2017.

parte delle pubbliche amministrazioni della qualità dei dati nei portali istituzionali implicitamente assicurandone il più possibile completezza, comprensibilità, tempestività e costante aggiornamento<sup>203</sup>. In altri termini, assicurarne la completezza comprensibilità e il costante aggiornamento è sintomo di qualità degli stessi.

Secondo parte della dottrina<sup>204</sup> che studia il tema, l'importanza della qualità dei dati utilizzati dalle pubbliche amministrazioni è legata alla prospettiva del loro riutilizzo e ciò è possibile rinvenirlo in toto anche e soprattutto nella normativa europea relativa al trattamento dei dati personali dove l'articolo 5<sup>205</sup> relativo ai principi applicabili in tema di protezione dei dati personali ingloba una forte tutela relativa alla necessaria ricerca di qualità del dato trattato e ciò

---

<sup>203</sup> L'articolo 6 del decreto legislativo 33 del 2013 prevede che *“Le pubbliche amministrazioni garantiscono la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti dalla legge, assicurandone l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, nonché la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità secondo quanto previsto dall'articolo 7. L'esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l'omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti.”*

<sup>204</sup> Sempre E. CARLONI, *Qualità dei dati, big data e amministrazione pubblica*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino, p. 117 e ss, 2021.

<sup>205</sup> L'articolo 5 del GDPR prevede che a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime e, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in 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 («integrità e riservatezza»).

ha delle ripercussioni anche sul piano interno in virtù della natura di regolamento.

Il GDPR ha posto delle grandi limitazioni all'attività di raccolta e trattamento dei dati soprattutto quando si tratta di quantità ingenti, dunque di Big Data.

Nello specifico, la limitazione della finalità consente di stabilire delle condizioni precise in presenza delle quali, i dati raccolti per un determinato scopo non possono essere utilizzati per scopi diversi. In tal modo, viene ristretta in via preventiva e dunque ex ante la quantità, nonché la qualità dei dati utilizzabili al fine di utilizzarli ad un solo scopo specifico individuato a priori.

La tutela dei dati in mano pubblica deve sempre rinvenirsi nel GDPR, che richiede il rispetto del principio di finalità del trattamento. Tale principio, come si è avuto modo di anticipare, consente di controllare l'utilizzo dei dati personali da parte della pubblica amministrazione orientandolo verso il rispetto del principio di legalità in virtù del quale il trattamento dovrà considerarsi lecito laddove vi sia un compito di interesse pubblico o l'attribuzione di un potere da parte della legge.

Il soggetto che raccoglie dati personali in virtù di un esercizio di un compito di interesse pubblico rispetto alle altre basi giuridiche individuate dalla norma ha dei limiti molto stringenti e delle precondizioni imposte proprio dalla legge.

Ebbene, il soggetto di diritto comune tratta i dati e determina in autonomia la finalità specifica grazie al consenso, in esecuzione di un contratto, in adempimento di un obbligo legale o a salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. La finalità, per il soggetto che raccoglie dati personali al fine di esercitare un compito di interesse pubblico, è integralmente etero-determinata ex ante<sup>206</sup> dal legislatore.

---

<sup>206</sup> Vedasi B. PONTI, *L'amministrazione come fornitore e come fruitore di dati personali pubblici: sono praticabili soluzioni basate sulla Big Data Analytics/machine learning?* In *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino, p. 117 e ss.

Il principio di finalità del trattamento racchiude e ingloba in sé il principio di legalità e il principio di proporzionalità. Ebbene, il soggetto pubblico titolare del trattamento deve porsi nella condizione di verificare e controllare che il trattamento dei dati, anche se in quantità ingenti, sia connesso con la finalità predefinita identificata dalla base giuridica. Tale principio, può entrare in crisi con le nuove tecniche di *machine learning*<sup>207</sup>.

Nello specifico, nel rispetto del principio di finalità del trattamento, non è consentito alla pubblica amministrazione di mettere a disposizione di soggetti terzi, una raccolta di dati conservati per fini istituzionali.

La possibilità di derogare a tale principio è prevista solamente nel caso in cui sia espressamente previsto dalla legge.

L'articolo 86 del GDPR prevede infatti che *“I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento”*. Nell'ordinamento italiano, il legislatore ha previsto dei casi tassativamente individuati in cui i dati personali devono essere resi conoscibili a chiunque per finalità di trasparenza. In tali ipotesi, sia ha una dequotazione sostanziale della riservatezza e della tutela dei dati personali a favore del principio cardine di trasparenza.

Ciò in quanto, il legislatore ha voluto garantire al cittadino, nel pieno rispetto del principio democratico, l'accesso alle informazioni, all'attività e alle

---

<sup>207</sup> Si veda per un approfondimento M. INTERLANDI – L. TOMASSI, La decisione amministrativa algoritmica, in *Approfondimenti di diritto amministrativo*, a cura di A. Contieri, 2020, Editoriale scientifica, Napoli; A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la pubblica amministrazione Principi e regole del procedimento amministrativo algoritmico* a cura di E. Belisario e G. Cassano, Pacini Giuridica, 2023, p. 173 e ss.

modalità di organizzazione della pubblica amministrazione mediante il d.lgs. n. 33 del 2013 sul *“Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”*<sup>208</sup>. Il decreto prevede appunto, una pubblicazione obbligatoria per le finalità individuate dal legislatore.

La questione controversa, soprattutto di recente in virtù dei nuovi sistemi di evoluzione tecnologica, riguarda in particolare la possibilità di riutilizzare i dati personali pubblicati per espressa previsione di legge.

Sul punto occorre rilevare che con l'introduzione del GDPR, di primaria importanza per rispondere a tale quesito è diventato il principio di *accountability*.

Ebbene, prima dell'introduzione del GDPR, le *“Linee guida in materia di trattamento dei dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati”* adottate con provvedimento del 15 maggio 2014<sup>209</sup> prevedevano, non tanto un principio di *“responsabilizzazione”* del titolare del trattamento, bensì facevano ricadere la responsabilità sulle pubbliche amministrazioni, le quali, avevano il compito di controllare,

---

<sup>208</sup> L'articolo 5 prevede che *“1. I dati personali sono: (C39) a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in 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 («integrità e riservatezza»).* 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74).

limitare, proibire la possibilità di ri-utilizzo dei dati personali pubblicati ai sensi del decreto trasparenza in virtù di una rigorosa e preventiva valutazione di impatto in materia di protezione dei dati.

Un principio cardine, che ha il ruolo di guidare i soggetti nella raccolta e trattamento dei dati è il principio di proporzionalità<sup>209</sup>. Esso, correlato al principio di minimizzazione dei dati<sup>210</sup>, consente, in virtù di una motivazione piena, di dimostrare la proporzionalità della misura utilizzata. Con specifico riferimento alle pubbliche amministrazioni, esse devono rispettare pedissequamente i principi di limitazione della finalità e di minimizzazione dei dati nella raccolta e conservazione nei propri archivi e banche dati tuttavia, l'articolo 6 del GDPR prevede una deroga individuando le modalità di accesso a tali banche dati anche in presenza di ulteriori finalità.

Come si è avuto modo di anticipare, la qualità dei dati è importante poiché i dati per essere aggregati, raccolti conservati e interconnessi devono essere esatti, accurati, in senso di pulizia, completezza e copertura e non contenere alcuna falsa rappresentazione della realtà<sup>211</sup>.

---

<sup>209</sup> Si veda D.U. GALETTA, I principi di proporzionalità e ragionevolezza, in Principi e regole dell'azione amministrativa, a cura di M.A Sandulli coordinato da F. Aperio Bella, Quarta Edizione, 2023, p. 169 e ss.

<sup>210</sup> Il principio di minimizzazione dei dati è previsto dall'articolo 5 del GDPR alla lettera c il quale prevede che "1. I dati personali sono: (C39) a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)."

<sup>211</sup> L'articolo 17 prevede che "*l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società*

Oggi, con la nuova evoluzione tecnologica, la pubblica amministrazione si è trovata a gestire, conservare e riutilizzare una vasta quantità incontrollabile di dati.

Secondo parte della dottrina, la soluzione precedente al GDPR individuata dal decreto trasparenza e dalle linee guida poneva un onere in capo alle pubbliche amministrazioni di mantenere un controllo costante su tutte le informazioni e dati che potevano essere riutilizzati da possibili fruitori determinando un'inefficienza della stessa nel suo ruolo imposto dalla legge di "controllore" nei confronti di terzi e dandole compiti al di fuori della sua portata.

Il GDPR ha introdotto invece il principio di accountability<sup>212</sup> che in tale contesto consente di responsabilizzare il titolare del trattamento.

Occorre sottolineare che in virtù di tale principio, il titolare del trattamento per l'eventuale riutilizzo dei dati legittimamente pubblicati, non è più la pubblica amministrazione che ha un obbligo di controllo sulla circolazione, fuoriuscita,

---

*dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria."*

<sup>212</sup> Il principio di accountability prevede all'articolo 24 che "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento."

riutilizzo dei dati, bensì sono i terzi fruitori che, riutilizzando il dato, diventano titolare poiché li vanno a trattare<sup>213</sup>.

Peculiare, è dunque, l'influenza forte che ha il GDPR nell'attività della pubblica amministrazione, laddove il principio di trasparenza incontra la protezione dei dati personali.

Se cambia, per legge il titolare del trattamento, muta anche il relativo regime e la pubblica amministrazione non avrà più il compito di dover essere controllore di dati pubblicati legittimamente ma riutilizzati da terzi, a volte illecitamente.

La Corte costituzionale<sup>214</sup> ha fatto emergere che la pubblicazione di quantità "massicce" di dati non agevola il cittadino, deteriora il principio di finalità nonché il principio di trasparenza dell'azione amministrativa.

Orbene, sarebbe preferibile che invece di rendere pubbliche quantità ingenti di dati, il legislatore selezionasse a monte con precisione le informazioni e i dati davvero indispensabili a fini di trasparenza, facendo ciò, verrebbe rispettato non solo il principio di finalità del trattamento.

In definitiva, le finalità devono essere definite a priori, e i dati personali possono essere riutilizzati, se già detenuti, solo per le finalità che ne avevano anche giustificato la raccolta stessa o ai sensi del comma 4 dell'articolo 6 per ulteriori finalità considerate compatibili con le prime finalità mediante una valutazione discrezionale e bilanciata.

---

<sup>213</sup> Così vedasi B. PONTI, *L'amministrazione come fornitore e come fruitore di dati personali pubblici: sono praticabili soluzioni basate sulla Big Data Analytics/Machine Learning*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di R. Cavallo Perin con il coordinamento editoriale di I. Alberti, L'università degli Studi di Torino, 2021.

<sup>214</sup> Corte Cost., sentenza 27 febbraio 2019, n. 20.

### **3. L'organizzazione amministrativa nella gestione dei dati pubblici: dal modello Government as a platform al Polo strategico Nazionale.**

A questo punto, occorre comprendere in concreto come sono organizzate le banche dati delle pubbliche amministrazioni, la loro possibile interoperabilità e una eventuale riflessione futura al fine di gestire al meglio la comunicazione tra i vari sistemi informatici del settore pubblico.

Nello specifico, la pubblica amministrazione ha subito un cambiamento profondo indirizzato verso la sperimentazione di modelli di ecosistemi digitali idonei a ri-orientare il futuro dell'amministrazione nell'era digitale<sup>215</sup>.

La transizione digitale che ha accompagnato le istituzioni e la pubblica amministrazione mira a realizzare un ecosistema digitale antropocentrico secondo il modello *Government as a platform*<sup>216</sup> fondato sulle nuove tecnologie.

La digitalizzazione della pubblica amministrazione<sup>217</sup>, nella misura in cui consente la messa a disposizione di plurime piattaforme capaci di strutturare l'ambiente amministrativo per assicurare la piena interoperabilità tra i vari servizi offerti dalle pubbliche amministrazioni mediante un processo di apprendimento volto alla valorizzazione delle strutture, alla portata infrastrutturante delle piattaforme, e alla centralità della funzione nell'ambiente di

---

<sup>215</sup> Così B. BOSCHETTI, *La transizione della pubblica amministrazione*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli, con prefazione di A. Clarich, Giappichelli Editore, Torino, 2022, p.3 e ss; A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, Il Mulino, Bologna 1971; L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro Amministrativo*, II, 2018, p. 9.

<sup>216</sup> Per la definizione vedasi Harvard Kennedy school, ash center for democratic governance and innovation, *playbook: government as a platform*, a cura di R. Pope, Novembre 2019, [https://ash.harvard.edu/files/ash/files/293091\\_hvd\\_ash\\_gvmnt\\_as\\_platform\\_v2.pdf](https://ash.harvard.edu/files/ash/files/293091_hvd_ash_gvmnt_as_platform_v2.pdf).

<sup>217</sup> Si veda D. SORACE, *Diritto delle amministrazioni pubbliche. Una introduzione*, Il Mulino, Bologna, 2014; F. MARTINES, *La digitalizzazione della pubblica amministrazione*, in *Rivista di diritto dei media*, 2018, p. 2.; A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513; M. CLARICH, *Prefazione*, in A. Lalli, *La pubblica amministrazione nell'era digitale*, Torino, Giappichelli, 2022, XIV.

relazione, non tanto da un punto di vista definitorio e statico bensì guardando al futuro della transizione digitale delle pubbliche amministrazioni anche da un punto di vista dinamico tenendo conto del valore organizzatorio della piattaforma come infrastruttura.

Le tecnologie utilizzate per l'infrastrutturazione dell'amministrazione, secondo l'agenda digitale italiana ed europea<sup>218</sup> riguardano quelle relative alla connettività, al cloud computing, quelle relative alla cybersecurity<sup>219</sup> e sull'interoperabilità dei dati sui servizi online resi al cittadino. Orbene, per arrivare a ciò, occorre sempre tener conto della protezione dei dati personali.

Le banche dati della pubblica amministrazione italiana sono normalmente organizzate secondo “*data silos*” OLTP<sup>220</sup>. La struttura a silos è un modello che consente di comprendere un insieme di dati contenuti in vari database e organizzarli secondo uno schema.

Lo schema è volto alla definizione delle relazioni fra dati e descrive preventivamente dunque *ex ante* la conoscenza che il progettista del data base ha del dato e della sua correlazione con gli altri dati. Tuttavia, tale sistema di *datasilos* è effettivamente controverso e problematico poiché non essendoci un unico schema si va a creare un'interferenza vera e propria nel momento in cui vi è la necessità (come avviene per le pubbliche amministrazioni sempre più di frequente) di incrociare dati di più database diversi. L'incrocio di dati necessita della creazione di un nuovo database e dunque di un nuovo schema volto ad unirli. Ciò determina ogni volta una crescita dei costi e dei tempi per la creazione ogni volta di un nuovo database (schema) inadeguato, inoltre, alla ricerca continua di nuove interrelazioni fra dati<sup>221</sup>.

---

<sup>218</sup> <https://innovazione.gov.it/argomenti/italia-digitale-2026/>

<sup>219</sup> Per un approfondimento sulla cybersicurezza vedasi S. ROSSA, *La dimensione verticale della Cybersicurezza pubblica fra Unione Europea e Ordinamento nazionale* in *Cybersicurezza e pubblica amministrazione*, Editoriale scientifica Napoli, 2023, p. 65;

<sup>220</sup> *Online transaction processing*.

<sup>221</sup> COSÌ M. ALDINUCCI, *L'infrastruttura necessaria per creare interoperabilità tra pubbliche amministrazioni*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza*

In altri termini, il problema primario è l'incrocio dei dati poiché dal momento in cui la pubblica amministrazione deve incrociare i dati emerge l'inadeguatezza del modello di “*datasilos*” dove è richiesta la creazione continua di nuovi schemi.

Una soluzione per organizzare i dati della pubblica amministrazione potrebbe essere proprio l'approccio *Big Data*. Come si è avuto modo di anticipare, il modello “*datalake*” sistema OLAP<sup>222</sup> è un insieme di dati eterogenei che non richiede uno schema già definito ex ante dal progettista.

In ragione di ciò, si è evidenziato come tale modello potrebbe essere la soluzione nel momento in cui le pubbliche amministrazioni hanno necessità di incrociare i dati. Ebbene, concretamente, il “*datalake*” consente di creare delle correlazioni tra dati che non richiedono la precondizione di essere ex ante conosciute, previste e conoscibili.

Un problema maggiore riguarda la conservazione dei dati e delle informazioni. Ciò in quanto, per arrivare ad un'amministrazione ecosistemica, il fulcro principale è garantire la piena interoperabilità dei dati<sup>223</sup> mediante una struttura, architettura, in grado di interconnettere i data set delle pubbliche amministrazioni con modalità digitali.

Ebbene, con il Piano Nazionale di Ripresa e Resilienza (PNRR) sono stati stanziati risorse di 0,65 miliardi di euro rivolte direttamente al tema dell'interoperabilità dei dati.

---

Artificiale, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino, 2021; A. SCOGNAMIGLIO, *Diritto di accesso e banche dati pubbliche*, in Foro amministrativo c.d.s., 2005,2, p.492.; G. CARULLO, *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in Concorrenza e mercato, vol. 23, 2016, pp. 181-204; G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino 2017; L. FLORIDI, *La Rivoluzione dell'informazione*, Turin, Codice Edizioni, 2012.

<sup>222</sup> Online Transaction Processing

<sup>223</sup> L'articolo 1 comma 1 lettera dd), d.lgs 7 marzo 2005, n. 82, con il termine interoperabilità, si vuole intendere la caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.

Tra gli obiettivi principali del processo di trasformazione digitale occorre evidenziare quello della valorizzazione del patrimonio informativo detenuto dalle pubbliche amministrazioni nonché il miglioramento qualitativo dei servizi pubblici offerti ai privati cittadini. Al fine di semplificare e snellire le procedure di scambio di informazioni tra amministrazioni, all'interno del programma degli investimenti stanziati nel PNRR è stata prevista una "Piattaforma digitale nazionale dei Dati" al fine di evitare di dover fornire lo stesso dato o la stessa informazione alle amministrazioni più di una volta e idonea a garantire in concreto la conoscenza nonché l'utilizzo dei dati pubblici. La Piattaforma Digitale Nazionale dei Dati, gestita dalla Presidenza del Consiglio dei Ministri, mira a diventare l'infrastruttura tecnologica idonea a rendere concreto lo scambio tra i sistemi informativi delle pubbliche amministrazioni lo scambio di dati mediante una fluente interoperabilità.

Invero, ogni pubblica amministrazione dovrà mettere a disposizione i propri dati all'interno della piattaforma utilizzando le cosiddette "Application Programming Interface" interfacce digitali sviluppate da programmatori abilitati in conformità alle linee guida dell'AgID<sup>224</sup> in materia di interoperabilità, successivamente, le interfacce verranno raccolte in un catalogo specifico a disposizione di tutte le pubbliche amministrazioni centrali e periferiche. Le interfacce digitali descrivono le modalità tecniche attraverso cui un servizio pubblico deve essere attivato tramite un programma informatico garantendo la classificazione del dato secondo il programma.

Ebbene, il Dipartimento per la trasformazione digitale ha il compito di supportare tutte le pubbliche amministrazioni nell'adottare un modello di interoperabilità che condurrà a una riduzione dei costi di gestione per la pubblica amministrazione poiché l'interoperabilità dei dati mediante un'unica

---

<sup>224</sup>Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati adottate con determinazione n. 627/2021.

sola piattaforma nazionale determinerà un risparmio delle risorse finanziarie con la possibilità di una diversa allocazione dei fini.

Inoltre, lo scambio di dati e informazioni contestuale tra enti abilitati secondo il catalogo, consente di svolgere procedimenti amministrativi complessi in minor tempo consentendo alle amministrazioni di condividere finalmente i dati in maniera veloce e sicura riducendo le inefficienze dovute essenzialmente ad una incompletezza di disponibilità di informazioni e dati nel tempo necessario allo svolgimento dei procedimenti<sup>225</sup>.

Tornando sulla scia dell'approccio "Big Data", la disponibilità di un'ingente mole di dati in un'unica piattaforma digitale nelle mani pubbliche consentirà di utilizzare strumenti peculiari di analisi al fine di migliorare il processo decisionale progettando interventi pubblici e definendo politiche pubbliche volte a soddisfare sempre di più le esigenze del cittadino nel rispetto del principio democratico.

I cittadini, sulla base del principio del "once only" trasmetteranno in unica soluzione dati e informazioni alle pubbliche informazioni interessate semplificando i processi e snellendo le procedure complesse. Grazie a tale piattaforma cittadini e imprese non dovranno più fornire informazioni e dati già in possesso di altre amministrazioni ma, nonostante ciò, verrà comunque garantita una sicurezza nell'ambito della trasmissione dei dati favorendo il riutilizzo da parte di tutti gli attori coinvolti. Infatti, l'articolo 50 ter del CAD<sup>226</sup> ha espressamente previsto che all'interno della piattaforma non

---

<sup>225</sup> Vedasi F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.*, 2/2015, 227; D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica amministrazione*, in *Il diritto dell'era digitale*, edito da R.GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milan, 2022, p. 625.

<sup>226</sup> L'articolo 50 ter del CAD prevede che "1. La Presidenza del Consiglio dei ministri promuove la progettazione, lo sviluppo e la sperimentazione di una Piattaforma Digitale Nazionale Dati finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto, per finalità istituzionali, dai soggetti di cui all'articolo 2, comma 2, lettera a), ad esclusione delle autorità amministrative indipendenti di garanzia, vigilanza e regolazione, nonché alla condivisione dei dati tra i soggetti che hanno diritto ad accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese, in conformità alla disciplina vigente.2. In sede di prima applicazione, la

potranno confluire i dati relativi alla sicurezza pubblica e all'ordine pubblico, alla difesa nazionale, alla polizia giudiziaria ed economica finanziaria.

La messa a disposizione di un ambiente informatico in cui attraverso la rete internet possono essere conservati e collocati i dati mediante un sistema di condivisione è sempre più utilizzata anche nel settore pubblico

Il concetto di “network -based computing”<sup>227</sup> ha faticato ad entrare nel nostro paese ma oggi, nonostante ciò è diventato dirimente avere un cloud nazionale per la pubblica amministrazione soprattutto al fine di garantire una maggiore affidabilità e concretezza.

Ebbene, mediante il cloud computing, ossia l'utilizzo di risorse remote poste a distanza dagli apparati utilizzati per accedervi dall'utente, l'erogazione di servizi è garantita da remoto mediante piattaforme centralizzate in grado di

---

*sperimentazione della Piattaforma Digitale Nazionale Dati è affidata al Commissario straordinario per l'attuazione dell'Agenda digitale non oltre il 15 settembre 2019.3. Ai fini dello svolgimento delle funzioni di cui al comma 2, il Commissario straordinario per l'attuazione dell'Agenda digitale provvede, nel rispetto dei limiti, delle condizioni e delle modalità stabilite dal Garante per la protezione dei dati personali e dal decreto di cui al comma 4, ad acquisire i dati detenuti dai soggetti di cui all'articolo 2, comma 2, lettera a), ad esclusione delle autorità amministrative indipendenti di garanzia, vigilanza e regolazione, organizzarli e conservarli, nel rispetto delle norme tecniche e delle metodologie idonee a garantire la condivisione dei dati tra le pubbliche amministrazioni stabilite da AgID nelle Linee guida. I soggetti che detengono i dati identificati nel decreto di cui al comma 4, hanno l'obbligo di riscontrare la richiesta del Commissario, rendendo disponibili i dati richiesti senza nuovi o maggiori oneri per la finanza pubblica.4. Con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e le Amministrazioni titolari dei dati, sono stabilite le modalità di attuazione del presente articolo al fine di favorire la condivisione dei dati fra le pubbliche amministrazioni, di semplificare l'accesso ai dati stessi da parte dei soggetti che hanno diritto ad accedervi e di semplificare gli adempimenti e gli oneri amministrativi per i cittadini e le imprese, ed è identificato l'elenco dei dati che i soggetti di cui all'articolo 2, comma 2, lettera a), ad esclusione delle autorità amministrative indipendenti di garanzia, vigilanza e regolazione, sono tenuti a rendere disponibili per le finalità di cui al comma 3; l'elenco è aggiornato periodicamente con decreto del Presidente del Consiglio dei ministri, sentito il Garante per la protezione dei dati personali e le Amministrazioni titolari dei dati, sono stabilite le modalità di attuazione del presente articolo al fine di favorire la condivisione dei dati fra le pubbliche amministrazioni, di semplificare l'accesso ai dati stessi da parte dei soggetti che hanno diritto ad accedervi e di semplificare gli adempimenti e gli oneri amministrativi per i cittadini e le imprese, ed è identificato l'elenco dei dati che i soggetti di cui all'articolo 2, comma 2, lettera a), ad esclusione delle autorità amministrative indipendenti di garanzia, vigilanza e regolazione, sono tenuti a rendere disponibili per le finalità di cui al comma 3; l'elenco è aggiornato periodicamente con decreto del Presidente del Consiglio dei ministri, sentito il Garante per la protezione dei dati personali e le Amministrazioni titolari dei dati. Con il medesimo decreto sono stabiliti i limiti e le modalità di acquisizione, organizzazione e conservazione dei dati.5. Il trasferimento dei dati nella Piattaforma <sup>Digitale</sup> Nazionale Dati non modifica la titolarità del dato,*

<sup>227</sup> Vedasi G. CERRINA FERONI – C. FONTANA – E. C. RAFFIOTTA, *Ai Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, 2022, p. 9 e ss.

garantire una maggiore efficienza agli utenti, un affidamento concreto a terzi nella gestione dell'infrastruttura nonché una grande de-responsabilizzazione<sup>228</sup>.

La riconduzione dei servizi a un solo centro computazionale consente una centralizzazione delle risorse e delle funzioni di memoria e di calcolo garantendo la riconduzione a un unico centro di servizi.

In ragione di ciò, si è ritenuto<sup>229</sup> che la scelta di optare per infrastrutture gestite da soggetti terzi mediante l'utilizzo del cloud computing (*cloud first*) possa essere la soluzione per produrre dei benefici maggiori in termini di costi e rischi. Nello specifico, il beneficio maggiore derivante da un sistema cloud rispetto a un servizio erogato da una sola amministrazione è quello relativo a una maggiore efficienza trattandosi di infrastrutture funzionali e moderne, nonché la ricerca di una interoperabilità maggiore al fine di superare il sistema di divisione in silos che come si è anticipato precedentemente, impediscono di avere una visione omogenea di dati e informazioni a disposizione e aggravano i procedimenti delle amministrazioni pubbliche. In altri termini, la migrazione verso il cloud nella pubblica amministrazione consente sicuramente una dismissione e un decentramento dai data center obsoleti e inaffidabili avendo come scopo principale quello di ridurre i costi di gestione delle infrastrutture. Tuttavia, al di là dei benefici in termini di accelerazione dei processi e semplificazione delle attività occorre nel presente lavoro porre in luce gli evidenti e concreti problemi che vengono a crearsi nei sistemi cloud con specifico riferimento alla protezione dei dati personali e alla privacy.

---

<sup>228</sup> Sul tema si veda, B. CAROTTI, *Il settore pubblico e il cloud computing*, in *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, a cura di V. Bontempi, Roma, Roma tre press, 2022, p. 147 e ss.

<sup>229</sup> Ancora così B. CAROTTI, *Il sistema di governo di internet*, Milano, Giuffrè, 2016; A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi pubblici "online". Lineamenti del disegno normativo*, in *Diritto Pubblico*, no. 1/2019, 124 e ss.

Invero, è possibile andare incontro a *data breach* nonché attacchi cyber volti a estrapolare dai sistemi cloud dati e informazioni identificative anche personali tali da rendere vulnerabile l'intero sistema.

Orbene, la tutela della privacy rimane una questione aperta e controversa in questo settore ancora in costruzione, ciò che rileva è che il GDPR continua a rimanere un punto fermo quale erogatore di principi cardine da seguire e attuare quando la tecnologia entra in collisione con la protezione dei dati personali. In ragione di ciò, si fa sempre più vicina la necessità di dotare il Paese di una infrastruttura definitiva, unica e cardine a servizio della pubblica amministrazione e localizzata nel territorio nazionale.

#### **4. Cloud nazionale: tra utopia e primi problemi applicativi.**

La realizzazione di un Polo Strategico Nazionale è l'obiettivo principale degli ultimi tempi nella nuova era tecnologica nel settore pubblico.

Nello specifico, la realizzazione concreta del Polo strategico Nazionale è il progetto più importante di riqualificazione preso in considerazione dal Piano Nazionale di Ripresa e Resilienza.

Come si è anticipato, la migrazione dei dati, dei servizi e delle informazioni verso il cloud computing ha accelerato gli obiettivi di digitalizzazione e semplificazione.

Il 31 maggio 2017 il Presidente del Consiglio dei Ministri ha approvato con decreto il Piano triennale per l'informatica nella pubblica amministrazione avviando un percorso di riqualificazione delle infrastrutture della Pubblica Amministrazione basato proprio sul principio del cloud first.

L'AgID, al fine di classificare le infrastrutture sul piano dell'interoperabilità e della sicurezza ha tracciato i confini per proteggere i dati e le informazioni personali migrate nel cloud individuando plurimi livelli di protezione<sup>230</sup>.

Nello specifico, si è concentrata l'attenzione sull'importanza di effettuare una distinzione per classi di dati e servizi della pubblica amministrazione, in particolare la classificazione avrà lo scopo di individuare preventivamente quali sono i dati, le informazioni e i servizi migrati nel cloud che meritano una maggiore protezione e tutela rispetto agli altri. Una struttura distinta ordinata in cui vengono classificati livelli strategici in cui confluiscono dati e servizi che laddove vengono compromessi possono determinare un forte impatto sulla sicurezza nazionale che differiscono dal livello ordinario di base in cui confluiscono invece dati e servizi la cui compromissione non va a determinare un impatto così forte sull'attività e sulla sicurezza nazionale.

Nello specifico, l'Agenzia per l'Italia Digitale mediante un censimento del patrimonio *Information and Communication Technology* ha tentato di classificare le infrastrutture in termini di sicurezza e affidabilità nel rispetto dei bisogni dei cittadini e delle imprese.

Al fine di comprendere le criticità dei sistemi di cloud computing occorre soffermarsi sulla circolare n. 1 del 2019 dell'AgID con cui è stata effettuata una valutazione concreta dello stato di salute delle piattaforme utilizzate dalle pubbliche amministrazioni, criticando principalmente le strutture non centralizzate "a rischio" poiché aventi un apparato obsoleto. Nel 2020, l'AgID nell'ultima rilevazione sui data center italiani, su un numero di 1252 data center, ha posto in luce il fatto che solo 35 data center su 1252, dunque il 3 % è risultato concretamente dotato di infrastrutture veramente affidabili e non a

---

<sup>230</sup> Così G. ITALIANO, *La protezione dei dati nel cloud nazionale*, in *Il ruolo del Garante per la protezione dei dati personali – la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. Cerrina Feroni, Il Mulino, 2023, p. 97 e ss.

rischio mentre il 2%, quindi 27 su 1252 data center analizzati in Italia, è risultato di media qualità quindi non concretamente affidabili.

Ci si è interrogati dunque, sul perché il restante 95% relativo a 1190 data center su 1252 analizzati e presenti sul territorio italiano, risulta privo dei requisiti minimi di affidabilità e sicurezza e non idonei a garantire la continuità e omogeneità del servizio offerto<sup>231</sup>.

Tale classificazione, ha consentito di individuare in concreto le infrastrutture ipotizzabili come Polo Strategico Nazionale idonee dunque ad erogare servizi di Information and Communication Technology ad altre pubbliche amministrazioni in modo continuativo omogeneo e sistematico.

Inoltre, tale analisi ha consentito di catalogare anche le infrastrutture aventi requisiti minimi di affidabilità ma comunque non candidabili come Polo Strategico Nazionale nonché quelle aventi proprio una carenza strutturale e organizzativa per ciò non idonea ad assicurare continuità dei servizi e affidabilità.

Ciò che è emerso da tale verifica<sup>232</sup> è che il quadro risulta molto frammentato in termini di disomogeneità e alta inefficienza da parte di plurime amministrazioni.

Ebbene, molti data center sono risultati del tutto inefficienti, caratterizzati da sistemi e strutture inadeguate e non idonei a garantire un livello normale di sicurezza.

Per far fronte a questa inefficienza dimostrata tramite dei dati specifici, al fine di promuovere *“lo sviluppo di un’infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e consolidamento dei centri per l’elaborazione delle informazioni”* il D.L. 16 luglio 2020, n. 76 su *Misure*

---

<sup>231</sup> Vedasi A. SORO, *Dati e democrazia*, in Il ruolo del Garante per la protezione dei dati personali – la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro, a cura di G. Cerrina Feroni, Il Mulino, 2023, p. 97 e ss.; G. ITALIANO, *La protezione dei dati nel cloud nazionale*, in Il ruolo del Garante per la protezione dei dati personali – la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro, a cura di G. Cerrina Feroni, Il Mulino, 2023, p. 97 e ss.

<sup>232</sup> Delibera dell’Agenzia n. 1 del 14 giugno 2019.

*urgenti per la semplificazione e l'innovazione* digitali convertito in Legge 11 settembre 2020, n. 120, ha previsto che le amministrazioni che sono dotate di data center di tipo B<sup>233</sup> dunque non affidabili in concreto, debbano migrare tutti i loro centri per elaborare le informazioni verso delle strutture più conformi e idonee secondo gli standard.

Ebbene, è l'Agenzia per la sicurezza cibernetica che deve individuare i propri livelli di sicurezza qualità e scalabilità dei servizi di cloud per la pubblica amministrazione.

Grazie al PNRR il Governo ha cercato di raggiungere più velocemente l'obiettivo di digitalizzazione della pubblica amministrazione con una migrazione di dati e sistemi informatici verso un sistema cloud nuovo e implementato quale è il Polo strategico nazionale.

Occorre comprenderne la struttura e la modalità di gestione dei servizi all'interno del Polo nonché le eventuali criticità di sistema.

In primo luogo, l'ordinamento italiano ha assunto nei confronti dell'Unione Europea un impegno ad affidare la gestione dell'infrastruttura pubblica nonché la predisposizione di servizi cloud a un operatore tecnologico selezionato mediante una gara utilizzando lo strumento del partenariato pubblico - privato<sup>234</sup>.

Ebbene, parte della dottrina<sup>235</sup> ha posto in luce il fatto che prima di individuare come strumento cardine il partenariato pubblico privato per l'implementazione futura di un Polo strategico nazionale, tra le opzioni sul tavolo vi erano la realizzazione diretta da parte dello Stato, il ricorso a una sola

---

<sup>233</sup> Così B. CAROTTI, *Il settore pubblico e il cloud computing*, in *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, a cura di V. Bontempi, Roma, Roma tre press, 2022, p. 147 e ss.

<sup>234</sup> Vedasi G. NAPOLITANO, *Il partenariato public-privato per l'implementazione del Polo Strategico Nazionale* in *Giorn. Dir. Amm.*, 6/2021, 703-707.

<sup>235</sup> Si veda anche A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513.

società in house<sup>236</sup> partecipata dallo Stato, nonché un affidamento ai privati attraverso un appalto a favore di un operatore nazionale o europeo in possesso delle tecnologie digitali.

Tuttavia, tali strumenti non avrebbero consentito di gestire sul piano industriale, tecnologico e istituzionale i rapporti tra le pubbliche amministrazioni mentre il partenariato pubblico – privato è considerato una *“scelta ragionevole di compromesso in grado di contemperare adeguatamente le diverse esigenze”*<sup>237</sup>.

La questione controversa e problematica ha tuttavia riguardato la copertura dei costi di migrazione e di fruizione delle amministrazioni oltre che quello di assicurare e garantire un’adeguata remuneratività degli operatori che vengono coinvolti.

Ebbene, sia che il partenariato pubblico privato avvenga mediante la stipula di un contratto di concessione o di un altro accordo di partenariato, sia che avvenga tramite la costituzione di una società mista, comunque portano ad analizzare la questione circa la copertura dei costi e l’allocazione delle risorse. Il problema riguarda il fatto che le modalità di allocazione delle risorse destinate a coprire i costi di migrazione e la remunerazione dell’intervento non sono state ancora definite chiaramente quindi ci si è interrogati sulla possibilità astratta di qualificarle in termini di aiuti di stato.

Ciò in quanto, il Piano prevede che con qualunque forma di partenariato venga svolto il Polo, comunque la copertura dei costi nonché la remunerazione nei confronti dell’operatore debba derivare in astratto dalla percentuale dei risparmi che vengono generati e da un ulteriore corrispettivo annuale che garantisce la copertura degli investimenti.

---

<sup>236</sup> Vedasi V. DONATIVI, *Le società a partecipazione pubblica*, Milan, 2016; *Codice delle Società a partecipazione pubblica*, editore by G. MORBIDELLI, MILANO, 2018; A. NATALINI, *Come il passato influenza la digitalizzazione della pubblica Amministrazione*, in *Riv. trim. dir. pubbl.*, no. 1, 2022, 95

<sup>237</sup> Così G. NAPOLITANO, *Il partenariato public-privato per l’implementazione del Polo Strategico Nazionale* in *Giorn. Dir. Amm.*, 6/2021, 703-707.

La Commissione Europea, ha osservato che i servizi di cloud laddove siano offerti direttamente ed esclusivamente alle pubbliche amministrazioni e non sono destinate allo sfruttamento commerciale sul libero mercato, può essere esclusa l'applicazione della disciplina degli Aiuti di Stato.

Per quel che qui rileva, per il PSN si è fatto ricorso alla finanza di progetto<sup>238</sup> volta a preferire la gestione di lavori e servizi di pubblica utilità mediante l'utilizzo di capitali privati.

Ebbene, parte della dottrina ha rilevato che il ricorso alla finanza di progetto rispetto alla soluzione di un appalto di lavoro o servizio bandita per il tramite dell'amministrazione committente, consente di garantire un coinvolgimento attivo di operatori nel complesso del progetto esonerando l'amministrazione in parte degli oneri ciò in quanto il fulcro principale della finanza di progetto è proprio l'assunzione del rischio di impresa da parte del concessionario.

Le amministrazioni, alla stregua di un cliente, laddove decidano di aderire al progetto sulla base di una valutazione di convenienza dovranno versare un prezzo al concessionario per gestire i centri dati e la fruizione delle applicazioni con la modalità cloud.

In tal modo le pubbliche amministrazioni decideranno di far migrare i propri dati verso il Polo strategico Nazionale, il quale costituirà la fonte subprimaria di copertura dei costi di investimento e di gestione dei costi che sono stati sostenuti dagli operatori privati.

La Missione 1 del PNRR ha previsto la realizzazione dell'infrastruttura digitale nel rispetto del principio del Cloud first.

Il PNRR ha dunque stanziato una dotazione di circa 900.000.000,00 euro in favore delle pubbliche amministrazioni volte a realizzare la migrazione dei dati.

---

<sup>238</sup> Si veda, V. MONTANI, *Il project financing inquadramento giuridico e logiche manutentive*, Giappichelli Editore Torino, 2018; B. MARCHETTI, Voce *Amministrazione Digitale*, in *Enciclopedia del Diritto*, Milan, 2022, 76.

Il completamento dell'intero progetto è stato previsto in una logica futura non lontana per il secondo trimestre del 2026.

Come si è avuto modo di evidenziare, il project financing è stato ritenuto lo strumento utile per la predisposizione del Polo Strategico Nazionale e il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri ha promosso la procedura di project financing.

L'iniziativa ha preso il via il 28 settembre del 2021 da parte di un gruppo di operatori industriali e finanziari<sup>239</sup> che hanno presentato al Ministero per l'innovazione tecnologica e la transizione digitale una proposta di finanza di progetto relativa all'affidamento in concessione di servizi infrastrutturali in cloud per gestire i dati detenuti dalle pubbliche amministrazioni mediante appunto il cd Polo Strategico Nazionale.

Le garanzie di sicurezza e correttezza nella migrazione dei dati della pubblica amministrazione sono garantite dalla partecipazione pubblica maggioritaria.

Il 24 novembre 2023 la Commissione Europea ha reso nota la sua valutazione positiva sulla proposta di revisione del Piano Nazionale di Ripresa e Resilienza e ha specificato le modalità di migrazione verso il cloud stabilendo che *“entro il 30 settembre 2024 almeno 100 amministrazioni pubbliche centrali devono migrare almeno un servizio verso il Polo Strategico Nazionale.”*

La finalità primaria della revisione non è stata quella di ridurre gli obiettivi in corso d'opera, bensì quella di andare incontro alle pubbliche amministrazioni bisognose di un supporto maggiore nella fase di migrazione dei propri dati e servizi digitali.

Il 22 febbraio 2024 la Corte dei Conti, in occasione della quarta Relazione semestrale di attuazione del PNRR ha presentato una bozza di documento complesso contenente tutte le iniziative relative al Piano diventando una

---

<sup>239</sup> CDP Equity Spa, Leonardo Spa, Tim Spa, Sogei Spa.

finestra sui finanziamenti ricevuti, sulla loro efficacia e fra i tanti temi affrontati, il riferimento principale si è fatto alla “Missione” relativa alla trasformazione digitale dei servizi per i cittadini e le imprese mediante la migrazione dei dati delle pubbliche amministrazioni al cloud, Polo Strategico Nazionale. Come si è avuto modo di anticipare, il Polo Strategico Nazionale è un’organizzazione, un ecosistema, che pone in luce e interseca soluzioni infrastrutturali tenendo conto di standard di elevata tecnologia e qualità volti a portare la pubblica amministrazione a innovare i propri servizi in modo sicuro sostenibile e più efficiente possibile<sup>240</sup>. In particolare, il Polo Strategico Nazionale è, secondo l’AgID<sup>241</sup> “l’abilitatore primario della trasformazione digitale”.

Ciò in quanto, collabora concretamente con ogni pubblica amministrazione per controllare e progettare al meglio la migrazione e la sua evoluzione.

Il coordinamento complessivo invece spetta al Dipartimento per la Trasformazione Digitale.

La migrazione dei servizi verso il Polo Strategico Nazionale aiuta e coordina le amministrazioni pubbliche a ridurre drasticamente i processi amministrativi legati alla gestione di un data center di proprietà riducendone anche i costi<sup>242</sup> notevolmente.

Al fine di comprendere al meglio le modalità di migrazione verso il PSN, occorre sottolineare che le pubbliche amministrazioni che hanno scelto di migrare i propri servizi al PSN diventano il cliente finale di tutto l’ecosistema infrastrutturale che collabora con le competenze settoriali e specifiche dei soci (Tim, Leonardo, CDP e Sogei).

Il controllo sull’operato della pubblica amministrazione è tanto sulla migrazione dei dati e servizi quanto su ciò che accade successivamente e

---

<sup>240</sup><https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/02/21/strategia-infrastrutture-digitali-pubblica-amministrazione>

<sup>241</sup> <https://innovazione.gov.it/dipartimento/focus/polo-strategico-nazionale/>

<sup>242</sup> <https://www.polostrategiconazionale.it/>

dunque sulla concreta gestione dei servizi digitali che poi vengono erogati a cittadini e imprese.

Occorre dunque interrogarsi sulla concretezza di tali previsioni normative e sulla effettiva attuazione da parte delle pubbliche amministrazioni coinvolte e da parte dei soci individuati.

In altri termini, occorre comprendere in toto le modalità di collaborazione alla luce di quanto esaminato.

Per comprendere l'effettivo funzionamento del Polo Strategico Nazionale appare opportuno concentrarsi su un'analisi statistica.

Ciò che è stato evidenziato, è che il governo, nella quarta Relazione

Ebbene, si è avuto modo di precisare che l'obiettivo principale è ancora oggi quello di dotare le pubbliche amministrazioni di un Cloud sicuro digitale, di un'infrastruttura cloud sicura efficiente e affidabile.

La collaborazione tra Polo Strategico Nazionale e Pubbliche amministrazioni, consente di razionalizzare in sicurezza le infrastrutture pubbliche. Tra i principali punti di forza sono emersi in particolare, la previsione di *Data Center* al fine di assicurare risparmio energetico e garantire una affidabilità massima.

Inoltre, la conservazione di copie dei dati in tempo reale al fine di garantire una sicurezza certa è data dalla logica active-active che permette di effettuare concretamente dei backup e conservare i dati in tempo reale. In altri termini, Il Polo Strategico Nazionale garantirà alle pubbliche amministrazioni una gestione sicura e controllata dei propri dati tutti racchiusi in modo omogeneo e controllato nei Data Center dove la gestione dei dati e servizi può avere un forte impatto sul risparmio energetico e sulla spesa pubblica.

Inoltre, il risparmio dei costi di gestione, si potrà avere poiché la migrazione dei dati verso un cloud come il PSN che può dirsi “qualificato” e non di proprietà e privati, avviene mediante un finanziamento determinato dall'accesso a fondi previsti dal PNRR.

È possibile desumere che, ad oggi, l'effettiva e concreta migrazione dei servizi digitali negli ambienti di PSN ha compiuto enormi progressi e sta determinando sempre di più conseguenze positive come una trasformazione sia digitale che culturale dotata di un atteggiamento pragmatico e costruttivo volta sempre di più ad assicurare l'obiettivo principale di efficienza, trasparenza interoperabilità e sicurezza del cloud nazionale.

A questo punto, alla luce della disamina svolta, occorre soffermarsi sul punto di vista del giudice amministrativo.

Nello specifico, dopo aver evidenziato tutti gli aspetti positivi, la giurisprudenza ha avuto una fase di arretramento.

In particolare, il Consiglio di Stato, il 24 ottobre 2023<sup>243</sup> ha ritenuto illegittima l'aggiudicazione del Polo Strategico Nazionale al RTI composto da Tim spa, Leonardo, Sogei e CDP aventi un diritto di prelazione.

Ebbene, il Dipartimento per la trasformazione digitale della Presidenza del consiglio dei Ministri ad agosto 2022 aveva sottoscritto con l'RTI la convenzione per l'affidamento in concessione della progettazione e gestione dell'infrastruttura del Cloud Polo Strategico Nazionale successivamente all'aggiudicazione della gara poiché l'RTI vantava un diritto di prelazione rispetto agli altri operatori.

Ciò è rilevante poiché inizialmente, il raggruppamento composto da Fastweb e Aruba era risultati aggiudicatari della gara ma l'RTI composto da Tim, Sogei Leonardo e CDP in virtù del diritto di prelazione si era aggiudicata definitivamente l'appalto.

In ragione di ciò, il RTI secondo classificato composto da Fastweb e Aruba proponeva ricorso al TAR Lazio contro l'aggiudicazione del primo classificato avvenuta in virtù della prelazione.

---

<sup>243</sup> Cons. Stato, Sez. V, 24 ottobre 2023, n. 9210.

Il TAR Lazio<sup>244</sup> aveva accolto il ricorso ritenendo inammissibile l'offerta presentata dal RTI aggiudicatario poiché apportato modifiche non consentite al progetto di fattibilità posto a base della gara.

Di conseguenza, la Presidenza del Consiglio dei Ministri, il Ministero della Difesa, il Ministero dell'Economia e delle Finanze, Difesa Servizi spa chiedevano al Consiglio di Stato la riforma della sentenza non definitiva del TAR Lazio<sup>245</sup>.

Il Consiglio di Stato, pur ritenendo illegittima l'aggiudicazione del Polo Strategico Nazionale avvenuta per diritto di prelazione nei confronti del RTI Tim, vista l'innegabile strategicità dell'infrastruttura, ha ritenuto di non annullare l'aggiudicazione nei confronti del predetto operatore economico condannandolo al risarcimento del danno in favore del secondo classificato RTI Fastweb.

Prescindendo in questa sede dal merito processuale (la questione è ancora *sub iudice* in quanto la sentenza del Consiglio di Stato è stata impugnata ex articolo 111 ultimo comma della Costituzione dinnanzi alle Sezioni Unite della Corte di Cassazione), i fondi nazionali ed europei del PNRR relativi alla Missione 1.1 "Infrastrutture Digitali" dedicati alla migrazione esclusiva dei servizi digitali e dati delle pubbliche amministrazioni verso il Polo Strategico Nazionale non sono stati messi a rischio dalla sentenza del Consiglio di Stato. L'obiettivo fissato con il PNRR del Polo Strategico Nazionale quale cloud unico per le pubbliche amministrazioni ha mantenuto la sua importanza e

---

<sup>244</sup> Si veda V. CAMPANILE, *Art. 19, Codice dei Contratti Pubblici* by C. CONTESSA - P. DEL VECCHIO, Napoli, 2023.; P. CLARIZIA, *E-procurement*, in *The Digital State in the National Recovery and Resilience Plan*, Roma, 2022, 109; F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione*, in *L'azione amministrativa* a cura di A. ROMANO, Torino, Giappichelli, 2016, 242; G. CARLOTTI, *I principi nel codice dei contratti pubblici: digitalizzazione*, in *giustizia-amministrativa.it*, 2023, 6.

<sup>245</sup> Tar Lazio sez. 1 bis, 13 marzo, n. 4338 del 2023.

dunque il lavoro sinergico tra pubbliche amministrazioni e Polo Strategico Nazionale sta continuando verso la trasformazione digitale del Paese<sup>246</sup>.

In conclusione, può evidenziarsi che il cloud unico nazionale è un obiettivo, ad oggi già in fase di attuazione avente una funzione strategica e rilevante.

Ebbene, tutto ciò trova le sue radici nel principio del cloud first che vuole che la pubblica amministrazione abbandoni le infrastrutture IT proprietarie private per migrare e convertirsi verso una tecnologia cloud con i profili e le condizioni esaminate.

Ciò potrebbe diventare un criterio di regolazione essenziale della transizione digitale nella pubblica amministrazione anche se ancora occorre superare alcune lacune e carenze come l'assenza di un concreto piano organico con una visione complessiva e non frammentata dei processi di innovazione nel settore pubblico.

Si auspica che gli oneri imposti dai nuovi regolamenti in materia di protezione e circolazione dei dati determineranno un ordine nella gestione sia dei flussi informativi che dell'organizzazione interna nella migrazione dei dati e servizi<sup>247</sup>.

---

<sup>246</sup> <https://www.polostrategiconazionale.it/>

<sup>247</sup> F. TRIMARCHI BANFI, *Il diritto ad una buona amministrazione*, in M.P. CHITI, G. GRECO, *Trattato di diritto amministrativo europeo. Parte generale*, Tomo I, Milan, 2007, 49; S. CIVITARESE MATTEUCCI, "Umano troppo umano". *Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubbl*, 2019, p. 16; Y.N. HARARI, *Homo Deus, breve storia del futuro*, Milano, Bompiani, 2018.

## CAPITOLO IV

### Spunti Conclusivi

Riferendosi all'utilizzo dei sistemi di intelligenza artificiale da parte delle pubbliche amministrazioni, come si è avuto modo di analizzare nel presente lavoro, lo spazio amministrativo infrastrutturato è diventato oggi lo scenario di una nuova *“ecologia amministrativa, giuridica e ecosistemica”*<sup>248</sup>.

Il processo di piattaforma<sup>249</sup> della sfera pubblica richiede una *“ri-ontologizzazione delle categorie generali del diritto”* mediante la creazione di un nuovo costituzionalismo digitale ridefinendo i principi e le regole delle infrastrutture al fine di garantire una relazionalità democratica.

Sul punto, come affermato da autorevole Dottrina, *“le piattaforme di maggior successo non sono più semplici attori di mercato né banalmente estendono i mercati esistenti (mercati dei beni o delle idee, ma più radicalmente li sostituiscono dettando esse stesse le condizioni tecnologiche e giuridiche che presiedono allo svolgimento degli scambi”*<sup>250</sup>.

Occorre dunque svolgere al riguardo alcune riflessioni.

In primo luogo occorre osservare che i principio di imparzialità e di buon andamento della pubblica amministrazione enucleati dall'articolo 97 della Costituzione, possono trovare una protezione più concreta e dinamica mediante l'utilizzo delle nuove infrastrutture e degli strumenti di

---

<sup>248</sup> B. BOSCHETTI, *La transizione della pubblica amministrazione verso il modello Government as a platform*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. LALLI, Torino, 2022, p. 37.

<sup>249</sup> M. SORICE, *La piattaforma della sfera pubblica*, in *Comunicazione Politica*, 2020, n. 3, p. 371.

<sup>250</sup> G. RESTA, *Poteri privati e regolazione*, in *Enciclopedia del Diritto*, 2023, § 9.

digitalizzazione dei sistemi pubblici poiché volti, anche grazie all'utilizzo dei big data e dei sistemi di intelligenza artificiale, a convertire verso un'azione amministrativa meno opaca possibile.

Proprio la ricerca dell'eliminazione dell'opacità per offrire maggiori garanzie nell'utilizzo delle piattaforme digitali è il nuovo substrato del costituzionalismo "digitale" dove vi è la necessità concreta di bilanciare valori costituzionali e garantire forme di partecipazione del cittadino nella sfera pubblica.

Anche nel settore pubblico, dunque, è necessaria una rimodulazione delle categorie principali del diritto costituzionale, al fine di abbracciare ad ampio spettro il settore tecnologico in continua evoluzione. Le categorie generali non devono essere accantonate ma solo rimodulate alla luce delle nuove esigenze e dei nuovi regolamenti europei che influenzano fortemente il nostro ordinamento. Occorre tener conto, in altre parole, di un nuovo approccio alla tecnologia mediante un percorso di azione innovativo che tiene conto del rapporto autorità-libertà.

Le tecnologie all'avanguardia come i sistemi di intelligenza artificiale, le nuove connessioni, il web, hanno creato dei contesti di mercato totalmente innovativi che continuano a segnare il ruolo dell'essere umano. Si può concretamente affermare che anche l'amministrazione pubblica stia subendo l'evoluzione della tecnologia tentando comunque di svolgere, a fatica, il suo ruolo di "controllore".

A tal riguardo parte della dottrina ha fatto riferimento alla designazione di un nuovo "Stato digitale"<sup>251</sup>, o meglio una nuova era digitale in cui oltre a modificare gli strumenti e le metodologie utilizzate, viene richiesta costantemente alla sfera pubblica una ri-articolazione delle strutture pubbliche

---

<sup>251</sup> L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023, *passim*.

che hanno determinato una rimodulazione delle regole di esercizio del pubblico potere, nonché delle modalità di controllo dello stesso.

L'evoluzione delle nuove tecnologie impone quindi un serrato processo di digitalizzazione della sfera pubblica, mediante, tra l'altro, la realizzazione di un'architettura *cloud* all'interno del quale si vuole assicurare (come si è avuto modo di analizzare) la prestazione di servizi pubblici in modalità *cloud* per agevolare il riutilizzo dei dati nella prospettiva di una "nuova amministrazione" volta a semplificare le difficoltà imposte dalle pesanti procedure devolute all'essere umano. Tuttavia, occorre sottolineare che le predette implementazioni impongono implicitamente di mantenere un equilibrio tra le esigenze di protezione dei dati personali e i principi di "buona amministrazione"<sup>252</sup> previsti dall'articolo 41 della Carta dei diritti Fondamentali dell'Unione Europea.

La debolezza di uno dei fattori di sviluppo tecnologico individuati nell'interconnessione tra piattaforme, algoritmi e dati può dequotare la solidità della nuova amministrazione. In altri termini, occorre tener conto in tutti i settori analizzati nei precedenti capitoli dell'importanza di un temperamento tra i contrapposti interessi in gioco, alla luce di un bilanciamento tra le vere e proprie esigenze di *good administration* da un lato e esigenze di semplificazione mediante l'utilizzo di nuove tecnologie.

Orbene, nella descritta ridefinizione del modello di amministrazione pubblica occorre sottolineare che l'interoperabilità e la digitalizzazione tra sistemi informatici, rappresenta una sfida importante e una grande opportunità di sistema al fine di migliorare concretamente un processo trasparente ed efficiente della trasmissione di dati ed erogazione di servizi. È proprio per questo che nell'analisi svolta si è fatto principalmente riferimento ad una

---

<sup>252</sup> Sul punto si veda D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedurali nei confronti della Pubblica Amministrazione*, in *RIDPC*, 2005/3, p. 819 ss.

pluralità di obiettivi fissi da raggiungere. Nello specifico, è di particolare rilievo che la pubblica amministrazione sviluppi delle modalità di funzionamento e gestione dei dati efficaci e volte a garantire un'interscambiabilità tra una pluralità di piattaforme e banche dati esistenti e distinte tra loro che dovranno dunque iniziare a “dialogare”.

In definitiva, dall'analisi svolta, è evidente che entro il 2026 sarà rafforzata la trasformazione digitale del Paese anche grazie al Piano Triennale per l'informatica nella Pubblica Amministrazione redatto da AgID il 12 febbraio 2023 con il quale è stata promossa la trasformazione digitale delle pubbliche amministrazioni italiane.

Il Piano Triennale 2024 – 2026, in particolare, ha una strategia peculiare che consente di tratteggiare le fondamenta solide per individuare un'architettura organizzativa e tecnologica con l'obiettivo di supportare la collaborazione tra i livelli istituzionali, nonché tra questi e gli amministrati. Il Piano ha un pregio peculiare per la presente ricerca poiché oltre a delineare la strada verso una consapevolezza maggiore per l'utilizzo delle tecnologie nella pubblica amministrazione, contiene un capitolo interamente dedicato all'utilizzo dell'Intelligenza Artificiale nel settore pubblico. Nello specifico, nel piano sono state definite delle linee guida e degli obiettivi chiari da seguire. Tra gli obiettivi primari vi è quello di un'organizzazione solida delle PA come si è visto con il PSN (cfr. Capitolo III), indirizzando in concreto il funzionamento di un sistema informativo pubblico complessivo del Paese nel rispetto del principio del *cloud first* e di una struttura antropocentrica e decentrata con l'individuazione di strumenti e tecniche che consentano anche una pianificazione concreta degli investimenti. Tra i principi guida che possono riassumere l'opera di trasformazione digitale, si è vista l'importanza del *cloud first* secondo cui le pubbliche amministrazioni in fase di definizione di un progetto innovativo o di sviluppo di nuovi servizi, devono adottare il paradigma *cloud* e utilizzare infrastrutture digitali adeguate. Inoltre, i servizi

pubblici da ora in avanti dovranno essere progettati ed erogati in modo da garantire non solo la sicurezza ma in particolar modo la protezione dei dati personali. Un altro principio che si è avuto modo di analizzare è il principio del *once only* che consente alle pubbliche amministrazioni di evitare di chiedere ai cittadini e alle imprese delle informazioni già fornite rendendo disponibile a livello transfrontaliero i servizi pubblici rilevanti. Dalla lettura del piano, appare anche opportuno sottolineare l'importanza della volontà di supportare la personalizzazione dei servizi incentrata sull'utente con l'aumento dell'efficacia di erogazione di servizi pubblici con meccanismi di proattività, il miglioramento del processo decisionale basato sui dati.

Tra le ulteriori sfide poste dal processo di digitalizzazione si ricorda l'utilizzo di sistemi di IA nel settore pubblico. Sul punto, oltre al Regolamento Europeo sull'IA (analizzato nei capitoli precedenti) appare opportuno dare conto anche dell'importanza del disegno di legge del 23 aprile 2024 approvato dal Consiglio dei Ministri su proposta del Presidente e del Ministro della Giustizia per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale.

Il disegno di legge, non si sovrappone al Regolamento Europeo sull'IA, bensì *“accompagna il quadro regolatorio in quegli spazi propri del diritto interno tenuto conto che il regolamento è impostato su un'architettura di rischi connessi all'uso dell'intelligenza artificiale”*<sup>253</sup>.

Sempre al fine di adeguarsi al regolamento sull'IA, le norme prevedono che il ciclo di vita di tutti i sistemi di intelligenza artificiale si debba basare sul rispetto dei diritti fondamentali e delle libertà nonché sui principi richiamati nel presente lavoro ancora prima del suddetto disegno di legge, in particolare, sul principio di trasparenza, proporzionalità, valorizzazione economica del dato e riservatezza.

---

<sup>253</sup> <https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501>

Il presente disegno di legge consente di avvalorare e dare concretezza alle riflessioni svolte sull'importanza del rispetto della vita democratica del Paese, della tutela dei diritti fondamentali e del necessario bilanciamento tra trasparenza e riservatezza nell'utilizzo di tali sistemi sia nel settore pubblico che nel settore privato ogni qualvolta vi sia il rischio di una compromissione dei dati personali.

Con specifico riguardo al settore della pubblica amministrazione, per quel che qui rileva, le norme prevedono la regolazione del settore come già predisposto dal regolamento europeo, al fine di garantire il buon andamento e l'efficienza dell'attività amministrativa cercando di incentrare lo sviluppo tecnologico in tale settore verso una visione antropocentrica tenendo conto il principio dell'autodeterminazione e della responsabilità umana.

Sul dibattito circa l'autorità nazionale competente in materia, nel presente lavoro si era fatto riferimento alla professionalità del Garante per la protezione dei dati personali che da anni si occupa del tema come autorità indipendente e imparziale, tuttavia, nel presente disegno di legge il compito di garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di Intelligenza Artificiale è stato attribuito all'AgID e all'Agenzia per la cybersicurezza nazionale ciascuna per quanto di rispettiva competenza al fine di assicurare l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale in conformità alla normativa dell'Unione Europea e nazionale.

Ragionando su una pubblica amministrazione fruitrice di open data, è possibile evidenziare questi ultimi, possano essere considerati un utile strumento per aumentare le possibilità di controllo dell'amministrazione stessa e sul suo operato. Ciò in quanto, si realizza, mediante l'apertura dei dati, una

“democratizzazione dell’interpretazione degli stessi”<sup>254</sup> in una nuova visione prospettica di alleanza tra il cittadino e l’amministrazione pubblica.

Invero, informazioni e dati diventano progressivamente lo strumento cardine dell’attivazione di forme di collaborazione Stato-cittadino e coinvolgimento di quest’ultimo nell’iter decisionale pubblico.

Tra le prospettive future, si auspica un’implementazione del processo di “democratizzazione”, caratteristica cardine del diritto alla privacy attinente all’asservimento tecnologico dell’uomo<sup>255</sup>. Invero, al fine di promuovere una civiltà digitale, è necessario avere a mente un contesto digitale e sociale in cui la direzione dell’innovazione tecnologica non venga subita dall’essere umano ma da esso partecipata e agita<sup>256</sup>.

Con l’avvento della società digitale nonché con la diffusione dell’IA, l’attitudine democratica della privacy e la sua capacità di ampliarsi e adattarsi al nuovo contesto ha comunque reso evidente l’importanza di una guida antropocentrica del processo di innovazione tecnologica al fine di garantire una collaborazione congiunta senza sostituzioni automatiche.

L’uomo “connesso” deve essere tutelato al fine di vedersi garantito il diritto a un libero sviluppo della sua personalità non solo nel contesto “digitale” (*i.e.* con la creazione del concetto di “nuovo soggetto giuridico digitale”), ma anche nel contesto “reale/analogico” ove dev’essere garantito il medesimo livello di protezione dei diritti fondamentali.

Non si può non tener conto del fatto che pur non volendo sostituire con soluzioni tecnologiche nuove l’essere umano, quest’ultimo si trova a doversi

---

<sup>254</sup> F. COSTANTINO, *Gli open data come strumento di legittimazione delle istituzioni pubbliche?*, in *L’amministrazione pubblica con i big data: da Torino un dibattito sull’intelligenza artificiale*, a cura di R. CAVALLO PERIN, Torino, 2021, p. 160.

<sup>255</sup> P. STANZIONE, *Conclusioni a tutela della persona*, in *Il ruolo del Garante per la protezione dei dati personali. La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. CERRINA FERONI, Bologna, 2023, p. 285.

<sup>256</sup> P. STANZIONE, *Conclusioni a tutela della persona*, in *Il ruolo del Garante per la protezione dei dati personali. La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. CERRINA FERONI, Bologna, 2023, p. 287.

ri-adattare a nuove realtà in continua evoluzione inserendosi in un complesso nuovo con dimensioni trasformate del potere pubblico.

Tra le sfide future dunque, è evidente che occorre avere a mente una società nuova ove si consenta all'amministrato di valutare, comprendere, partecipare, ad un sistema nuovo che veda la sfera pubblica servirsi di sistemi di intelligenza artificiale senza sovrapposizioni ma con complementarità.

Autorevoli Studiosi<sup>257</sup> hanno proposto delle raccomandazioni finalizzate a utilizzare gli strumenti di intelligenza artificiale anche in virtù del nuovo regolamento approvando secondo una prospettiva positiva, antropocentrica e omogenea.

In tale scenario, uno dei rischi più significativi è quello del “*digital divide*” con il quale si vuole intendere l'incapacità concreta di cittadini (non necessariamente appartenenti a categorie particolari) nel relazionarsi con gli strumenti tecnologici a disposizione sia sul piano valoriale che economico.

Ciò determina sicuramente delle diseguaglianze nella popolazione.

In primo luogo, preventivamente, si dovrà verificare in concreto, alla luce della normativa vigente e dei regolamenti trasversali, quali compiti possono essere delegati interamente (e quali non) ai sistemi di intelligenza artificiale.

In secondo luogo, occorre tener conto che in futuro dovrà propendersi per lo sviluppo di strutture idonee a sviluppare la spiegabilità dei sistemi di intelligenza artificiale nonché implementare un'adeguata alfabetizzazione digitale dei cittadini. Ciò in quanto, la fiducia del cittadino nei confronti di tali sistemi può essere promossa e soprattutto implementata mediante l'introduzione di meccanismi e tecniche accessibili che consentano di contenere i costi derivanti da danni arrecati da sistemi e tecnologie di intelligenza artificiale non utilizzate secondo le opportune modalità.

---

<sup>257</sup> L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppo, opportunità, sfide*, Raffaello Cortina Editore, 2022, 279.

Spetterà ai giuristi, ricercare concretamente le modalità attraverso cui l'intelligenza artificiale potrà essere utilizzata a beneficio di tutte le classi sociali senza intaccare i diritti e le libertà costituzionali dei cittadini.

In conclusione, primi segnali di una presa di coscienza del legislatore nazionale rispetto ai temi trattati nel presente elaborato sembrano ricavarsi dalla lettura del citato disegno di legge che si auspica possa entrare in vigore senza discostarsi dal quadro normativo europeo in materia di protezione dati personali e IA, così da garantire agli amministrati un contesto regolatorio il più possibile chiaro ed esaustivo.

## BIBLIOGRAFIA

- T. COOLEY, *A treatise on the Law of Torts or the Wrongs which arise independent of contracts*, 1888, University of Michigan Law School.;
- A. BALDASSARRE, *Privacy e costituzione: L'esperienza statunitense*, Roma, 1974;
- V. MAYER SCHONBERGER, *Delete: the virtue of forgetting in the digital age*, Princeton University Press 2009.
- V. VARANO - V. BARSOTTI, *La tradizione giuridica occidentale, testo e materiali per un confronto civil law common law*, settima edizione, Giappichelli Editore, Torino, 2021;
- C. COLAPIETRO, *The impact of the information and technology revolution on constitutional rights with particular attention to personal data protection issues*, in M. BELOV (a cura di), *Information and Technology Revolution and its impact on State, Constitutionalism and Constitutional Law*, London, 2020;
- S. RODOTÀ, *Riservatezza*, in Enciclopedia Italiana – VI Appendice 2000, [treccani.it](http://treccani.it);
- S. RODOTÀ, *Tecnologia e diritto*, il Mulino, 2021;
- S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. CONTI, Editori Laterza, 2005;
- S. RODOTÀ, R. ZACCARIA, *Diritto dell'informazione e della comunicazione*, Padova, 2007;
- L. PALADIN, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in *La libertà d'informazione*, a cura di L. Paladin, Torino, 1979;

- M. TIMIANI, Un contributo allo studio sul diritto alla riservatezza, in Riv. studi. parl. pol. cost., 176/2012, 51 ss.; G. Busia, Riservatezza (diritto alla), in Dig. disc. pubbl., agg., 2000.
- A. TORRENTE – P. SCHLESINGER, Manuale di diritto privato, ventiseiesima edizione, Giuffrè Editore, luglio 2023;
- F. GAZZONI, Manuale di diritto privato, Edizioni scientifiche italiane, 2023.
- G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Il Mulino, 2007.
- A. WESTIN, *Privacy and freedom*, Atheneum, n.y., 1967.
- G. PASCUZZI, *Il diritto dell'era digitale*, pag. 82 e ss, Il mulino 2020.
- A. MONTI – R. WACKS, *Protecting personal information, the right to privacy reconsidered*, 30 maggio 2019, Hart Pub Ltd.
- G. CERRINA FERRONI, *Il Ruolo del Garante per la protezione dei dati personali, La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, Il Mulino, Bologna, 2023.
- W.V. GERVEN, *The European Union a polity of States and Peoples*, Stanford University Press, California, 2005, p.7 e ss.;
- A.M. CALAMIA – V. VIGIAK, *Diritto dell'Unione Europea*, Giuffrè, Milano, 2018, p.5 e ss.;
- G.TESAURO, *Diritto dell'Unione Europea*, Cedam, Padova, 2012, p.1 e ss.;
- L. NEVILLE BROWN – T.KENNEDY, *The Court of Justice of the European Communities*, Sweet and Maxwell, London, 2000, p.2 e ss.;
- C. AMALFITANO- M. CONDINANZI, *Unione Europea, fonti, adattamento e rapporti tra ordinamenti*, Giappichelli Editore, Torino, 2015, p.1 e ss.;

- S. WEATHERILL, *Cases and Materials on EU Law*, Oxford University Press, New York, 2007, p.5;
- F. POCAR, *Diritto dell'Unione Europea*, Giuffrè Editore, Milano, 2010, p.7 e ss.;
- R. ADAM-A.TIZZANO, *Manuale di diritto dell'Unione Europea*, Giappichelli Editore, Torino, 2017, p.18 e ss.;
- U.DRAETTA, *Elementi di diritto dell'Unione Europea*, Giuffrè Editore, Milano, 2014, p.7 e ss.;
- N. BOSCHIERO - T. SCOVAZZI - C. PITEA – C. RAGNI, *International Courts and the Development of International Law – Essays in Honour of Tullio Treves*, Springer - Asser Press, UK, 2013;
- E. DI SALVATORE, *L'identità costituzionale dell'Unione Europea e degli Stati membri, il decentramento politico – istituzionale nel processo di integrazione*, Giappichelli Editore – Torino, 2008;
- G. NOLTE, *European and Us Constitutionalism*, Cambridge University Press, 2005.
- M.A. SANDULLI, *I Principi costituzionali e comunitari di giurisdizione amministrativa*, in *Il nuovo processo amministrativo*, a cura di M.A. SANDULLI, Giuffrè Editore, Milano, 2013, p. 29.
- M. CARTABIA, *La tutela multilivello dei diritti fondamentali. Il cammino della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona*, in [cortecostituzionale.it](http://cortecostituzionale.it), 2014.
- U.VILLANI, *Istituzioni di Diritto dell'Unione Europea*, Cacucci Editore, Bari, 2017.
- A.CELOTTO, *L'Italia e l'Unione Europea*, in *Diritto Pubblico*, a cura di F. MODUGNO, Giappichelli Editore, Torino, 2015, p. 218.
- M.P. CHITI, *Diritto Amministrativo Europeo*, Giuffrè Editore, Milano, 2011, p. 34 e ss.

- C. KOENIG- A. HARATSCHB - M. BONINI, *Diritto Europeo*, Giuffrè Editore, 2000, p.4;
- G. STROZZI - R. MASTROIANNI, *Diritto dell'Unione Europea parte istituzionale*, Giappichelli Editore, Torino, 2013, p.11 e ss.;
- F. POLITI, *Temi di diritto dell'Unione Europea*, Giappichelli Editore, Torino, 2015, p.28;
- J.H. JANS – R. DE LANGE – S. PRECHAL – R.J.G.M. WIDDERSHOVEN, *Europeanisation of Public Law*, Europa Law Publishing, 2007.
- N. RONZITTI, *Introduzione al diritto internazionale*, Giappichelli Editore, Torino, 2013, p. 313;
- S. BARTOLE – P. DE SENA – V. ZAGREBELSKY *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2012;
- A. ROYER, *Le Conseil d'Europe*, Les essentiel Milan, 2009;
- C. ZANGHÌ, *Diritto delle organizzazioni internazionali*, Giappichelli Editore, Torino, 2013;
- M. ALLENA, *Art 6 CEDU, procedimento e processo amministrativo*, Editoriale Scientifica, Napoli, 2012;
- G.RAIMONDI, *Il consiglio d'europa e la convenzione europea dei diritti dell'uomo*, Editoriale Scientifica, Napoli, 2009;
- U. DRAETTA-M.F. MERAVIGLIA, *Il diritto delle organizzazioni internazionali, parte speciale*, Giuffrè Editore, Milano, 2011, p.359 e ss; *Convenzione Europea dei diritti dell'Uomo e delle libertà fondamentali* in [treccani.it](http://treccani.it) ;
- R. ROMBOLI, *La influenza della Cedu e della giurisprudenza della Corte Europea dei diritti umani nell'ordinamento Costituzionale italiano*, dicembre 2018, in [giurcost.org](http://giurcost.org);

- R.DICKMANN , *Corte Costituzionale e diritto internazionale nel sindacato delle leggi per contrasto con l'articolo 117 primo comma della Costituzione* in federalismi.it.
- V. PICCONE- O. POLLICINO, *La carta dei diritti fondamentali dell'Unione Europea efficacia ed effettività*, Editoriale Scientifica, Napoli, 2018; R. MASTROIANNI- O. POLLICINO- S. ALLEGREZZA- F. PAPPALARDO- O. RAZZOLINI , *Carta dei diritti fondamentali dell'Unione Europea*, Giuffrè Editore, Milano.
- M. FRAGOLA, *Il Trattato di Lisbona che modifica il trattato sull'Unione Europea e il Trattato della Comunità Europea, versione ragionata e sistematica per una consultazione coordinata degli articoli alla luce dei Protocolli e delle Dichiarazioni*, Giuffrè Editore, Milano, 2010;
- P. BILANCIA- M. D'AMICO, *La nuova Europa dopo il trattato di Lisbona*, Giuffrè Editore, Milano, 2009;
- E. CHITI – B.G. MATTARELLA, *Global Administrative Law and Eu Administrative Law, Relationship, Legal issues and Comparison*, Springer, 2011;
- S. R. BEDI, *The development of Human Rights Law by the Judges of the International Court of Justice – Studies in International Law*, Hart Publishing – Oxford – Portland Oregon, 2007;
- F. BIONDI, *Quale dialogo tra le Corti?*, in Federalismi.it, 2019.
- G. PASQUALI, *Le novità del Trattato di Lisbona*, Edizioni Nuova Cultura, Roma, 2010;
- V.M. BRESCIA, *Le competenze dell'Unione Europea nel Trattato di Lisbona*, Edizioni scientifiche italiane, Roma, 2008; A. ADINOLFI, *I fondamenti del diritto dell'UE nella giurisprudenza della Corte di Giustizia: il rinvio pregiudiziale*, in *Il dir. un. eur.*, 2019;
- R. BIFULCO, *La Costituzione Italiana dopo il Trattato di Lisbona*, in *Riv. it. dir. pubbl. comunit.*, 2012;
- E. CANNIZZARO, *Sui rapporti tra sistemi processuali nazionali e diritto dell'Unione Europea*, in *Dir. un. eur.*, 2008.

- M.A. SANDULLI, *Principi e regole dell'azione amministrativa*, Giuffrè Francis Lefebvre, 2020, pp.107 e ss.
- V. LOPILATO, *Manuale di diritto amministrativo, parte generale*, terza edizione, Giappichelli Editore, 2021,
- T. BALLARINO, *Diritto dell'Unione Europea*, Cedam, Padova, 2010, p. 173;
- R. DEHOUSSE, *The European Court of Justice*, European Union Series, New York, 1998 ;
- G.D. BÜRCA-J.H.H. WEILER, *The European Court of Justice*, Oxford University Press, Oxford;
- G. CAGGIANO, *La Corte di Giustizia difende il principio del primato a fronte della ribellione delle corti costituzionali di Polonia, Ungheria e Romania*, in *Studi sull'integrazione europea*, Cacucci Editore, 2021, pp.473 e ss;
- G. GERIN, *La Corte di Giustizia delle Comunità Europee*, Cedam, Padova, 2010, p. 34.
- H. KELSEN, *Lineamenti di dottrina pura del diritto*, Piccola Biblioteca Einaudi, Torino, 1952, p.155
- G. PALMISANO, *Il Sistema giuridico internazionale e l'ordinamento comunitario*, 2012, in *treccani.it*.
- A.ROYER, *Le Conseil d'Europe*, Les essentiels Milan, 2009;
- G.RAIMONDI, *Il consiglio d'europa e la convenzione europea dei diritti dell'uomo*, Editoriale Scientifica, Napoli, 2009;
- C.ZANGHÌ, *Diritto delle organizzazioni internazionali*, Giappichelli Editore, Torino, 2013;
- U.DRAETTA-M.F.MERAVIGLIA, *Il diritto delle organizzazioni internazionali, parte speciale*, Giuffrè Editore, Milano, 2011, p.359 e ss.

- R.ROMBOLI, *La influenza della Cedu e della giurisprudenza della Corte Europea dei diritti umani nell'ordinamento Costituzionale italiano*, dicembre 2018, in giurcost.org
- C.COLAPIETRO - M.RUOTOLO, *Diritti e Libertà in Diritto Pubblico*, a cura di F. MODUGNO, cit, p. 641 e ss.
- PV. DASTOLI, *Corte Europea dei diritti dell'Uomo*, in treccani.it
- C. MASCIOTTA in *Il ricorso diretto a Strasburgo in deroga al principio del previo esaurimento, ex art 35 cedu : un possibile cortocircuito tra sistema costituzionale e convenzionale di tutela? In osservatoriosullefonti.it*, 2018.
- F.A. BELLA, *Tra Procedimento e Processo, contributo allo studio delle tutele nei confronti nella pubblica amministrazione*, cit., p.217ss;
- R.ROMBOLI, *la influenza della Cedu e della Giurisprudenza della Corte Europea dei diritti umani nell'ordinamento costituzionale italiano*, in giurcost.org
- G.SILVESTRI, *Le limitazioni della sovranità statale in favore dell'Unione Europea nella giurisprudenza costituzionale – il sistema delle fonti*, a cura di RICCARDO NEVOLA, in cortecostituzionale.it
- D.TEGA *Le sentenze della Corte Costituzionale nn.348 e 349 del 2007: la CEDU da fonte ordinaria a fonte subcostituzionale del diritto*, in forumcostituzionale.it.
- M. C. CARROZZA, C. ODDO, S. ORVIETO, A. DI MININ, G. MONTEMAGNI, *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale*, in *BioLaw Journal*, n. 3, 2019, p. 245 e ss;
- C. CASONATO, *Intelligenza Artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019, pp. 101-130.

- P.G. CHIARA, *Sistemi intelligenti autonomi e responsabilità civile: stato dell'arte e prospettive nell'esperienza comunitaria*, in *Diritto ed economia dell'impresa*, n. 1, 2020;
- A. SIMONCINI, *L'algoritmo incostituzionale: Intelligenza Artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n.1, 2019, pp. 69-71.;
- J. BURREL, *How the machine 'thinks': Understanding opacity in machine learning*
- E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.*, n. 3, 2022, p. 1120.;
- D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Riv. it. inf. e dir.*, n. 2, 2022.
- F. LA VIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *Osservatorio sulle fonti*, n. 3, 2021, pp. 1163 ss;
- C. COLAPIETRO, *Gli algoritmi tra trasparenza e protezione dei dati personali*, 22 febbraio 2023, Osservatorio sulla Trasparenza, in [Federalismi.it](http://Federalismi.it);
- L. VIOLANTE, A. PAJNO, *Diritto e etica dell'Intelligenza Artificiale. Presentazione.*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3, 2019;
- F. PIZZETTI, (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018;
- E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.*, n. 3, 2022;

- D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Riv. it. inf. e dir.*, n. 2, 2022.
- S. CAL, *Il quadro normativo vigente in materia di IA nella Pubblica Amministrazione (CAD, GDPR, IA ACT) in Intelligenza Artificiale per la pubblica amministrazione, Principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini giuridica, 2023;
- A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico? Focus Lavoro, persona, tecnologia*, 18 ottobre 2023, in *Federalismi.it*;
- C. NOVELLI, *L'artificial Intelligence Act Europeo: alcune questioni di implementazione*, 24 gennaio 2024 in *Federalismi.it*;
- T. AVEN, *Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation*, in *European Journal of Operational Research*, 253, n. 1, 2016.
- A. SIMONCINI, M. G. LOSANO, “*La lunga marcia dell'informatica nelle istituzioni italiane, in il diritto dell'amministrazione pubblica digitale*” a cura di R. Cavallo Perin e Diana Urania Galetta, 2020, Giappichelli Editore, Introduzione.
- G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>*.
- A. CORRADO *Il principio di trasparenza*, in M. A. SANDULLI, (a cura di), *Principi e regole dell'azione amministrativa*, Giuffrè Editore, Milano, 2023;
- A. CORRADO *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018;

- F. MERLONI, *La trasparenza amministrativa*, Milano, Giuffrè, 2008;  
M.R. SPASIANO, *I principi di pubblicità. Trasparenza e imparzialità*, in *Codice dell'azione amministrativa*, (a cura di) M. A . SANDULLI, Milano, 2017;
- C. COLAPIETRO – A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, a cura di C. COLAPIETRO – L. CALIFANO, Editoriale Scientifica, Napoli, 2014, pp. 117 e ss;
- M. A . SANDULLI – L. DROGHINI, *La trasparenza amministrativa nel FOIA italiano. Il principio della conoscibilità generalizzata e la sua difficile attuazione*, in *Federalismi.it*, 2020;
- M. A. SANDULLI, *Voce Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, IV aggiorn., Milano, 2000;
- V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte Costituzionale (n. 20/2019)*, in *federalismi.it*, n. 5, 2020;
- P. CANAPARO, *La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni*, in *Federalismi.it*, 2014;
- A. SIMONATI, *La ricerca in materia di trasparenza amministrativa: stato dell'arte e prospettive future*, in *Dir. amm.*, 2018;

- C. COLAPIETRO – C. SANTARELLI, *Accesso civico*, in *Libro dell'Anno del Diritto 2014*, in Treccani.it.
- G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>*.
- P. STANZIONE, *Il potere dell'innovazione e la solitudine digitale la protezione dei dati a tutela della persona*, Relazione annuale sull'attività svolta dal Garante per la protezione dei dati personali, Presidente Pasquale Stanzone, 2022.
- A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'Intelligenza Artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, pp. 87 ss
- P. OTRANTO, *Riflessioni in tema di decisione amministrativa, Intelligenza Artificiale e legalità*, in *Federalismi.it*, n. 7, 2021;
- E. FALLETTI, *La formazione delle black box: garanzie della privacy e tutela antidiscriminatoria*, in M. D'AMICO, B. LIBERALI, ANTONIO P. MIRAS, E. C. RAFFIOTTA, S. ROMBOLI, G. M. TERUEL LOZANO (a cura di), *Europa, società aperta. Problemi attuali e prospettive future*, ESI, Napoli, 2022;
- G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 11 agosto 2018, n. 101*, Bologna, 2017;
- A.D. SELBST, J.POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 2017;

- G. FINOCCHIARO, F. PAOLUCCI, O. POLLICINO, *Intelligenza artificiale e diritti individuali a perimetro ancora incerto*, in *Il Sole 24 ore*, 16 giugno 2023.
- G. PITRUZZELLA, *Le autorità amministrative indipendenti: bilancio e prospettive*, in *Il ruolo del Garante per la protezione dei dati personali, la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di Ginevra Cerrina Feroni, Il Mulino, 2024;
- G.P. CIRILLO – R. CHIEPPA, *Le Autorità amministrative indipendenti*, in G. Santaniello, *Trattato di diritto amministrativo*, vol. 41. Padova, Cedam, 2010;
- G. P. ALPA – A. CATRICALA', *Diritto dei consumatori*, Bologna, Il Mulino, 2016.
- G. CERRINA FERONI, *Le stagioni del Garante. La privacy e il cambiamento del Paese*, G. CERRINA FERONI, *Intelligenza Artificiale e ruolo della protezione dei dati personali*, il Mulino 2024, pp. 59 e ss. L'analisi di Ginevra Cerina Feroni (Garante Privacy) intervento disponibile su <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.
- G. D'ACQUISTO, *Trattamento dei dati personali e processo decisionale automatizzato nella PA*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 203 e ss;
- A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*. in *Il diritto dell'amministrazione pubblica digitale*, a cura di R. Cavallo Perin e D. U. Galetta, Giappichelli Editore, 2020, p. 21 e ss.
- A. CORRADO, *La Trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, 22 febbraio 2023, in [Federalismi.it](https://www.federalismi.it).

- T. COCCHI, *La partecipazione procedimentale*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 134 e ss
- A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 174 e ss.
- M.S. Giannini, *Rapporto sui principali problemi dell'Amministrazione dello Stato*, 16 novembre 1979.
- D.U. GALETTA – J. G. CORVALAN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi*, 3/2019;
- M. A. SANDULLI, *Il Giudizio amministrativo, Principi e regole*, Editoriale Scientifica Napoli, 2024;
- V. LOPILATO, *Manuale di diritto amministrativo*, II, III ed., ,Torino, 2023;
- P. CHIRULLI, *La partecipazione al procedimento*, in *Principi e regole dell'azione amministrativa*, a cura di M. A SANDULLI, Milano, 2023;
- M. SPASIANO, *Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto*, in *Dir. dell'Econ.*, 2022, 30.
- L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023
- E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2, 2020, 281;
- U. ALLEGRETTI, *Democrazia partecipativa*, in *Enc. dir., Annali*, V, Milano, 2011;

- A. G. OROFINO – G. GALLONE, L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione, in *Giur. it.*, 7, 2020, 1738 ss;
- S. TRANQUILLI, Rapporto pubblico – privato nell'adozione della decisione amministrativa "robotica", in *Dir. soc.*, 2, 2020, 281 ss;
- A. ALEMANNI, Unpacking the principle of openness in EU Law. Transparency, participation and democracy, in *Eur. Law Rev.*, 2014.
- Vedasi E. CARLONI, Tendenze recenti e nuovi principi della digitalizzazione pubblica, in *Giornale Dir. Amm.*, n.2, 2015.;
- E. CARLONI, La qualità delle informazioni pubbliche, l'esperienza italiana nella prospettiva comparata, in *Rivista trimestrale di diritto pubblico*, 2009;
- S. CASSESE, che cosa resta dell'amministrazione pubblica?, in *Riv. trim. dir. pub.*, n. 1, 2019.;
- P. COSTANZO, La democrazia digitale. Precauzioni per l'uso, in *Diritto pubblico*, 1, 2019.
- D.U. GALETTA, Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT), in *Diritto dell'Amministrazione pubblica digitale*, Giappichelli, 2020;
- D.U. GALETTA – J. G. CORVALÁN, Intelligenza Artificiale per una Pubblica Amministrazione 4.0 potenzialità, rischi e sfide della rivoluzione tecnologica in atto, in *federalismi.it* 6 febbraio 2019.
- F. FAINI, Trasparenza, apertura e controllo democratico dell'amministrazione pubblica, in *Cib. dir.*, 2014;
- E. BELISARIO – F. RICCIULLI, Legalità algoritmica e vizi procedurali, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 159 e ss.

- A. CORRADO, Discrezionalità algoritmica e sindacato del giudice amministrativo, in *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p. 175 e ss.
- G. CERRINA FERONI, *La dimensione umana nell'era dei dati e delle intelligenze artificiali in occasione del convegno "Il diritto e le nuove dimensioni dell'essere"*. In ricordo di Antonio Palma, Fondazione Cesifin 11 marzo 2024.
- M.A. SANDULLI, usa espressione nel testo *Principi e regole dell'azione amministrativa*, a cura di M.A. SANDULLI Milano, Giuffrè 2023.
- F. NASSUATO, *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*, in *Ceridap*, 2022.
- C. TASSO, Attori, processi, meriti e responsabilità nell'utilizzo di algoritmi di Intelligenza Artificiale: Il caso del Machine Learning, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di Roberto Cavallo Perin, Università degli studi di Torino, 2020, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino, pp 19 e ss;
- P. CARROZZA, *Governo e amministrazione*, in *Diritto costituzionale comparato*, a cura di P. Carrozza, A. Di Giovine e G.F. Ferrari, Laterza, Roma – Bari, 2017.
- F. PATRONI GRIFFI, *Il giudice amministrativo oggi: ruolo, etica, responsabilità*, Relazione introduttiva al Primo congresso nazionale dei Magistrati amministrativi, Palazzo Spada, 7-8 giugno 2019, in [www.giustizia-amministrativa.it](http://www.giustizia-amministrativa.it);
- A. TRAVI, *Eccesso di potere giurisdizionale e diniego della giurisdizione dei giudici speciali al vaglio delle Sezioni Unite della Cassazione*, intervento al Seminario di Studi tenutosi presso la Corte di Cassazione di Roma, 21 settembre 2017;

- C. MEOLI, *Il declino della legge statale*, in *Libro dell'anno del Diritto*, Roma, 2013.
- P. STANZIONE, L'uomo e le macchine: una visione antropocentrica dell'Intelligenza Artificiale, in *AI Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il mulino, 2022.
- A. CORRADO, La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica, in *Osservatorio sulla trasparenza in Federalismi*, 22 febbraio 2023.
- M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Editoriale Scientifica 2023.
- G. D'ACQUISTO, in *Intelligenza artificiale, sicurezza nazionale e difesa*, in *AI Anthology Profili giuridici, economici e sociali dell'Intelligenza Artificiale*, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il Mulino, 2022, pp 309 e ss:
- N. RANGONE, Intelligenza Artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli, con prefazione di M. Clarich, Giappichelli, 2022.
- G. D'ACQUISTO, *Intelligenza Artificiale per la Pubblica Amministrazione, principi e regole del procedimento amministrativo algoritmico*, a cura di E. Belisario e G. Cassano, Pacini Giuridica, p.204 e ss.
- M. PANDOLFI, in *Intelligenza artificiale, sicurezza nazionale e difesa*, in *AI Anthology Profili giuridici, economici e sociali dell'Intelligenza Artificiale*, a cura di G. Cerrina Feroni, C. Fontana, E. C. Raffiotta, Il Mulino, 2022. pp 513 e ss.
- F. DI PORTO, *Opacità algoritmica e trasparenza delle decisioni amministrative*, in *L'amministrazione pubblica con i Big Data: Da Torino un dibattito sull'intelligenza artificiale*, a cura di Roberto Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli studi di Torino;

- L. TORCHIA, *Lo stato digitale una introduzione*, Il Mulino, 2023, pp. 17 e ss.; B. BOSCHETTI, *La transizione della pubblica amministrazione*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli con prefazione di M. Clarich, Giappichelli, 2022, p. 3 e ss.
- F. CARDARELLI, *Le banche dati pubbliche: una definizione*, in *Il diritto dell'informatica*, 2022, volume 18, p.321 e ss.
- A. SORO, *Dati e democrazia*, in *Il ruolo del garante per la protezione dei dati personali, La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. CERRINA FERONI, 2024. p 94 e ss.
- S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021; L. TORCHIA, *Lo Stato digitale e i nuovi stati digitali*, in *Lo Stato digitale una introduzione*, Il Mulino Itinerari, 2023.
- S. TOSCHEI, *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*, in *Innovazione tecnologica e valore della persona*, L. CALIFANO E C. COLAPIETRO, Editoriale scientifica, p.433 e ss, 2020.
- R. CAVALLO PERIN, *Pubblica amministrazione e data analysis*, in *L'amministrazione pubblica con i Big Data: Da Torino un dibattito sull'intelligenza artificiale*, a cura di Roberto Cavallo Perin, Università di Torino, 2021.
- P. CANAPARO, *La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni*, in *Federalismi.it*, 2020.
- A. CORRADO, *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018.
- M. DELMASTRO – A. NICITA, *Big Data, come stanno cambiando il nostro mondo*, Bologna, Il Mulino, 2019;
- G. PASCUZZI, *Big Data*, in *Il diritto dell'era digitale*, Il mulino, p.265 e ss, 2020;

- R. KITCHIN, G. MCARDLE, *What Makes Big Data? Exploring the Ontological Characteristics of 26 Datasets*, in *Big Data & Society*, 1, 2016, p. 1 ss;
- V. MAYER-SCHONBERGER, K.N. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, trad. it. a cura di R. Merlini, Garzanti, Milano, 2013;
- S. LEONELLI, *La ricerca scientifica nell'era dei Big Data*, Meltemi, Milano, 2018;
- A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 1, 2012;
- R. MORO VISCONTI, *Valutazione dei Big data e impatto su innovazione e digital branding*, in *Il Diritto industriale*, 1, 2016;
- J. SHKABATUR, *The Global Commons of Data*, in *Stanford Technology Law Review*, 22, 2019; G. AZZONE – F. CAIO, *In un mare di dati. Quali dati per le politiche, quali politiche per i dati*, Milano, Mondadori, 2020.
- P. FALLETTA, *La riforma delle amministrazioni pubbliche, tra piattaforme interoperabili e atti amministrativi digitali*, in *Federalismi.it*, 27 dicembre 2023.
- V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2019, p. 32.
- G. CARULLO, *Dati, banche dati, blockchain e interoperabilità dei sistemi informatici*, in *Il diritto dell'amministrazione pubblica digitale*, a cura di R. Cavallo Perin – D. U. Galetta, Giappichelli Editore, Torino, 2020 p. 197 e ss.
- G. RACCA, *La digitalizzazione dei contratti pubblici: adeguatezza delle pubbliche amministrazioni e qualificazione delle imprese*, in *Il diritto dell'amministrazione pubblica digitale*, a cura di R. Cavallo Perin – D. U. Galetta, Giappichelli Editore, Torino, 2020 p. 321 e ss; G. PASCUZZI, *Big Data*, in *Il diritto dell'era digitale*, Il mulino, p.265 e ss, 2020.
- U. PAGALLO, *Big data open data e black box society*, in *L'amministrazione pubblica con i big data: da Torino un dibattito*

sull'intelligenza artificiale, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, p. 49 e ss, Università degli studi di Torino, 2021.

- A. CORRADO, *Il principio di trasparenza*, in M. A SANDULLI, (a cura di), *Principi e regole dell'azione amministrativa*, Giuffrè Editore, Milano, 2023;
- A. CORRADO *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, Jovene, 2018;
- M.R. SPASIANO, *I principi di pubblicità. Trasparenza e imparzialità, in Codice dell'azione amministrativa*, (a cura di) M. A. SANDULLI, Milano, 2017;
- C. COLAPIETRO – A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in *Le nuove frontiere della trasparenza nella dimensione costituzionale*, a cura di C. COLAPIETRO – L. CALIFANO, Editoriale Scientifica, Napoli, 2014, pp. 117 e ss;
- M. A . SANDULLI, *Voce Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, IV aggiorn., Milano, 2000;
- V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte Costituzionale (n. 20/2019)*, in *federalismi.it*, n. 5, 2020;
- P. CANAPARO, *La via italiana della trasparenza pubblica: il diritto di informazione indifferenziato e il ruolo proattivo delle Pubbliche amministrazioni*, in *Federalismi.it*, 2014;
- A. SIMONATI, *La ricerca in materia di trasparenza amministrativa: stato dell'arte e prospettive future*, in *Dir. amm.*, 2018.
- E. CARLONI, *Qualità dei dati, big data e amministrazione pubblica*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino;
- E. CARLONI, *v*, in B. Ponti (a cura di), *il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, Rimini, 2008.

- S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino, 1973;
- L. CALIFANO – C. COLAPIETRO, *Innovazione tecnologica e valore della persona, il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, 2017.
- B. PONTI, *L'amministrazione come fornitore e come fruitore di dati personali pubblici: sono praticabili soluzioni basate sulla Big Data Analytics/machine learning?* In *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino, p. 117 e ss.
- M. INTERLANDI – L. TOMASSI, *La decisione amministrativa algoritmica*, in *Approfondimenti di diritto amministrativo*, a cura di A. Contieri, 2020, Editoriale scientifica, Napoli;
- A. CORRADO, *Discrezionalità algoritmica e sindacato del giudice amministrativo*, in *Intelligenza Artificiale per la pubblica amministrazione Principi e regole del procedimento amministrativo algoritmico* a cura di E. Belisario e G. Cassano, Pacini Giuridica, 2023, p. 173 e ss.
- D.U. GALETTA, *I principi di proporzionalità e ragionevolezza*, in *Principi e regole dell'azione amministrativa*, a cura di M.A Sandulli coordinato da F. Aperio Bella, Quarta Edizione, 2023, p. 169 e ss.
- B. BOSCHETTI, *La transizione della pubblica amministrazione*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. Lalli, con prefazione di A. Clarich, Giappichelli Editore, Torino, 2022, p.3 e ss;
- A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, Il Mulino, Bologna 1971;
- L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro Amministrativo*, II, 2018, p. 9.
- D. SORACE, *Diritto delle amministrazioni pubbliche. Una introduzione*, Il Mulino, Bologna, 2014;

- F. MARTINES, *La digitalizzazione della pubblica amministrazione*, in *Rivista di diritto dei media*, 2018, p. 2.;
- A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513;
- M. CLARICH, *Prefazione*, in A. Lalli, *La pubblica amministrazione nell'era digitale*, Torino, Giappichelli, 2022, XIV.
- D. SORACE, *Diritto delle amministrazioni pubbliche. Una introduzione*, Il Mulino, Bologna, 2014;
- F. MARTINES, *La digitalizzazione della pubblica amministrazione*, in *Rivista di diritto dei media*, 2018, p. 2.;
- A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513;
- M. CLARICH, *Prefazione*, in A. Lalli, *La pubblica amministrazione nell'era digitale*, Torino, Giappichelli, 2022, XIV.
- S. ROSSA, *La dimensione verticale della Cybersicurezza pubblica fra Unione Europea e Ordinamento nazionale in Cybersicurezza e pubblica amministrazione*, Editoriale scientifica Napoli, 2023, p. 65;
- M. ALDINUCCI, *L'infrastruttura necessaria per creare interoperabilità tra pubbliche amministrazioni*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'Intelligenza Artificiale*, a cura di R. Cavallo Perin, con il coordinamento editoriale di Isabella Alberti, Università degli Studi di Torino, 2021;
- A. SCOGNAMIGLIO, *Diritto di accesso e banche dati pubbliche*, in *Foro amministrativo c.d.s.*, 2005,2, p.492.;
- L. FLORIDI, *La Rivoluzione dell'informazione*, Turin, Codice Edizioni, 2012.
- F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.*, 2/2015, 227;

- D. BOLOGNINO-A.CORRADO-A.STORTO, *Digitalizzazione e pubblica amministrazione*, in *Il diritto dell'era digitale*, edito da R.GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milan, 2022, p. 625.
- G. CERRINA FERONI – C. FONTANA – E. C. RAFFIOTTA, *Ai Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, 2022, p. 9 e ss.
- B. CAROTTI, *Il settore pubblico e il cloud computing*, in *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, a cura di V. Bontempi, Roma, Roma tre press, 2022, p. 147
- B. CAROTTI, *Il sistema di governo di internet*, Milano, Giuffrè, 2016; A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi pubblici "online". Lineamenti del disegno normativo*, in *Diritto Pubblico*, no. 1/2019, 124 e ss.
- G. ITALIANO, *La protezione dei dati nel cloud nazionale*, in *Il ruolo del Garante per la protezione dei dati personali – la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. Cerrina Feroni, Il Mulino, 2023, p. 97 e ss.
- A. SORO, *Dati e democrazia*, in *Il ruolo del Garante per la protezione dei dati personali – la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. Cerrina Feroni, Il Mulino, 2023, p. 97 e ss.;
- B. CAROTTI, *Il settore pubblico e il cloud computing*, in *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, a cura di V. Bontempi, Roma, Roma tre press, 2022, p. 147 e ss.
- G. NAPOLITANO, *Il partenariato public-privato per l'implementazione del Polo Strategico Nazionale* in *Giorn. Dir. Amm.*, 6/2021, 703-707.
- A. SANDULLI, *Pubblico e Privato nelle Infrastrutture nazionali digitali strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 513

- V. DONATIVI, *Le società a partecipazione pubblica*, Milan, 2016;  
*Codice delle Società a partecipazione pubblica*, editore by G. MORBIDELLI, MILANO, 2018;
- A. NATALINI, *Come il passato influenza la digitalizzazione della pubblica Amministrazione*, in *Riv. trim. dir. pubbl.*, no. 1, 2022, 95
- V. MONTANI, *Il project financing inquadramento giuridico e logiche manutentive*, Giappichelli Editore Torino, 2018;
- B. MARCHETTI, Voce *Amministrazione Digitale*, in *Enciclopedia del Diritto*, Milan, 2022, 76.
- V. CAMPANILE, *Art. 19*, Codice dei Contratti Pubblici by C. CONTESSA - P. DEL VECCHIO, Napoli, 2023.;
- P. CLARIZIA, *E-procurement*, in *The Digital State in the National Recovery and Resilience Plan*, Roma, 2022, 109;
- F. COSTANTINO, *L'uso della telematica nella pubblica amministrazione*, in *L'azione amministrativa* a cura di A. ROMANO, Torino, Giappichelli, 2016, 242;
- G. CARLOTTI, *I principi nel codice dei contratti pubblici: digitalizzazione*, in *giustizia-amministrativa.it*, 2023, 6.
- F. TRIMARCHI BANFI, *Il diritto ad una buona amministrazione*, in M.P. CHITI, G. GRECO, *Trattato di diritto amministrativo europeo. Parte generale*, Tomo I, Milan, 2007, 49;
- S. CIVITARESE MATTEUCCI, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubbl.*, 2019, p. 16;
- Y.N. HARARI, *Homo Deus, breve storia del futuro*, Milano, Bompiani, 2018.

- B. BOSCHETTI, *La transizione della pubblica amministrazione verso il modello Government as a platform*, in *L'amministrazione pubblica nell'era digitale*, a cura di A. LALLI, Torino, 2022, p. 37.
- M. SORICE, *La piattaformizzazione della sfera pubblica*, in *Comunicazione Politica*, 2020, n. 3, p. 371.
- G. RESTA, *Poteri privati e regolazione*, in *Enciclopedia del Diritto*, 2023, § 9.
- L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023, *passim*.
- D.U. GALETTA, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedurali nei confronti della Pubblica Amministrazione*, in *RIDPC*, 2005/3, p. 819 ss.
- F. COSTANTINO, *Gli open data come strumento di legittimazione delle istituzioni pubbliche?*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di R. CAVALLO PERIN, Torino, 2021, p. 160.
- P. STANZIONE, *Conclusioni a tutela della persona*, in *Il ruolo del Garante per la protezione dei dati personali. La tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di G. CERRINA FERONI, Bologna, 2023, p. 285.
- L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppo, opportunità, sfide*, Raffaello Cortina Editore, 2022, 279.





