UNIVERSITÀ
DEGLI STUDI
FIRENZE

DOTTORATO DI RICERCA IN

SCIENZE GIURIDICHE

CICLO XXXV

LA DATA GOVERNANCE NEL SETTORE PUBBLICO. IL MODELLO DEGLI ECOSISTEMI DIGITALI URBANI

Settore Scientifico Disciplinare IUS/08

A.A.2021/2022

Dottoranda

Dott.ssa Valentina Pagnanelli

Supervisore

Prof. Andrea Simoncini

Coordinatore

Prof. Alessandro Simoni

SOMMARIO

TAVOLA DELLE SIGLE

ACN	*Agenzia per la Cybersicurezza Nazionale*
AgID	*Agenzia per l'Italia Digitale*
AI	*Artificial Intelligence*
AIA	*Artificial Intelligence Act*
CAD	*Codice dell'Amministrazione Digitale*
CE	*Commissione europea*
DGA	*Data Governance Act*
DPIA	*Data Protection Impact Assessment*
DPO	*Data Protection Officer*
EDPB	*European Data Protection Board*
EDPS	*European Data Protection Supervisor*
ENISA	*European Union Agency for Cybersecurity*
FFD	*Free Flow Data (Regulation)*
FOIA	*Freedom of Information Act*
GDPR	*General Data Protection Regulation*
IA	*Intelligenza artificiale*
ICT	*Information and Communication Technology*
ITED	*(Direzione) Innovazione Tecnologica E Digitale*
NIS	*Network and Information Security (Directive)*
PA	*Pubblica Amministrazione / Pubbliche Amministrazioni*

PDND	*Piattaforma Digitale Nazionale Dati*
PNRR	*Piano Nazionale di Ripresa e Resilienza*
PTI	*Piano Triennale per l'Informatica (nella Pubblica Amministrazione)*
TFUE	*Trattato sul funzionamento dell'Unione europea*
TUE	*Trattato sull'Unione europea*
TUEL	*Testo unico degli Enti locali*
UE	*Unione europea*
WP29	*Working Party (Article) 29*

PREMESSA

Genesi della ricerca.

Il percorso di ricerca di cui questo elaborato restituisce i risultati si è sviluppato nell'ambito di una convenzione tra la Città metropolitana di Firenze ed il Dipartimento di Scienze Giuridiche dell'Università di Firenze per il finanziamento di una borsa di ricerca dal titolo "*Modelli di attuazione del Regolamento europeo in materia di tutela dei dati personali*". La convenzione prevedeva che il Dipartimento di Scienze Giuridiche fornisse supporto nell'interpretazione e armonizzazione delle disposizioni di legge nazionali e delle fonti subordinate, anche interne all'amministrazione, con le previsioni normative europee, specialmente in materia di dati; al contempo l'ente locale si impegnava ad offrire agli studiosi l'opportunità di affrontare "sul campo" le questioni applicative giuridicamente più complesse.

Il progetto si è poi concretizzato attraverso una stretta e proficua collaborazione tra l'Ufficio del *Data Protection Officer* della Città metropolitana di Firenze e la scrivente, in qualità di assegnataria della borsa di ricerca co-finanziata. Grazie alla ulteriore convenzione stipulata tra la Città metropolitana ed il Comune di Firenze, con la quale i due enti hanno deciso di condividere la figura del Responsabile per la Protezione dei dati personali, la sottoscritta ha potuto estendere l'ambito della ricerca, comprendendovi le due dimensioni amministrative, comunale e di area vasta.

L'aumento costante, durante il triennio dottorale, della produzione e dell'utilizzo di *Big Data* anche negli enti locali, insieme alla crescente valorizzazione degli stessi attraverso i sistemi di Intelligenza artificiale, ha reso necessario ampliare ulteriormente la ricerca estendendo l'analisi del modello di applicazione del GDPR negli enti locali ad un modello di *governance* dei dati *tout-court*.

L'ente locale digitalizzato, in cui vengono costantemente prodotti, raccolti ed elaborati dati personali e non personali che, attraverso l'impiego di sistemi di Intelligenza artificiale consentono all'amministrazione di elaborare politiche e fornire servizi ai cittadini, diviene così una "città intelligente".

L’ultima fase della ricerca si è svolta, ancora una volta “sul campo”. Infatti ho avuto la possibilità di analizzare i modelli di governo dei dati, nonché le principali problematiche ad essi connesse, nelle *Smart cities* di Firenze e Milano.

INTRODUZIONE

Il metodo di ricerca

La rilettura del diritto in chiave digitale è una grande sfida, che pure necessita di essere affrontata in quanto non si tratta di una speculazione dottrinale ma piuttosto della esigenza per lo Stato di dotarsi di strumenti giuridici che abbiano presa su di una realtà in cui i fenomeni si evolvono con grande velocità e in maniera liquida (come in più circostanze evidenziato da Bauman[1]).

L'occhio del giurista non può soffermarsi esclusivamente alla componente descrittiva di quella realtà, ma deve piuttosto cercare di ricondurre i fenomeni umani, anche innovativi, entro il contesto dei principi e delle regole del diritto, nella cornice costituzionale che regola il corretto svolgimento della vita democratica di una comunità (locale, nazionale, sovranazionale, internazionale)[2].

Lo studio che segue reca le conclusioni di una ricerca che, nella vastità e complessità del panorama appena tratteggiato, ha preso in esame un particolare ambito della società digitale[3], il settore pubblico. Oggetto di analisi sono stati, come anticipato, gli enti locali, Comuni e Città metropolitane. Il percorso di ricerca ha preso avvio con l'entrata in vigore, nell'Unione europea del Regolamento europeo n. 2016/679 (*General Data Protection Regulation*). L'inserimento di un *corpus* normativo organico, recante penetranti requisiti di *compliance*, entro apparati rigidamente organizzati e soggetti a stringenti vincoli normativi quali sono gli enti locali, ha fatto emergere numerose questioni di sicuro rilievo giuridico, derivanti in primo luogo dalla apparente contrapposizione tra il principio di *accountability*, introdotto dal nuovo regolamento sui dati personali, e il principio di legalità.

Il percorso che ha visto la progressiva elaborazione di un modello di applicazione del GDPR nella Città metropolitana di Firenze mi ha fornito importanti indicazioni per proseguire la

[1] Z. BAUMAN, *Modernità liquida*, Laterza, Roma-Bari, 2010.

[2] A. SIMONCINI, *Sovranità e potere nell'era digitale*, in *Diritti e libertà in internet*, a cura di E.T. FROSINI, O. POLLICINO, E. APA, M. BASSINI, Le Monnier Università, Firenze, 2017, p. 19-38.

[3] F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefebvre, Milano, 2019.

ricerca. In primo luogo, l'analisi di questioni legate alla corretta applicazione della normativa in materia di dati personali all'interno degli enti locali ha imposto di esaminare norme che sono applicate a tutto il settore pubblico; sì che dal particolare è stato possibile giungere a considerazioni valide anche per altre Pubbliche Amministrazioni, e non solamente per il caso di studio specifico. In secondo luogo, dall'osservazione della attività di adeguamento della Città metropolitana di Firenze al GDPR ho tratto importanti indicazioni di carattere metodologico. Infatti lo studio approfondito della normativa in materia di dati personali e la sua applicazione nella *governance* dei dati personali della Città metropolitana ha consentito a chi scrive di definire e applicare all'intera ricerca uno specifico metodo, basato sulla analisi dei flussi di dati e sulla regolazione giuridica degli stessi.

Nel *mare magnum* dei fenomeni tecnologici, sociali, politici che caratterizzano la Quarta rivoluzione[4] il metodo di ricerca *data-driven* mi ha consentito di procedere gradualmente nella analisi dei fenomeni e delle normative, mantenendo il *focus* sui flussi di dati[5]. Questa metodologia mi ha consentito di esaminare i flussi di dati all'interno delle Città intelligenti descrivendo le stesse come "Ecosistemi digitali urbani" dei quali analizzare limiti e possibilità di sviluppo.

Non vi è dubbio che attraverso l'utilizzo dei sistemi di Intelligenza artificiale e dei *Big Data* gli enti locali possano progettare servizi ed elaborare politiche volte al miglioramento della qualità della vita dei cittadini, nel pieno rispetto dei loro diritti e delle loro libertà. Come il presente studio ambisce ad evidenziare, una coerente e solida disciplina dei dati costituirebbe un valido presupposto per garantire al contempo il legittimo utilizzo dell'*asset* informativo pubblico e il rispetto di tutte le regole giuridiche che incidono su di esso.

Il lavoro di ricerca che segue è volto ad individuare, attraverso successive approssimazioni, le caratteristiche del modello di *data governance* degli enti locali, adottati come caso di studio per individuare caratteristiche estendibili in termini generali al settore pubblico. Il percorso proposto, caratterizzato da una alternanza tra riflessioni teoriche e analisi

[4] L. FLORIDI, *La quarta rivoluzione*. *Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017.

[5] Per questa ragione, riferimenti a normative ed aspetti della *data society* e della *data economy* che abbiano un oggetto differente saranno presenti nell'elaborato solamente ove essi rilevino nella disciplina dei dati (del settore pubblico).

di esempi pratici, muove dal concetto di *data management*, inteso come insieme delle regole organizzative e delle *policies* che consentono il corretto fluire dei dati all'interno di una organizzazione, attraverso i differenti livelli e le possibili ramificazioni della stessa[6] . Alla individuazione del concetto di *data management* seguirà l'analisi del modello di *data governance*, inteso come assetto delle relazioni tra i diversi attori di un ecosistema digitale le cui regole di funzionamento sono il risultato di interazioni, cooperazione e negoziazioni orizzontali tra i diversi *stakeholders* (amministrazione pubblica, attori privati, società civile, accademia…), piuttosto che l'esclusiva applicazione del dettato normativo statale[7]. Si cercherà, in altri termini, di indagare dapprima quanto l'innovazione tecnologica abbia inciso sugli assetti organizzativi del settore pubblico, secondariamente quanto questi assetti abbiano modificato la modalità di interazione tra la PA e gli attori della società civile.

A valle dell'analisi del caso di studio dell'Ecosistema digitale urbano del Comune di Milano, si accederà alla definizione di un modello di *data governance* da cui sia possibile evincere l'assetto dei rapporti di potere tra gli attori in gioco. Proprio attraverso l'osservazione dei flussi di dati, alla luce delle regole giuridiche che ne delineano le dinamiche principali, sarà infatti possibile cogliere «*the power relations between all the actors affected by, or having an effect on, the way data is accessed, controlled, shared and used, the various socio-technical arrangements set in place to generate value from data and how such value is redistributed between actors*[8]*».*

Nelle pagine conclusive si tenterà di comprendere se attraverso l'analisi dei modelli di *data governance* nel settore pubblico sia possibile osservare e descrivere i nuovi rapporti di potere che si delineano nella società digitale e se il governo, consapevole e organizzato, dei flussi di dati possa costituire uno strumento in mano alle istituzioni pubbliche per assorbire l'impatto dell'innovazione e mantenere al centro del proprio agire il perseguimento del benessere e degli interessi della collettività.

[6] Il modello di *data management* descritto vedrà il suo caso di studio nell'analisi del Regolamento privacy della Città metropolitana di Firenze

[7] Ved. M. MICHELI, M. PONTI, M. CRAGLIA, A. BERTI SUMAN, *Emerging models of data governance in the age of datification*, in Big Data & Society, July-December: 1-15, 2020, p. 2.

[8] *Ivi*, p. 3.

CAPITOLO 1 – L'IMPATTO DEI BIG DATA NELLA PUBBLICA AMMINISTRAZIONE

1.1 Big Data e Big Data Analytics. Un nuovo paradigma

Viviamo in un'epoca in cui l'innovazione tecnologica muove a velocità fino a qualche anno fa inimmaginabili, imprimendo alla società cambiamenti epocali[1] e ponendo questioni etiche di non poco conto[2]. I progressi nel campo dell'Intelligenza artificiale consentono di sperimentare quasi quotidianamente nuove possibilità di utilizzo degli algoritmi per svolgere in maniera più rapida, meno faticosa e tendenzialmente più efficiente compiti che finora erano riservati alle capacità e alle attitudini umane. Ciò che solo alcuni anni fa era considerato un grande passo in avanti delle prestazioni dei primi *smartphone* (pensiamo ai primi esempi di assistenti vocali) oggi è ampiamente superato da oggetti connessi alla rete internet (*Internet of Things*) capaci di interagire con l'utilizzatore e di modificare il proprio agire in base alle richieste dello stesso o a elementi che il *software* elabora per individuare la risposta / il comportamento migliore da restituire all'utente in una determinata circostanza.

La caratteristica distintiva della rivoluzione digitale che stiamo vivendo è rappresentata dal ruolo centrale dei *Big Data*: persone fisiche, oggetti, reti, infrastrutture, elaboratori producono quotidianamente enormi quantità di dati che costituiscono la versione *datificata* di

[1] «*Digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate and relate with each other. Digital communication, social media interaction, e-commerce, and digital enterprises are steadly transforming our world. They are generating an even-increasing amount of data, which, if pooled and used, can lead to a completely new means and levels of value creation. It is a transformation as fundamental as that caused by the industrial revolution*», cfr. European Commission, *Communication: Shaping Europe's digital future*, 19 febbraio 2020.

[2] L. D'AVACK, *La rivoluzione tecnologica e la nuova era digitale: problemi etici*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 3 ss.; G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, ivi, p. 63 ss.. Si vedano anche gli *Orientamenti etici per un'IA affidabile*, elaborati dal Gruppo indipendente di esperti ad alto livello sull'Intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018, che indicano l'adesione a principi e valori etici tra le componenti necessarie per rendere un sistema di Intelligenza artificiale affidabile.

ogni aspetto della realtà[3]. Con l'espressione *Big Data* ci si riferisce dunque a un fenomeno tecnologico che rileva prima di tutto da un punto di vista "quantitativo"[4]. I Big Data vengono considerati nella loro globalità (come un insieme molto grande di dati) in ragione dell'impatto che questa mole di dati ha avuto e continua ad avere nella società grazie alle tecniche di analisi a fini predittivi e allo sviluppo di algoritmi di Intelligenza artificiale[5]. Anzi, lo sviluppo di *software* di Intelligenza artificiale sempre più sofisticati è stato agevolato proprio dalla comparsa sulla scena dei *Big Data*: le prestazioni dei due sistemi di *machine-learning* e *deep-learning*, che caratterizzano la maggior parte delle applicazioni dell'IA, sono migliorate grazie alla disponibilità di quantità immense di dati sui quali addestrare i *software*[6].

Una delle più citate definizioni dei *Big Data* si basa sulle c.d. "cinque V": *volume*, *variety*, *velocity*, *veracity*, *value*[7]. Le "V" bene rappresentano l'imponente mole di dati poc'anzi descritta. I *Big Data* sono, appunto, grandi quantità di dati, di varia origine (personali, non personali, industriali, ambientali…), prodotti rapidamente e idonei ad essere trasmessi con tempi di latenza ridotti; sono dati accurati nel loro contenuto informativo e utilizzabili per creare valore a seguito della loro elaborazione[8]. Questo ultimo aspetto è dirimente: infatti i *Big Data* acquistano valore

[3] S. CALZOLAIO, *Protezione dei dati personali*, *aggiornamento*, in *Digesto delle discipline pubblicistiche*, UTET, Torino, 2107, p. 598.

[4] K. CUKIER, V. MAYER-SCHOENBERGER, *The Rise of Big Data: How It's Changing the Way We Think About the World*, in *Foreign Aff.*, 2013, 28, pp. 28-40.

[5] Cfr. MCKINSEY GLOBAL INSTITUTE, *Big data: The next frontier for innovation, competition, and productivity,* http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

[6] Ved. OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, Paris, 2015.

[7] Una successiva definizione si è arricchita delle caratteristiche *Visualization* e *Variability*. Nella Risoluzione del Parlamento europeo sulle implicazioni dei Big Data per i diritti fondamentali si fa riferimento alla «*raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli (analisi dei Big Data)*», cfr. Parlamento europeo, *Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)), "Implicazioni dei Big Data in termini di diritti fondamentali".*

[8] Per una sintesi dei tentativi definitori del fenomeno ved. G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati e Big Data*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019, pp. 454-459.

solamente a seguito delle analisi che vengono effettuate attraverso sistemi algoritmici in grado di estrapolare, gestire e processare le informazioni ivi racchiuse entro un tempo ragionevole[9].

L'analisi dei *Big Data* ha cambiato di fatto la relazione dell'uomo con le informazioni[10]. Attraverso l'applicazione a enormi quantità di dati di tecniche di *data mining* si realizza un salto di paradigma interpretativo della realtà economica e sociale[11]. Infatti nel modello di analisi basato sugli *small-data* per rispondere a una singola domanda occorreva prima formulare un quesito secondo parametri precisi e poi raccogliere dati per rispondervi. Nell'epoca dei *Big Data* i dati vengono invece raccolti a monte e a prescindere da specifici bisogni di conoscenza[12]. Non solo. L'elaborazione di grandi quantità di dati, con mezzi tecnici prima inimmaginabili, consente ora di superare tecniche basate sulla ricerca del nesso di causalità, per sostituirle, grazie agli algoritmi, con l'analisi delle correlazioni dei fenomeni[13].

Le prestazioni degli algoritmi c.d. predittivi, in particolare, non si basano sulla relazione causa-effetto, ma piuttosto su un modello per cui la macchina restituisce risultati, informazioni, azioni, predizioni, come conseguenza di calcoli e correlazioni tra dati che avvengono nella scatola nera, ovvero ad un livello di complessità che rende quasi inaccessibile la logica[14] sottesa agli *output*, persino agli esperti del settore[15].

[9] M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne editrice, Canterano (RM), 2018, p. 151.

[10] Cfr. A. MURRAY, *Information Technology Law. The Law & Society*, Oxford University Press, 2019, pp. 3-21. Per una descrizione efficace dei rischi e delle potenzialità legati alla Big data analytics si veda S. CALZOLAIO, *Protezione dei dati personali*, *aggiornamento*, cit., p. 594 ss.; su *Big Data* e *machine learning*, A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, I, giugno 2019, pp. 87-106.

[11] Autorità per le garanzie nelle comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 2.

[12] M. PALMIRANI, Big Data e conoscenza, in Riv. fil. dir., 2020, 1, pp. 73-92.

[13] *Ibidem*, p. 14; F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Diritto pubblico*, Fascicolo 1, gennaio-aprile 2019, p. 47.

[14] Cfr. gli articoli 13,14,15 del regolamento europeo n. 2016/679.

[15] F. PASQUALE, *The black box society. The Secret Algorithms That Control Money and Information*, Harvard University Press, USA, 2015.

1.2. Il patrimonio informativo digitale della PA

1.2.1 Un quadro d'insieme

La Pubblica Amministrazione italiana, alla pari dei soggetti privati è stata profondamente influenzata dall'evoluzione tecnologica e dal processo di digitalizzazione della società [16], assistendo agli effetti dei profondi cambiamenti poc'anzi delineati e facendosene fruitrice e protagonista. Nell'analisi del fenomeno *Big Data*, il settore pubblico riveste un ruolo centrale, poiché le PA hanno nella propria disponibilità un'ingente mole di dati, ascrivibili alle più eterogenee tipologie [17]. La progressiva digitalizzazione del patrimonio informativo delle pubbliche amministrazioni, che le ha portate a disporre di banche dati costantemente alimentate [18], contenenti quantità straordinarie di informazioni, siano esse dati personali, categorie particolari di dati, o dati non personali[19], colloca infatti le PA tra i principali produttori di *Big Data*.

Lo Stato, come qualsiasi centro di potere, è sempre stato un produttore e un distributore di informazioni e di conoscenze [20], dunque il patrimonio informativo pubblico come tradizionalmente inteso è già di per sé immenso[21] e comprende informazioni di ogni genere[22]. Si

[16] F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022, p. 301; I. MACRÌ, *Digitalizzazione, innovazione e sicurezza nella P.A.*, Wolters Kluwer, Milano, 2022; B. MARCHETTI, *Amministrazione digitale*, in *Enc. dir. (i tematici), III Funzioni amministrative*, Milano, Giuffrè, 2022.

[17] G. CARULLO, *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e mercato*, 23/2016, p. 182.

[18] Basti scorrere l'elenco delle Basi di dati di interesse nazionale, all'art. 60 del Codice dell'Amministrazione Digitale (CAD, d. lgs. n. 82/2005).

[19] Le definizioni di queste categorie sono contenute negli artt. 4 e 9 del regolamento europeo sulla protezione dei dati personali (UE) 2016/679 (*General Data Protection Regulation*) e nell'art. 3 del regolamento europeo sulla libera circolazione dei dati non personali (UE) 2018/1807 (*Free Flow Data Regulation*).

[20] Cfr. A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, cit., p. 70.

[21] «*Le amministrazioni statali e locali hanno accumulato per secoli enormi quantità di informazioni di ogni tipo: fiscali, sociali, immobiliari, geologiche e già prima sapevano come impiegare questi dati per provvedere all'attività di cura concreta dell'interesse pubblico e motivare le loro decisioni*», cfr. F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 302.

[22] Anagrafiche, sanitarie, tributarie, giudiziarie… .

tratta delle informazioni trasmesse dai cittadini, di quelle prodotte dalle PA stesse come risultato della loro attività, delle informazioni ottenute da altre PA, e anche delle informazioni che le PA comunicano a loro volta ai cittadini[23]. Basti pensare alle Basi di dati di interesse nazionale individuate nel Codice dell'Amministrazione Digitale. Vi compaiono ad esempio il casellario giudiziale, il registro delle imprese, gli archivi in materia di immigrazione, l'anagrafe nazionale della popolazione residente[24]. Nell'era della digitalizzazione questa immensa banca dati diviene interconnessa e interoperabile, ponendo in capo all'amministrazione la responsabilità di gestire, ordinare, condividere, elaborare, enormi banche dati, da cui possono essere tratte informazioni in grado di migliorare i servizi offerti o al contrario di compromettere interessi nazionali ed individuali[25].

Infatti a seguito dell'avvento della *Big Data Analytics,* la possibilità di analizzare i dati attraverso gli algoritmi consente oggi di estrarne informazioni utili a predisporre politiche e servizi maggiormente rispondenti ai bisogni[26], in tempo più rapido e possibilmente con meno dispendio di denaro, ma al contempo pone in capo alle istituzioni amministrative nuovi doveri e responsabilità[27]. La più rilevante novità che caratterizza l'impatto della tecnologia nelle amministrazioni pubbliche si rinviene nel fatto che le enormi quantità di dati in loro possesso sono ora sempre più spesso convertite in decisioni grazie all'uso di algoritmi[28].

---

[23] G. PALOMBELLI, *Le informazioni pubbliche come risorsa. Profili comparati*, in F. MERLONI (a cura di), *L'informazione delle pubbliche amministrazioni*, Maggioli, Santarcangelo di Romagna, 2002, p. 233.

[24] Ved. Codice dell'Amministrazione Digitale, art. 60.

[25] Cfr. S. CALZOLAIO, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, 31/2016, p. 198.

[26] F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, cit., p. 46.

[27] «*La organizzazione di banche di dati impone una disciplina adeguata del processo di raccolta, memorizzazione e distribuzione delle informazioni, del loro costo e della loro funzione, delle situazioni di doverosità dei cittadini, relative al reperimento delle informazioni, delle loro situazioni di diritto e di interesse, sotto vari profili: la tutela dei segreti individuali, l'uguaglianza nella raccolta di informazioni, l'accesso alle informazioni raccolte, il loro uso da parte di poteri pubblici competenti e solo per gli scopi per i quali i dati vengono raccolti e la distribuzione di informazioni viene effettuata*», cfr. A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, cit., pp. 69-70.

[28] «*Il dato, dunque, molto significativo per l'amministrazione pubblica, è che, nella prospettiva algoritmica, la tecnologia digitale non viene usata – soltanto – per "redigere" un atto amministrativo, per conservarlo o trasmetterlo, ma viene usata per determinarne il contenuto, ovverosia per "decidere"* », cfr. A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in *Il diritto dell'amministrazione pubblica digitale*, R. CAVALLO PERIN, D.U. GALETTA (a cura di), Giappichelli, Torino, 2020, p. 5; ved. anche F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO,

L'introduzione e l'utilizzo di tecniche sempre più sofisticate di analisi dei dati nell'attività amministrativa ha fatto emergere questioni di legittimità e liceità di tali utilizzi, specie nelle attività decisionali a contenuto discrezionale[29], tema vastissimo che non può essere affrontato in questa sede[30].

Se è vero che fin dalla comparsa dei primi supporti informatici all'interno dell'Amministrazione pubblica ci si è posti la questione di come questi avrebbero influito nell'organizzazione degli apparati, fino a chiedersi se effettivamente la inevitabile variazione delle procedure avrebbe comportato una radicale modifica degli assetti interni oppure se gli stessi avrebbero resistito all'impatto[31], la digitalizzazione e l'amministrazione algoritmica hanno imposto la questione in modo netto, evidenziando lo scarto tra la rigidità degli apparati amministrativi e le esigenze di riorganizzazione collegate alle nuove modalità di svolgimento e di fruizione dell'attività amministrativa "digitalizzata"[32].

Nel contesto attuale la PA deve garantire una organizzazione dei contenuti, oltre che la capacità di condividerli con le altre Pubbliche Amministrazioni, i cittadini e le imprese, secondo procedure e *standard* certi, e garantendo la riservatezza e la sicurezza cibernetica del patrimonio informativo pubblico, e la salvaguardia dei diritti fondamentali che inevitabilmente sono messi a rischio nella elaborazione massiva di dati molto spesso personali[33]. Ciò impone perlomeno la verifica costante della qualità dei dati che vengono raccolti, trattati e conservati, entrando a far parte del patrimonio informativo pubblico, e al contempo la più rigorosa verifica della affidabilità degli algoritmi utilizzati per estrarre valore dai dati e per fornire servizi[34].

P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 303.

[29] Si veda da ultimo l'art. 30 del "*Codice dei contratti pubblici*", d.lgs. 31 marzo 2023, n. 36.

[30] Cfr. 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.it*, 6 febbraio 2019, p. 15 ss; F.F. PAGANO, *Pubblica amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 324 ss.; A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in *Il diritto dell'amministrazione pubblica digitale*, R. CAVALLO PERIN, D.U. GALETTA (a cura di), cit., p. 8 ss.

[31] Per tutti, A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, cit..

[32] V. a tale proposito l'art. 3-bis della legge 7 agosto 1990, n. 241, di cui si parlerà *infra*.

[33] A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, pp. 50-51.

[34] Sul tema della trasparenza algoritmica, e sull'amministrazione algoritmica in particolare si vedano, *ex plurimis*: F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, cit. p. 52 ss.; D.U. GALETTA, J.G. CORVALAN, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, cit.; F. PATRONI

Tutto ciò si sta realizzando gradualmente attraverso un complesso percorso comprendente il rinnovo degli *asset*, la formazione del personale, l'adozione di nuove procedure per la gestione del patrimonio digitale, il rispetto degli obblighi di condivisione e apertura dei dati. Il complesso di azioni appena descritto, nella Pubblica Amministrazione si assomma piuttosto che sostituirsi al sistema organizzativo degli apparati vincolato dal rispetto dei principi e delle regole del diritto amministrativo. Come si vedrà nei prossimi paragrafi, alcune normative di recente approvazione hanno guidato forse più di altre questo difficile percorso di ricalibrazione dell'intera macchina amministrativa, non perché siano rivolte a questo fine ma piuttosto perché le regole ivi contenute indicano una metodologia da seguire per il trattamento dei dati.

GRIFFI, *Intelligenza artificiale: amministrazione e giurisdizione*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., p. 475 ss.; G. ORSONI, E. D'ORLANDO, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del Federalismo*, n. 3, 2019, luglio/settembre, p. 593 ss.

1.2.2 Il percorso di digitalizzazione della PA. Cenni

I primi interventi legislativi in tema di innovazione tecnologica della PA risalgono agli anni Novanta. Con il d. lgs. n. 29/1993 l'informatizzazione assumeva un ruolo strategico nell'incremento dell'efficienza della PA[35]. Poi, con la legge n. 59/1997 si è rafforzato l'utilizzo della tecnologia nella Pubblica amministrazione, quale strumento per migliorare il dialogo con i cittadini e per semplificare la fruizione dei servizi. Nel 2000 entrava in vigore il Testo Unico sulla documentazione amministrativa (d.P.R. n. 445/2000).

Nel 2005 la legge 11 febbraio 2005 n. 15 modificava la legge 241/1990 sul procedimento amministrativo [36] introducendo l'art. 3-*bis*, a mente del quale «*per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica*[37]*, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*». Nello stesso anno, tale previsione trovava attuazione con il Codice dell'Amministrazione Digitale (CAD), adottato con d. lgs. 7 marzo 2005, n. 82 e modificato più volte[38]. Proprio il CAD ha rappresentato un momento di svolta nell'evoluzione normativa in materia, recando una disciplina organica dell'applicazione delle tecnologie informatiche nella Pubblica amministrazione e nel rapporto tra l'amministrazione e gli amministrati[39]. Il CAD mirava a semplificare i rapporti tra cittadini e Pubblica Amministrazione, oltre che le attività dell'amministrazione stessa, utilizzando gli strumenti della *Information and Communication Technology*, così stabilendo un vero e proprio

[35] D. DE GRAZIA, *Informatizzazione e semplificazione dell'attività amministrativa nel "nuovo" codice dell'amministrazione digitale*, in *Diritto pubblico*, Fascicolo 2, maggio-agosto 2011, p. 614.

[36] Ved. P. BURLA, G. FRACCASTORO, *Il diritto di accesso ai documenti della Pubblica amministrazione*, Laurus Robuffo, Roma, 2006.

[37] «*L'introduzione delle tecnologie informatiche nella vita quotidiana delle pubbliche amministrazioni è il frutto di una scelta relativamente recente dei legislatori nazionali. La svolta nel perseguimento di questa strategia è seguita all'avvento della telematica, ovvero dell'insieme delle tecnologie di trasmissione delle informazioni digitali, che ha segnato il passaggio da una informatizzazione finalizzata alla mera gestione interna dei dati e dei procedimenti da parte di ciascuna amministrazione alla possibilità di scambiare informazioni ed impostare così un proficuo "dialogo elettronico interattivo tra amministrazioni e tra queste e i privati"*», cfr. D. DE GRAZIA, *Informatizzazione e semplificazione dell'attività amministrativa nel "nuovo" codice dell'amministrazione digitale*, cit., p. 613.

[38] Da ultimo con il decreto-legge 16 luglio 2020, n. 76 (decreto semplificazioni) e il decreto-legge 31 maggio 2021, n. 77 convertito con modificazioni dalla legge 29 luglio 2021, n. 108

[39] F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 304.

"*diritto all'uso delle tecnologie*"[40]. Il CAD racchiude infatti i principi - cardine della digitalizzazione della PA, oltre a un vero e proprio statuto dei diritti digitali dei cittadini.

Nel 2012, con il decreto-legge 22 giugno 2012 n. 83, convertito con modificazioni dalla legge 7 agosto 2012, n. 134 è stata istituita l'Agenzia per l'Italia Digitale, con il compito di promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione, anche attraverso la definizione di *standard*, l'elaborazione di regole tecniche e il coordinamento informatico dei progetti inseriti nell'Agenda Digitale italiana.

Alcune normative hanno inciso più di altre nel percorso di digitalizzazione della PA e nell'accrescimento del patrimonio informativo digitale, facendo sì che la PA assumesse via via «*la responsabilità di gestire, trattare, condividere, elaborare, "archivi digitali" immensi*[41]*»*; basti pensare decreto-legge n. 179/2012, che ha portato alla progressiva creazione tra gli altri dell'"Anagrafe nazionale della popolazione residente", del "fascicolo elettronico dello studente", del "fascicolo sanitario elettronico" (istituito dalla Regioni e province autonome)[42]. Vanno ricordate, poi, anche le fonti aventi ad oggetto la trasparenza amministrativa, tra le quali assume particolare rilievo il d. lgs. 14 marzo 2013, n. 33.

[40] «*Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2 comma 2, anche ai dini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute*», art. 3 del CAD; ved. A. SIMONCINI, *Profili costituzionali dell'amministrazione algoritmica*, in *Rivista Trimestrale di Diritto Pubblico*, n. 4/2019, p. 1149 ss.

[41] S. CALZOLAIO, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, cit., p. 198.

[42] Il decreto-legge 31 maggio 2021, n. 77, recante governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure ha da ultimo istituito l'Anagrafe nazionale dell'istruzione e l'Anagrafe nazionale dell'istruzione superiore (Artt. 62-quater e 62-quinquies del CAD).

1.2.3 La *disclosure* del patrimonio informativo pubblico: Trasparenza amministrativa e politiche di *Open data*

Come ricordato poc'anzi, anche gli obblighi di trasparenza amministrativa [43] e l'accresciuta attenzione alla filosofia *Open data* [44] hanno costituito dei propulsori per l'accrescimento organizzato del patrimonio informativo della PA, contribuendo in modo significativo ad aumentare il volume dei dati che possono essere correlati e che rappresentano un fattore di "*disclosure* globale"[45] di informazioni[46].

La Costituzione italiana com'è noto non contiene un riferimento esplicito alla trasparenza amministrativa, che viene però riconosciuta quale principio costituzionalmente "implicito"[47]. La trasparenza, da cui discende il diritto di conoscere i dati, le informazioni e i

[43] Ved. L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014; G. ARENA, *Trasparenza amministrativa*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Vol. VI, Giuffrè, Milano, 2006, p. 5947 ss.; L. CALIFANO, *Trasparenza e privacy nell'evoluzione dell'ordinamento costituzionale*, in Giornale di Storia costituzionale, 31/2016; C. COLAPIETRO, *La "terza generazione" della trasparenza amministrativa. Dall'accesso documentale, all'accesso generalizzato, passando per l'accesso civico*, Editoriale scientifica, Napoli, 2016; F. PATRONI GRIFFI, *La trasparenza della Pubblica amministrazione tra accessibilità totale e riservatezza*, in *federalismi.it*, n. 8/2013 p. 1 ss.; B. PONTI (a cura di), *La trasparenza amministrativa dopo il d. lgs. 14 marzo 2013 n. 33. Analisi della normativa, impatti organizzativi ed indicazioni operative*, Maggioli, Santarcangelo di Romagna, 2013; C. COLAPIETRO, A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, cit., p. 117 ss.; D. DONATI, *Il principio di trasparenza in Costituzione*, in F. MERLONI (a cura di), *La trasparenza amministrativa*, Giuffrè, Milano, 2008, p. 123 ss.

[44] Ved. G. CARULLO, *Dati, banche dati, Blockchain e interoperabilità nei sistemi informatici del settore pubblico*, cit. p. 196 ss.; V. PAGNANELLI, *Accesso, accessibilità, Open data. Il modello italiano di Open data pubblico nel contesto europeo*, in Giornale di storia costituzionale, n. 31/2016, p. 205 ss.; F. FAINI, *Data Society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefevbre, Milano, 2019, pp. 117-159.

[45] S. CALZOLAIO, *Protezione dei dati personali*, *aggiornamento*, cit., p. 601.

[46] «*La pubblicità dei dati (Open Data) e la loro riutilizzazione ed elaborazione attraverso sistemi informatici capaci di automatizzare la loro raccolta e catalogazione può dar vita a un imprevedibile sviluppo di nuovi servizi basati su modi innovativi di combinare tali informazioni tra loro e di usarli*», cfr. A MASUCCI, *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, cit. p. 126.

[47] Nelle parole di Carlo Colapietro la trasparenza è un principio costituzionale *immanente* nell'ordinamento, fondato in primo luogo sull'interpretazione sistematica dei principi fondamentali della nostra forma di Stato (democrazia, rappresentanza, eguaglianza, imparzialità), dei quali essa costituisce il presupposto logico imprescindibile, cfr. C. COLAPIETRO, *Trasparenza e democrazia: conoscenza e/è potere*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, cit., p. 16.

documenti in possesso delle Pubbliche Amministrazioni, costituisce un presupposto e un principio la cui attuazione è necessaria per veder realizzati gli altri principi fondamentali, primo fra tutti il principio democratico, il quale prevede, per dirsi realizzato, la piena e consapevole partecipazione dei cittadini alla vita economica, sociale, politica del Paese[48].

La normativa che ha riguardato l'informatizzazione e poi la digitalizzazione dell'attività amministrativa è stata agevolata dall'introduzione delle disposizioni aventi a tema la trasparenza amministrativa che, è stato notato, per gli obblighi in essa contenuti – primo fra tutti l'utilizzo dei canali *web* per la pubblicazione delle informazioni ha costituito un vero e proprio catalizzatore del processo di digitalizzazione[49].

Oggi la mole di informazioni digitalizzate gestite dalla PA è arricchita dai dati forniti in ossequio agli obblighi di pubblicazione, alle regole di accessibilità totale e di riutilizzo[50]. Da esso discende dunque naturalmente il diritto in capo ai singoli cittadini di accedere alla maggiore quantità di informazioni possibili, nel rispetto dei segreti e dei diritti di riservatezza. Queste attività impongono alle pubbliche amministrazioni di svolgere una costante opera di valutazione e bilanciamento che riguarda in particolare il diritto alla protezione dei dati personali dei soggetti i cui dati sono di volta in volta coinvolti[51].

[48] Si veda, sulla precettività dell'obbligo di *open data* come corollario del principio di trasparenza garantito dall'art. 97 della Costituzione, G. DE MINICO, *Gli open data: una politica costituzionalmente necessaria?*, in *Forumcostituzionale.it*, 2014.

[49] *«[…] deve riconoscersi che l'attuazione del d. lgs. n. 33 del 2013 rappresenta – in primo luogo – un fattore di digitalizzazione delle amministrazioni pubbliche, poiché vincola le medesime a rendere strutturalmente accessibili informazioni attraverso il web*», cfr. S. CALZOLAIO, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, cit., p. 188.

[50] Si veda in proposito F. SCIACCHITANO, *Disciplina e utilizzo degli Open Data in Italia*, in Medialaws 1/2018, p. 281 ss.

[51] Ved. M. VIGGIANO, *I limiti alla pubblicità dell'azione amministrativa per finalità di trasparenza derivanti dalla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, cit., p. 227 ss.

1.2.3.1 Le principali tappe della trasparenza amministrativa in Italia

Il d. lgs. 25 maggio 2016, n. 97 ha introdotto nell'ordinamento italiano l'istituto dell'accesso civico generalizzato, compiendo in qualche modo il passaggio dalla trasparenza all'accessibilità totale. Il percorso che ha condotto alla enunciazione di un diritto di tale estensione può essere ricondotto a tre date fondamentali: 1990, 2013, 2016.

L'accesso, come disciplinato nel 1990 dalla legge sul procedimento amministrativo, corrisponde al diritto di prendere visione ed estrarre copia dei documenti amministrativi. Com'è noto tale diritto è riconosciuto a tutti i soggetti privati portatori di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento per il quale è chiesto l'accesso[52]. L'approvazione della legge sul procedimento amministrativo (legge n. 241 del 1990) è considerata una svolta fondamentale nella democratizzazione dei rapporti tra amministrazione e cittadini in termini di partecipazione e trasparenza, di cui il diritto di accesso alla documentazione amministrativa costituisce una delle più rilevanti manifestazioni[53].

Nel 2013 grazie al Decreto Trasparenza (d. lgs. n. 33 del 2013) questo diritto di accesso "tradizionale" è stato affiancato dall'istituto dell'accesso civico[54]. Il nuovo accesso (civico) attribuisce a chiunque, il diritto di richiedere la pubblicazione di dati, documenti o informazioni la cui ostensione, prevista dalla legge, sia stata omessa[55].

Nel 2016, con la riforma Madia è stato infine introdotto il diritto di chiunque di accedere ai dati e documenti detenuti dalle PA, indipendentemente dalla titolarità di situazioni giuridiche

[52] Cfr. l. n. 241/90, art. 22.

[53] Ved. C. COLAPIETRO, A. IANNUZZI, *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, cit., p. 123.

[54] Ved. R. CIFARELLI, *La trasparenza amministrativa dalla legge n. 241/1990 all'accesso civico: spunti di riflessione*, in *AstridRassegna* n. 16/2014.

[55] La natura del diritto di accesso civico è molto dibattuta in dottrina. Si vedano, ad es. M. MAGRI, *Diritto alla trasparenza e tutela giurisdizionale*, in *Istituzioni del Federalismo*, 2/2013, che sottolinea come in assenza di un obbligo di pubblicazione non sia configurabile alcun *diritto* di accesso civico, e D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *federalismi.it*, marzo 2016, che ne sostiene la natura non di autonomo diritto ma di *sanzione* per il mancato rispetto degli obblighi di pubblicazione.

rilevanti[56]: all'accesso ex legge n. 241/1990 e all'accesso civico si è affiancato un diritto di accesso generalizzato (o universale[57])[58].

Dunque, dopo l'elaborazione di uno strumento ibrido come il diritto di accesso civico, connaturato agli obblighi di pubblicazione enumerati, si passa ad un diritto autonomo e generalizzato di accessibilità, dove sono i limiti ad essere enumerati, mentre l'accessibilità totale diviene regola generale e residuale[59].

Oggi l'articolo 5, comma 3 del decreto n. 33/2013 recita: «*Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis*[60]».

Per quanto attiene nello specifico alla disciplina degli enti locali, il Testo unico degli enti locali [61] prevede all'articolo 10 un diritto di accesso e di informazione dei cittadini particolarmente esteso. La norma stabilisce la regola generale per cui tutti gli atti

[56] Cfr. art. 5 comma 3 del d. lgs. n. 33/2013: «*L'esercizio del diritto di cui ai commi 1 e 2 non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. L'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti e non richiede motivazione*».

[57] Nelle parole dell'allora Presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro, un "*accesso universale*", Cfr. *Audizione del Presidente sullo schema di decreto legislativo correttivo della disciplina in materia di trasparenza della Pubblica Amministrazione*, 6 aprile 2016, docweb n. 4861875.

[58] Cfr. M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, cit., pp. 22-23.

[59] Nelle parole della Corte costituzionale il d.lgs. n. 97 del 2016 costituisce «*il punto d'arrivo del processo evolutivo che ha condotto all'affermazione del principio di trasparenza amministrativa, che consente la conoscenza diffusa delle informazioni e dei dati detenuti dalle pubbliche amministrazioni*», cfr. Corte costituzionale, sentenza n. 20/2019, *Considerato in diritto*, 4.1.

[60] L'art. 5-bis comma 1 elenca gli interessi pubblici (inerenti a: sicurezza pubblica e ordine pubblico, sicurezza nazionale, difesa e questioni militari, relazioni internazionali, politica e stabilità finanziaria ed economica dello Stato, conduzione di indagini sui reati e loro perseguimento, regolare svolgimento di attività ispettive) e privati (protezione dei dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali, compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali) la cui tutela può giustificare una compressione del diritto di accesso.

[61] Su cui si tornerà nel prossimo capitolo.

dell'amministrazione comunale e provinciale sono pubblici[62]. Per via regolamentare debbono poi essere disciplinate le modalità di esercizio del diritto di accesso e viene assicurata l'informazione sull'attività amministrativa.

Nell'ordinamento dell'Unione europea, gli articoli 11, 41 e 42 della Carta di Nizza[63] garantiscono ai cittadini il diritto di ricevere informazioni, così come quello di accedere ai documenti che li riguardano nel corso di procedimenti nei loro confronti, e da ultimo il diritto di accesso ai documenti del Parlamento europeo, del Consiglio e della Commissione[64].

[62] Salvo quelli riservati per indicazione di legge o per temporanea e motivata dichiarazione del sindaco (o del presidente della provincia), a tutela della riservatezza di persone, gruppi o imprese coinvolti.

[63] Consultabile in http://www.europarl.europa.eu/charter/pdf/text_it.pdf

[64] Cfr. R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti: commento alla Carta dei diritti fondamentali dell'Unione europea*, Il Mulino, Bologna, 2001.

1.2.3.2 Oltre la trasparenza. La filosofia *Open data*

Diversa dal concetto di Trasparenza amministrativa è la filosofia *Open data*, che mira ad una apertura dei dati non finalizzata a rispondere ad una richiesta. I dati dovrebbero essere messi a disposizione perché possano essere riutilizzati, anche con modalità e per finalità non prevedibili e non dichiarate a monte. Secondo la definizione contenuta nell'*Open Data Charter* «*Open data is digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere».* Invece secondo la *Open definition* fornita dalla *Open Knowledge*[65] *«Open data and content can be freely used, modified, and shared by anyone for any purpose*[66]*».*

L'articolo 7-*bis*, comma 3 del Decreto Trasparenza, dopo la evoluzione verso il modello FOIA (*Freedom of Information Act*[67]), specifica che le PA possono pubblicare informazioni ulteriori rispetto a quelle la cui pubblicazione è prevista da una norma di legge o di regolamento, dopo aver anonimizzato i dati personali eventualmente presenti. Dunque mentre l'indicazione contenuta nell'articolo 7 riguarda le modalità tecniche di pubblicazione (con l'apposito riferimento al CAD), e al regime giuridico previsto per il loro riutilizzo (riferimento al decreto legislativo n. 36/2006 di attuazione della direttiva (UE) n. 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico e al decreto legislativo n. 196/2003, Codice della *privacy*), nell'articolo 7-*bis* il comma 3 è rivolto ad un ulteriore ampliamento della quota di dati condivisi, la cui estensione è però lasciata alla valutazione dei singoli uffici. La portata innovativa della norma è indebolita perché l'apertura dei dati è lasciata alla iniziativa pubblica o

[65] La *Open Knowledge Foundation* è una organizzazione globale *no profit* nata allo scopo di promuovere la più ampia diffusione della cultura dell'*Open Data*: «*Open Knowledge International is a worldwide non-profit network of people passionate about openness, using advocacy, technology and training to unlock information and enable people to work with it to create and share knowledge*»; cfr. https://okfn.org/about/ .

[66] La versione completa della *Open definition* 2.1 è reperibile al link http://opendefinition.org/od/2.1/en/ .

[67] Per una ricostruzione sulle origini dell'istituto ved. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e Pubblica Amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Riv. Ital. Dir. Pubbl. Comunitario*, 2016; M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, cit., pp. 22-23. Per alcuni esempi di utilizzo sociale degli *Open data*, *ivi*, pp. 42 ss.. Per una riflessione sulla distinzione tra l'istituto del FOIA e la più ampia filosofia *Open Data* sia consentito rinviare a V. PAGNANELLI, *Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, cit., p. 205 ss.

ad una reazione a seguito di una richiesta del cittadino, costretto ad attivarsi per accedere alle informazioni[68].

La necessità di sviluppare le politiche di *Open Data*, in un'ottica di miglioramento dei servizi offerti ai cittadini e quindi della qualità della vita degli stessi era inserita tra gli obiettivi della *Digital Agenda for Europe*, presentata dalla Commissione nel 2010 all'interno della strategia "Europa 2020"[69]. L'Italia si è allineata alle istanze europee con l'istituzione della Cabina di regia per l'attuazione dell'Agenda Digitale italiana[70]. Il decreto-legge n. 179/2012 ha introdotto rilevanti novità in tema di *Open Data*, prima di tutte il principio dell'*Open Data by default*, inserito nell'ordinamento italiano attraverso una modifica dell'art. 52 del CAD, secondo cui ogni documento pubblicato dalle Pubbliche Amministrazioni (in assenza di una licenza a norma del d. lgs. n. 36/2006[71]) si considera rilasciato come dato di tipo aperto[72] con la sola eccezione delle pubblicazioni riguardanti dati personali. La lettera l-bis reca la definizione di formato dei dati di tipo aperto, con la quale si identifica "*un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi".* A codesta definizione segue quella dei dati di tipo aperto (alla lettera l-ter)), resi disponibili gratuitamente[73], in formato di tipo aperto, con una licenza che ne permetta

[68] «*Se il dato detenuto dall'amministrazione appartiene al patrimonio indiviso di una collettività, su di esso il soggetto pubblico non può vantare un titolo proprietario esclusivo perché il dato è della collettività, mentre l'amministrazione ne è semplicemente il custode, peraltro temporaneo. E allora la p.a. non è facoltata, ma obbligata a diffonderlo perché non fa altro che restituire al suo legittimo proprietario quanto già gli appartiene*», così De Minico sull'*Open data* come precipitato diretto dell'art. 97 Cost. in quanto «*se il dovere di trasparenza7 impone all'amministrazione la visibilità dei suoi percorsi decisionali, esso prescriverà anche l'esibizione dei risultati del suo agire pubblico: i dati*», cfr. G. DE MINICO, *Gli open data: una politica "costituzionalmente necessaria?*, in www.forumcostituzionale.it , 12 giugno 2014.

[69] La *Digital Agenda for Europe* è una delle iniziative principali dell'Unione europea per il superamento del *digital divide* e per lo sviluppo della ICT (*Information e Communications Technology*) e la creazione di un mercato unico digitale; per un approfondimento sui contenuti dell'Agenda digitale europea si veda D. IELO, *L'Agenda digitale: dalle parole ai fatti. Sanità, scuola, ricerca, start up, smart city, infrastrutture, appalti, anticorruzione, radiotelevisione*, Giappichelli editore, Torino, 2015, p. 51 ss..

[70] Avvenuta con l'art. 47 del decreto-legge n. 5/2012; cfr. G. MANCOSU, *Trasparenza amministrativa e Open Data: un binomio in fase di rodaggio*, in *federalismi.it*, 17/2012, pp. 15-16; sul contenuto dell'Agenda Digitale italiana si veda R. PISA, *Il digital divide e le iniziative per superarlo*, in *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, F. MARCELLI, P. MARSOCCI, M. PIETRANGELO, (a cura di), Editoriale scientifica, Napoli, 2015.

[71] L'art. 2 comma 1 lett. h) del d. lgs. n. 36/2006 definisce licenza standard per il riutilizzo «*il contratto, o altro strumento negoziale, redatto ove possibile in forma elettronica, nel quale sono definite le modalità di riutilizzo dei documenti delle pubbliche amministrazioni o degli organismi di diritto pubblico*».

[72] A norma dell'art. 1 comma 2 lettere l-bis) e l-ter) del CAD.

[73] O con costi marginali.

l'utilizzo da parte di chiunque, anche per finalità commerciali e in formato disaggregato. In questa ultima definizione e nel citato principio dell'*Open Data by default* proclamato dall'art. 52 sembrano potersi ravvisare gli elementi tipizzanti della filosofia di *Open Data*. Il principio dell'apertura dei dati della PA come impostazione predefinita viene confermato, come poc'anzi ricordato, anche dall'articolo 7 del Decreto Trasparenza, che prevede che i dati e documenti soggetti a pubblicazione obbligatoria non possano essere soggetti ad alcuna licenza che vada oltre l'obbligo di citare la fonte e rispettarne l'integrità[74].

È importante sottolineare la significativa differenza tra i presupposti e le finalità dell'istituto dell'accessibilità totale e gli *Open data*. La normativa cosiddetta FOIA, introdotta con decreto legislativo n. 97 del 2016, disciplina il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria, ma questo può avvenire pur sempre a seguito di una istanza di accesso civico che, seppure non motivata, identifica i dati, le informazioni o i documenti richiesti[75]. Ben diversa la logica *Open data*, che mira invece alla apertura dei dati non finalizzata a rispondere ad una richiesta ma messa a disposizione perché possa essere riutilizzata anche in modalità non prevedibili a monte. Il *Freedom of Information Act* è un atto legislativo interamente dedicato alla disciplina dell'accesso (quindi l'accesso è oggetto e non strumento); l'*Open Data* rappresenta piuttosto una filosofia che, se applicata nei flussi informativi tra pubblico e privato, può permettere di ottenere benefici economici, culturali, sociali (i dataset *aperti* sono infatti pubblicati *in formato leggibile - machine-readable* - e, di conseguenza, possono essere condivisi e riutilizzati) [76].

[74] M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, cit., pp. 30-31.

[75] Ved. d. lgs. n. 33/2013, art. 5.

[76] F. PATRONI GRIFFI, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *federalismi.it*, 16 aprile 2013; L. CALIFANO, *Trasparenza e privacy nell'evoluzione dell'ordinamento costituzionale*, cit., p. 77 ss.

1.3 Coordinate di viaggio: CAD e Piano Triennale per l'Informatica nella PA

1.3.1 Il Decreto legislativo n. 82 del 2005

Come ricordato poc'anzi, il Codice dell'Amministrazione Digitale, approvato con d. lgs. n. 82 del 2005, rappresenta il cardine della normativa in materia di digitalizzazione della Pubblica Amministrazione. Il principio del *Digital first*, introdotto nel CAD con la Riforma Madia ed enunciato nell'articolo 1 della legge delega in materia di riorganizzazione delle amministrazioni pubbliche n. 124 del 2015, ne rappresenta lo spirito.

La delega incaricava il Governo di modificare il CAD «*al fine di garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché' al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici*[77] ». Il metodo per raggiungere l'obiettivo di ridefinire e semplificare i procedimenti amministrativi veniva così individuato nella applicazione del principio "*innanzitutto digitale*".

Il Codice dell'Amministrazione Digitale poggia su due pilastri: il riconoscimento in capo a cittadini ed imprese di nuovi diritti digitali e la riorganizzazione della PA, attraverso la digitalizzazione e l'utilizzo dell'ICT[78]. Per quanto attiene ai diritti, l'articolo 2, comma 1, impone alle amministrazioni di fare ricorso alle tecnologie informatiche per assicurare la «*disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale»*, configurando un vero e proprio diritto del cittadino all'amministrazione digitale[79]. Oltre al diritto all'uso delle nuove tecnologie, e il diritto di fruire dei servizi erogati dai soggetti pubblici anche attraverso dispositivi mobili [80] , vengono definiti altri concetti

[77] Legge 7 agosto 2015, n. 124, *Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*, articolo 1.

[78] F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 316.

[79] *Ivi*, p. 317.

[80] CAD, art. 7.

fondamentali per consentire al cittadino di fruire dei servizi e della cittadinanza digitale, primi fra tutti l'identità e il domicilio digitale. Si stabilisce poi la regola per cui le comunicazioni tra imprese e PA debbono avvenire esclusivamente attraverso le tecnologie dell'informazione e della comunicazione[81].

L'articolo 8-*bis* impegna le PA a "favorire" la disponibilità della connessione alla rete Internet presso gli uffici pubblici e altri luoghi pubblici, in particolare nei settori scolastico, sanitario e di interesse turistico, prevedendo la messa a disposizione anche per gli utenti. Il CAD attribuisce allo Stato e alle altre PA il compito di promuovere la diffusione della cultura digitale, lo sviluppo di competenze informatiche e l'utilizzo dei servizi digitali delle pubbliche amministrazioni. L'articolo 9 è dedicato alla partecipazione democratica elettronica, al fine di facilitare l'esercizio dei diritti politici e civili e di migliorare la qualità degli atti amministrativi attraverso processi di consultazione preventiva dei cittadini. Per quanto riguarda il secondo pilastro, cioè la riorganizzazione della PA attraverso la digitalizzazione, l'articolo 12 stabilisce che le PA utilizzino le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei diritti di uguaglianza e non discriminazione[82], nonché per il riconoscimento dei diritti digitali.

Merita di essere evidenziata la diretta correlazione tra l'inosservanza degli obblighi posti da questa norma e l'insorgere della responsabilità dirigenziale, oltre che l'impatto nella valutazione della *performance*[83]. L'articolo 15, disciplinando specificamente il tema della riorganizzazione gestionale e strutturale, attribuisce alle PA il compito di provvedere a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze di cittadini e imprese. L'attuazione della strategia per la riorganizzazione e la digitalizzazione è affidata al Responsabile per la transizione digitale, a norma dell'art. 17.

---

[81] CAD, art. 5-*bis*.

[82] È stato osservato come dalla lettura di queste norme emerga il carattere strumentale dell'innovazione tecnologica rispetto al perseguimento del principio del buon andamento dell'amministrazione di cui all'articolo 97 Cost., cfr. F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 306.

[83] Cfr. CAD, art. 12 comma 1-*ter*.

L'articolo 50 prevede che i dati delle PA siano formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione della comunicazione e che ne consentano la fruizione e il riutilizzo da parte delle altre PA e dei privati. Questa norma rappresenta il passaggio tra la raccolta delle informazioni in formato cartaceo e l'epoca del digitale, e va letta in combinato disposto con l'articolo 42 che regola il processo di dematerializzazione dei documenti amministrativi già esistenti e conservati in formato cartaceo negli uffici pubblici. In base all'arti. 42 debbono essere le stesse amministrazioni, a seguito di una valutazione costi/benefici, a stabilire quali documenti cartacei (la cui conservazione sia obbligatoria o opportuna), debbano essere trasferiti su supporto digitale, e a tal fine elaborano dei piani di sostituzione degli archivi cartacei con quelli informatici.

L'articolo 14 richiama il riparto costituzionale delle competenze legislative tra Stato e Regioni [84] specificando che spetta allo Stato disciplinare in via esclusiva il coordinamento informatico dei dati della PA. È sempre lo Stato a dettare le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati, mentre all'AgID spetta il compito di garantire il coordinamento tra i diversi livelli di governo «*con la finalità di progettare e monitorare l'evoluzione strategica del sistema informativo della Pubblica amministrazione*».

L'Agenzia per l'Italia Digitale, istituita con il decreto-legge n. 83/2012, è chiamata a promuovere l'innovazione digitale e l'utilizzo delle ICT nell'organizzazione della PA e nei rapporti tra questa e i cittadini e le imprese. La responsabilità per la redazione del Piano Triennale per l'informatica nella PA, insieme alla emanazione di Linee guida[85] e pareri tecnici, al monitoraggio dell'attività delle PA, e alla promozione della cultura digitale, assegnano ad AgiD un ruolo centrale nell'attuazione dell'Agenda digitale[86]. L'articolo 18-*bis* del CAD, introdotto dal decreto-

[84] «*In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime*», ved. Articolo 14, comma 1 del CAD.

[85] Ad esempio quelle sulla formazione, gestione e conservazione dei documenti informatici, del maggio 2021, o quelle sull'interoperabilità tecnica delle Pubbliche Amministrazioni, del maggio 2023, ved. https://www.agid.gov.it/it/linee-guida .

[86] L'Agenzia per l'Italia digitale ha il compito di redigere il Piano triennale per l'informatica nella pubblica amministrazione «*allo scopo di razionalizzare la spesa delle amministrazioni, migliorare la qualità dei servizi offerti ai cittadini e degli strumenti messi a disposizione degli operatori della p.a. e indirizzare il*

legge n. 77 del 2021, ha inoltre attribuito all'AgID funzioni di controllo, verifica, vigilanza e monitoraggio sul rispetto degli obblighi contenuti nel Codice e in ogni altra disposizione sull'innovazione tecnologica della PA, ivi comprese quelle previste nelle Linee Guida e nel Piano triennale per l'informatica nella Pubblica Amministrazione[87].

piano delle gare, dei finanziamenti e i piani triennali delle singole p.a.», cfr. G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, in *Istituzioni del Federalismo*, 2/2019, p. 472.

[87] CAD. art. 18-bis comma 1: «*L'AgID esercita poteri di vigilanza, verifica, controllo e monitoraggio sul rispetto delle disposizioni del presente Codice e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione, ivi comprese quelle contenute nelle Linee guida e nel Piano triennale per l'informatica nella pubblica amministrazione, e procede, d'ufficio ovvero su segnalazione del difensore civico digitale, all'accertamento delle relative violazioni da parte dei soggetti di cui all'articolo 2 comma 2*», ved. F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 309.

1.3.2 Il Piano Triennale per l'Informatica nella Pubblica amministrazione 2022-2024

Il Piano Triennale per l'Informatica nella Pubblica Amministrazione, redatto da AgiD e pubblicato nella Piattaforma nazionale per la *governance* dei dati[88], rappresenta il principale riferimento operativo per le PA, in quanto reca lo stato dell'arte, gli obiettivi da raggiungere nel triennio di riferimento ed i passi che le singole amministrazioni debbono compiere per raggiungere quegli obiettivi. Esso riveste particolare importanza nella gestione del patrimonio informativo dello Stato, rappresentando il documento di indirizzo strategico ed economico per la trasformazione digitale delle attività amministrative e il principale riferimento per le amministrazioni centrali e locali nello sviluppo dei propri sistemi informativi[89].

Nel suo aggiornamento 2022-2024 [90], il Piano triennale raccorda gli obiettivi di trasformazione digitale nella PA con gli assi strategici del PNRR ed in particolare con le linee di investimento dedicate alla digitalizzazione della PA. L'esperienza della pandemia di Covid-19 ha accelerato l'evoluzione tecnologica dei sistemi informativi del settore pubblico evidenziando, seppure sotto la spinta della emergenza, la necessità di rivedere l'organizzazione dei processi. D*igital & mobile first*, *digital identity only,* interoperabilità e sicurezza *by design,* accessibilità ed inclusione, codici aperti e dati bene comune sono tra principi – guida per la trasformazione digitale elencati nel Piano. Il richiamo, in apertura del documento, al nuovo art. 18-*bis* del CAD (Violazione degli obblighi di transizione digitale) imprime una maggiore vincolatività alle indicazioni contenute nel PTI, prevedendo sanzioni per la mancata ottemperanza agli obblighi previsti[91].

Il Piano triennale individua nella valorizzazione del patrimonio informativo pubblico un obiettivo strategico per la PA. Attraverso la massimizzazione dell'utilizzo dei dati le amministrazioni pubbliche potranno affrontare le sfide della *data economy*, supportare gli obiettivi della strategia europea in materia di dati, creare servizi digitale a valore aggiunto per

[88] Costituita al fine di favorire la consultazione pubblica e il confronto tra portatori di interessi relativamente alle modalità di attuazione dell'Agenda digitale, ved. CAD, art. 18.

[89] cfr. G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, cit., p. 472.

[90] Consultabile al link https://www.agid.gov.it/it/agenzia/piano-triennale .

[91] *Piano triennale per l'informatica nella PA. Aggiornamento 2022-2024*, p. 4.

tutti i portatori di interesse, fornire ai *policy-maker* strumenti *data-driven* da utilizzare nei processi decisionali e produttivi. A tal fine sarà necessario elaborare un sistema di governo dei dati coerente con la Direttiva europea 2019/1024 sul riutilizzo dell'informazione del settore pubblico[92]. Infatti anche gli adempimenti tecnici elencati nel documento[93] sono volti a migliorare la condivisione dei dati tra le pubbliche amministrazioni per finalità istituzionali e il riutilizzo dei dati, anche per finalità commerciali (O*pen data*). Per le realtà più piccole (nel documento vengono citati i Comuni con meno di 5.000 abitanti[94]) il PTI fa espresso riferimento ai meccanismi di sussidiarietà che possono essere attivati per raggiungere gli obiettivi indicati. Il capitolo 3 è dedicato alle piattaforme abilitanti[95], il cui sviluppo ha permesso una più agevole fruizione dei servizi digitali da parte dei cittadini.

La Piattaforma Digitale Nazionale Dati dovrà permettere l'apertura di flussi di dati tra le PA in modo che possa finalmente realizzarsi il principio c.d. *once only*[96]. A norma dell'art. 50-*ter* del CAD la Piattaforma Digitale Nazionale Dati, gestita dalla Presidenza del Consiglio dei ministri, è costituita da un'infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici[97]. L'accesso e l'operatività all'interno della piattaforma avvengono mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare al suo interno, mentre la condivisione di dati e informazioni avviene attraverso la messa a disposizione e l'utilizzo, da parte dei soggetti accreditati, delle c.d. API (A*pplication Programming Interface*). La PDND è finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto

[92] *Ivi*, p. 17.

[93] Relativi alle API per la fornitura di *dataset* e alla modalità di pubblicazione degli stessi.

[94] *Piano triennale 2022-2024, p. 17.*

[95] PagoPA, IO, SPID e CIE.

[96] *Ivi*, pp. 23-24. Ved. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "*Piano d'azione dell'UE per l'eGovernment 2016-2020. Accelerare la trasformazione digitale della pubblica amministrazione*", COM(2016) 179 final, 19 aprile 2016, p. 4; si veda anche R. KRIMMER, A. PRENTZA, S. MAMROT (Eds), *The Once-Only Principle. The TOOP project*, Springer International Publishing, 2021.

[97] «*L'interoperabilità permette la collaborazione e l'interazione telematica tra le pubbliche amministrazioni, cittadini e imprese, favorendo l'attuazione del principio once only e recependo le indicazioni dell'European interoperability Framework*», ved. PTI, p. 45. L'articolo 41 del CAD prevede già che le pubbliche amministrazioni forniscano, per ciascun procedimento amministrativo di loro competenza, gli opportuni servizi di interoperabilità. Si vedano anche le Linee guida "*Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici*" e le "*Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni*", adottate dall'Agenzia per l'Italia Digitale con la determinazione n. 547 del 1 ottobre 2021.

dai soggetti pubblici per finalità istituzionali, nonché la condivisione dei dati tra i soggetti che hanno diritto ad accedervi. Nella prospettiva delineata nel Piano triennale, la PDND consentirà in futuro anche l'analisi di *Big Data* pubblici, che agevoleranno l'elaborazione di politiche *data-driven*.

Infrastrutture digitali affidabili, sicure, energicamente efficienti ed economicamente sostenibili, oltre che tutelanti rispetto ai crescenti rischi, anche per la tutela dei dati personali[98] sono parte integrante della strategia di modernizzazione del settore pubblico, a fronte delle condizioni del patrimonio ICT delle PA che sono emerse dall'ultimo censimento effettuato. AgiD evidenzia come le carenze dal punto di vista di sicurezza ed affidabilità, oltre che sul piano strutturale ed organizzativo espongono il Paese a gravi rischi, come quello della interruzione o indisponibilità dei servizi, e degli attacchi cibernetici con accesso ai dati e pericolo di perdita o alterazione degli stessi. Questo scenario richiede dunque un intervento rapido con la migrazione dei servizi dalle vecchie ed inadeguate infrastrutture verso *data center* più sicuri e infrastrutture e servizi *cloud* qualificati.

In questa sezione del Piano triennale viene anche richiamata la costituzione del Polo Strategico Nazionale. Si tratta di una infrastruttura ad alta affidabilità, localizzata nel territorio nazionale per la realizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni destinate a tutte le PA. Il progetto, promosso dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, mira a tutelare l'autonomia tecnologica nazionale, a mettere in sicurezza le infrastrutture digitale, garantendo la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa di sistemi e dei servizi digitali. La creazione del PSN è la prima delle tre azioni fondamentali contenute nel documento "*Strategia Cloud Italia*[99]", licenziato dal Dipartimento per la trasformazione digitale e l'Agenzia per la cybersicurezza nazionale (settembre 2021). Esso dovrà ospitare sul territorio nazionale dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza dello Stato, in linea con quanto previsto in materia di Perimetro di sicurezza nazionale cibernetica dal DL 21 settembre 2019, n. 105 e dal DPCM 81/2021.

[98] *Piano triennale 2022-2024*, p. 36 ss..

[99] Consultabile al link https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/index.html .

La seconda e la terza priorità sono rispettivamente la creazione di un percorso di qualificazione di fornitori di *cloud* pubblico e dei loro servizi, e lo sviluppo di una metodologia di classificazione dei dati e dei servizi delle PA in modo da individuare la soluzione cloud più adeguata verso cui migrarli.

Il PRNN[100], l'istituzione dell'Agenzia per la Cybersicurezza Nazionale[101] e il decreto attuativo del Perimetro nazionale di sicurezza cibernetica[102] pongono la cybersicurezza a fondamento della digitalizzazione della PA[103]. Occorre accrescere la consapevolezza di fronte al numero crescente di minacce cibernetiche e di attacchi alla *supply chain*.

Nel capitolo dedicato alle Leve per l'innovazione (Cap. 7) oltre ad un *focus* sulle competenze digitali (di cittadini e dipendenti della PA), si parla di innovazione guidata dalla domanda pubblica. In particolare, lo sviluppo dei territori viene collegato alla creazione di *Smart communities* (in continuità con i concetti di *Smart city* e Borghi del futuro del Piano precedente). I Comuni e le città possono svolgere una funzione essenziale per migliorare la qualità della vita dei cittadini, innovare il contesto imprenditoriale, innalzare l'efficienza della PA secondo i criteri di accessibilità, innovazione e scalabilità[104]. Il programma *Smarter Italy* opererà nei settori mobilità, patrimonio culturale e salute e benessere, per estendersi poi a infrastrutture, ambiente, formazione.

Vale la pena di rilevare come molti dei temi elencati nel Piano triennale siano perfettamente sovrapponibili a quelli che caratterizzano il percorso degli enti locali verso la trasformazione in Città intelligenti: digitalizzazione, transizione ecologica, mobilità sostenibile, istruzione, inclusione e coesione sociale e salute sono temi in cui l'utilizzo di dati e sistemi di

[100] *Piano Nazionale di Ripresa e Resilienza*, approvato con decisione del Consiglio dell'Unione europea in data 13 luglio 2021, cfr. Commissione europea, *Proposta di Decisione di esecuzione del Consiglio relativa all'approvazione della valutazione del piano per la ripresa e la resilienza dell'Italia*, COM/2021/344 final, 22 giugno 2021.

[101] Ved. *Decreto-legge 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito con modificazioni dalla L. 4 agosto 2021, n. 109. A norma dell'articolo 5, comma 1 «*E' istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, l'Agenzia per la cybersicurezza nazionale […]*».

[102] Decreto-legge 21 settembre 2019, n. 105 convertito in L. 18 novembre 2019, n. 133.

[103] *Ivi*, p. 50.

[104] *Ivi*, p. 57.

Intelligenza artificiale possono permettere alle amministrazioni locali di elaborare politiche innovative ed efficienti.

Nelle pagine precedenti abbiamo cercato di delineare un quadro d'insieme della normativa rilevante, degli obiettivi, della strategia messa in campo per ottenere un reale rinnovamento *data-driven* della pubblica amministrazione, citando gli strumenti legislativi e regolamentari utilizzati e individuando i principali attori di questa trasformazione. Come abbiamo avuto modo di verificare, alle leggi ordinarie si affiancano strumenti non legislativi ma spiccatamente operativi come il Piano triennale per l'Informatica nella PA, mentre l'Agenzia per l'Italia Digitale è responsabile per l'attuazione della transizione digitale, la vigilanza sulle PA, e l'attività sanzionatoria in caso di violazione degli obblighi di transizione digitale[105].

Si deve però tener presente che sebbene il contesto normativo e regolamentare delineato appaia organico, esso è rivolto principalmente al passaggio dalla Pubblica Amministrazione analogica a quella digitale. Le indicazioni che si possono trarre dallo studio e dalla applicazione delle norme e dei documenti citati riguardano infatti la modalità attraverso la quale la PA diventa digitalizzata, ma non si occupa della gestione del prodotto di questa trasformazione. Il CAD non contiene indicazioni sulla *governance* dei dati, perché non ha ad oggetto i dati quanto tali ma piuttosto la digitalizzazione di processi amministrativi. Si tratta di una specificazione con rilevanti conseguenze pratiche. Infatti sebbene la PA italiana sia già da anni avviata nel percorso del passaggio al digitale (lo dimostrano i principi *digital first*, *cloud first*, *mobile first*…), proprio la PA si è mostrata non completamente pronta ad entrare nella *Digital Society*.

Com'è noto l'Unione europea ha individuato nella valorizzazione dei dati e nello sviluppo di sistemi di Intelligenza artificiale i due cardini dello sviluppo del Mercato Unico Digitale. La strategia si è poi concretizzata nella approvazione di numerosi atti normativi aventi ad oggetto le regole di trattamento dei dati. Torneremo più avanti diffusamente su questi aspetti, è sufficiente qui ricordare che la produzione legislativa europea ha toccato gli ambiti della protezione dei dati personali, la disciplina dei dati non personali, le regole per il riutilizzo dei dati nel settore pubblico, le tematiche della condivisione dei dati nei settori pubblico e privato. Ebbene l'applicazione di queste regole di matrice principalmente europea non è avvenuta senza

[105] Si tornerà su questi aspetti in modo più approfondito nell'ultimo capitolo.

difficoltà, proprio in quanto l'apparato di norme che disciplina il funzionamento della Pubblica amministrazione, seppure trasformato dalla digitalizzazione ha ad oggetto la gestione di procedimenti amministrativi, il rispetto delle procedure, l'adesione stretta a quanto stabilito dalla legge, ma non la *governance* dei dati.

Ecco allora che, a fronte della esigenza concreta di gestire il patrimonio informativo digitalizzato, quindi a fronte dell'emergere di una nuova, imponente, modalità di esercizio dell'attività amministrativa (con le corrispondenti, anch'esse inedite, responsabilità), l'adeguamento progressivo della PA alle regole europee in materia di dati ha richiesto a quegli stessi organismi di adeguarsi, e li ha quindi costretti ad intraprendere una faticosa metamorfosi. Le PA hanno dovuto ricalibrare procedure e modelli organizzativi alla luce della esigenza di introdurre un modello di gestione dei dati, che per sua stessa natura ha una portata tale da innescare una revisione globale.

CAPITOLO 2 - IL MODELLO DI APPLICAZIONE DEL GDPR NEGLI ENTI LOCALI

2.1 Dalla digitalizzazione al *data management*

Nell'era dei *Big Data* e della *Digital Society* la pubblica amministrazione deve affrontare una sfida ancora maggiore rispetto alla digitalizzazione. Ai pubblici poteri viene oramai richiesto non solo di svolgere la propria attività in modalità digitale, ma soprattutto di essere in grado di estrarre valore dai dati[1]. In questa prospettiva, la digitalizzazione, oltre a rappresentare un percorso obbligato di modernizzazione dell'azione amministrativa, può fungere da risorsa strategica[2].

In sede europea, alla luce delle radicali modifiche dell'economia e della società, e come conseguenza dei fenomeni tecnologici di cui si è dato atto nel capitolo precedente, la Commissione ha deciso di intraprendere un percorso volto al massimo sfruttamento del potenziale della digitalizzazione al fine di sviluppare il Mercato Unico Digitale e favorire il benessere dei cittadini europei[3]. Nell'ordinamento interno, la digitalizzazione della pubblica amministrazione, intesa come processo legislativo, amministrativo e informatico, si è realizzata attraverso il passaggio dalla modalità di svolgimento di determinate attività con strumenti analogici all'utilizzo delle tecnologie dell'informazione e della comunicazione.

Sebbene questa transizione sia stata accompagnata dal riconoscimento di diritti digitali e dei corrispettivi obblighi da parte della pubblica amministrazione, questa nuova dimensione non contiene in sé anche principi e regole per il governo del *risultato* di questa trasformazione, ovverosia dei dati. I principi-guida enunciati nel Codice dell'Amministrazione Digitale non

[1] G. CARULLO, *Dati, banche dati, Blockchain e interoperabilità nei sistemi informatici del settore pubblico*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020, p. 193. Ved. anche F. MERLONI, *Sull'emergere della funzione di informazione nelle pubbliche amministrazioni*, in F. MERLONI (a cura di) *L'informazione delle pubbliche amministrazioni*, Maggioli, Santarcangelo di Romagna, 2002, p. 16.

[2] A. MASUCCI, *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, in *Diritto pubblico*, Fasciolo 1, gennaio-aprile 2019, p. 118.

[3] Ved., *infra*, Cap. 3.

indicano modalità ed obiettivi che guidino la pubblica amministrazione verso la valorizzazione del proprio patrimonio informativo.

Poiché però è proprio attraverso i dati che si svolge la vita della società digitale, il *focus* della regolazione non può che riguardare i *data flows*. È attraverso la componente datificata della vita che ciascuno può esprimere la propria personalità, esercitare i propri diritti, svolgere le attività lavorative, contribuire allo sviluppo della società. È in un ecosistema di regole chiare che gli operatori economici possono accrescere le loro attività, fornire maggiori servizi, rafforzare il mercato. È attraverso l'uso sapiente e responsabile delle informazioni che gli organi di governo possono elaborare politiche migliori al servizio dei cittadini. Tutto ciò ha portato l'Unione europea a elaborare un piano strategico per consolidare una architettura normativa che favorisca la migliore gestione dei dati e al contempo garantisca il rispetto dei diritti fondamentali delle persone fisiche, la correttezza del mercato, la solidità della democrazia. Il primo e il più importante degli interventi normativi introdotti riguarda le regole per il trattamento dei dati personali. L'Unione ha elaborato un regolamento generale sulla protezione dei dati personali, n. 2016/679[4] (anche denominato GDPR), direttamente applicabile in tutti gli Stati membri, che pone regole univoche che possano garantire la libera circolazione dei dati personali e la tutela dei diritti e delle libertà delle persone fisiche con rispetto al trattamento dei dati personali. Il regolamento ha avuto un impatto molto significativo anche ai fini predetti, cioè nella determinazione di regole per il governo dei dati. Esso richiede ai soggetti su cui ricade la responsabilità giuridica per il trattamento dei dati personali, di dotarsi di una organizzazione interna e di predisporre procedure che garantiscano la sicurezza tecnica e giuridica nella gestione dei dati. L'apparato di principi e regole posti dal GDPR pone le basi per elaborare modelli di *data management*, ovverosia sistemi di gestione dei dati, basati su protocolli, *policies* e regole comuni di trattamento dei dati, che ne razionalizzino i flussi all'interno di una determinata organizzazione, sia essa pubblica o privata. La legislazione in materia di *data*

[4] *Regolamento (UE) 2016/679 del Parlamento 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).* Per una introduzione: G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, p. 1 ss.; LUCCHINI GUASTALLA E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. Impr*., 2018, p. 106 ss.

protection, dunque, per il suo carattere generale e la sua impostazione orizzontale e per i principi che introduce, può rappresentare un efficace impulso per una riorganizzazione dell'apparato amministrativo che, dopo aver risposto alla esigenza di digitalizzarsi, deve mostrarsi capace di governare i dati attraverso strumenti organizzativi idonei e un solido raccordo tra organi di vertice e di indirizzo politico e struttura amministrativa.

Prima di procedere a una disamina delle regole sul trattamento dei dati introdotte dalla normativa europea, e di osservarne successivamente gli effetti nei modelli di *data management* degli enti locali italiani, nel prossimo paragrafo richiameremo le tappe principali della legislazione in materia di protezione dei dati personali nell'Unione europea ed in Italia.

2.2 Cenni sulla normativa in materia di protezione dei dati personali nell'Unione europea e in Italia

2.2.1 Il contesto europeo, dalla Direttiva al Regolamento

I dati personali sono oggetto di regolazione unitaria da parte dell'allora "Comunità europea" dalla metà degli anni Novanta. Prima del 1995 alcuni Stati avevano adottato legislazioni in materia di dati, riguardanti in particolare l'impiego di elaboratori elettronici: negli anni Settanta, Austria, Lussemburgo, Francia, Repubblica Federale Tedesca, Svezia, Norvegia, Danimarca si erano dotati di norme segnate da un carattere prudenziale e tendenzialmente restrittivo; erano stati seguiti, nel decennio successivo, da Finlandia, Irlanda, Paesi Bassi e Islanda, e poi da Portogallo, Spagna, Belgio e diversi paesi dell'est d'Europa[5]. Il risultato di iniziative legislative così numerose e non coordinate restituiva un quadro giuridico disomogeneo, che non agevolava gli operatori economici negli scambi transfrontalieri. Vi era la necessità di una normativa che armonizzasse all'interno del "Mercato Unico" le differenti discipline in materia di dati allora in vigore[6].

La Direttiva 95/46/CE[7], nacque dunque per rispondere all'esigenza di garantire che la libera circolazione di persone, merci, servizi e capitali all'interno dello spazio giuridico europeo non fosse ostacolata da regole nazionali eterogenee. Già nel Considerando n. 3 comparivano gli "obiettivi gemelli": la libera circolazione dei dati personali doveva essere accompagnata dalla salvaguardia dei diritti fondamentali delle persone[8].

---

[5] Una disamina analitica in G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria e internazionale*, Giuffrè, Milano, 1997, p. 71 ss.

[6] Per una ricostruzione, S. CALZOLAIO, *Protezione dei dati personali*, aggiornamento, in *Digesto delle discipline pubblicistiche*, cit., p. 618.

[7] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.

[8] «*Considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato*

Sebbene la c.d. "Direttiva-madre" rappresenti il primo strumento legislativo della allora Comunità europea in materia di dati personali, è bene ricordare che la riflessione giuridica sugli aspetti del trattamento automatizzato dei dati personali si era già avviata da tempo. Ne dà conto proprio la Direttiva, che nel Considerando n. 11 richiama espressamente la Convenzione n. 108 del 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale[9], specificando che i principi di tutela dei diritti e delle libertà delle persone contenuti nella Direttiva *precisano ed ampliano* quelli enunciati nella Convenzione. E in effetti dalla Convenzione 108 la Direttiva 95/46 riprende principi e regole che, tutt'ora costituiscono i cardini della normativa europea in materia di protezione dei dati personali, quali la necessità di una base giuridica che legittimi il trattamento, il principio di finalità, l'esattezza, la limitazione della conservazione, il divieto di trattamento se non in presenza di adeguate garanzie, di dati che rivelino l'origine razziale, le opinioni politiche, le convinzioni religiose, lo stato di salute, la vita sessuale, oltre che relativi a condanne penali.

La Direttiva 95/46 recava le linee fondamentali di un modello europeo di protezione dei dati personali. L'articolato tratteggiava infatti uno schema contenente gli elementi essenziali per consentire agli Stati membri, su tale base, di predisporre normative nazionali a tutela della *privacy* che fossero omogenee nei tratti fondamentali: definizioni, disciplina, istituzione di una autorità di controllo, sanzioni, regole per i settori speciali.

Questo schema è stato poi declinato in modi anche sensibilmente diversi dai singoli Stati Membri, nella fase di recepimento. Tali divergenze nel recepimento della Direttiva, sono state

membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona», cfr. Direttiva n. 95/46, Considerando n. 3.

[9] Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 28 gennaio 1981*. Questa Convenzione è stata elaborata per integrare la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, anch'essa elaborata in seno al Consiglio d'Europa, che pur tutelando il rispetto della tutela della vita privata e familiare, non conteneva riferimenti ad una tutela più specifica rispetto alla dimensione digitale e ai trattamenti automatizzati di dati personali che potessero incidere sui diritti fondamentali delle persone fisiche. Per un commento si veda G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria e internazionale*, cit., p. 8 ss.

L'articolato è stato di recente oggetto di un intervento di modernizzazione, realizzatosi tramite l'azione di un protocollo di emendamento, ved. 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018), Ad hoc Committee on Data Protection (CAHDATA) –Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

affiancate nel tempo dall'emergere della necessità di adeguare alla evoluzione tecnologica le regole europee che nel frattempo avevano in parte perso la loro efficacia, in ragione di una realtà completamente rinnovata. La Direttiva 95/46 era nata, effettivamente, in un contesto tecnologico, economico e politico molto diverso da quello attuale. Essa interveniva a regolare un modello sostanzialmente statico di trattamento dei dati personali in cui il flusso di dati era univoco: dall'interessato al titolare del trattamento[10]. Il regolamento n. 2016/679[11], adottato per sostituire la Direttiva-madre, raccoglie e cerca di razionalizzare l'esperienza maturata in Europa negli ultimi venti anni[12], approntando una disciplina che tenga conto degli avanzamenti nel campo dell'ICT e dei *Big Data* che nel frattempo hanno ridisegnato le modalità di utilizzo dei dati[13].

Occorre ricordare, prima di procedere oltre, che il diritto alla protezione dei dati personali è stato oggetto, quasi di pari passo con il passaggio dalla Direttiva al regolamento, di un processo che ne ha sancito la natura di diritto fondamentale. La Carta dei diritti fondamentali dell'Unione europea[14], adottata nel 2000, oltre a confermare con l'articolo 7 l'esistenza di un diritto al rispetto della vita privata e familiare[15] , proclama all'articolo 8, un autonomo diritto alla protezione dei dati di carattere personale[16], e ne delinea il nucleo essenziale (principi del

[10] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 9.

[11] 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).

[12] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 14.

[13] «*La realtà dei social network e dei motori di ricerca, in un modo digitalmente sempre interconnesso […] si basa su un modello di condivisione e di cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale*», ved. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 9.

[14] R. ADAM, *Da Colonia a Nizza: la Carta dei diritti fondamentali dell'Unione europea*, in *Il diritto dell'Unione europea*, n. 4/2000; R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, cit..

[15] Ved. T. GROPPI, *art. 7, Rispetto della vita privata e della vita familiare*, in R. BIFULCO, M. CARTABIA, A. CELOTTO, *L'Europa dei diritti*. *Commento alla Carta dei diritti fondamentali dell'Unione Europea,* cit.; G. MARTINICO, *art. 7*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.

[16] Ved. O. POLLICINO, M. BASSINI, *art. 8*, in *Carta dei Diritti fondamentali dell'Unione europea*, R. MASTROIANNI, O. POLLICINO, A. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), cit.; F. DONATI, *art. 8, Protezione dei dati di carattere personale*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, cit..

trattamento, diritti degli interessati, ed una autorità indipendente preposta al controllo sul rispetto del diritto[17]).

La Carta ha poi assunto lo stesso valore giuridico dei Trattati (TUE e TFUE[18]) nel 2009[19], con l'approvazione del Trattato di Lisbona[20]. Ciò che più rileva in questo percorso di "costituzionalizzazione" del diritto alla protezione dei dati personali, deve rinvenirsi nella modifica dei trattati istitutivi dell'Unione europea. La proclamazione del diritto fondamentale alla protezione dei dati personali ha infatti indotto a inserire una competenza specifica dell'Unione europea nell'articolo 16 del Trattato sul funzionamento dell'Unione[21], che ora riconosce ad ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano e prevede che sia istituita una autorità indipendente che vigili sul rispetto delle norme in materia. A partire dal 2009 dunque con l'articolo 6 del TUE si è riconosciuto alla Carta dei diritti dell'Unione europea lo stesso valore giuridico dei Trattati, e con l'articolo 16 del TFUE si è allargata correlativamente la competenza materiale dell'Unione europea anche al settore della *data protection*[22].

Su questo fondamento giuridico è stato adottato il regolamento n. 2016/679. Merita di essere segnalato anche un altro aspetto, in quanto la Direttiva 95/46 era stata adottata sulla

[17] Cfr. S. CALZOLAIO, *Protezione dei dati personali*, aggiornamento, in *Digesto delle discipline pubblicistiche*, cit., p. 618.

[18] Il Trattato sull'Unione europea e il Trattato sul funzionamento dell'Unione europea. Ved. F. POCAR, M.C. BARUFFI, *Commentario breve ai trattati dell'Unione europea*, CEDAM, Padova, 2014.

[19] *Ex plurimis*, ved. V. PICCONE, O. POLLICINO (a cura di), *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività*, Editoriale scientifica, Napoli, 2018; G. DEMURO, *La Carta dei diritti*, in A. LUCARELLI, A. PATRONI GRIFFI (a cura di), *Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea*, Edizioni Scientifiche italiane, Napoli, 2009; P. GIANNITI (a cura di), *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Zanichelli, Bologna, 2013; N. LAZZERINI, *La carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Franco Angeli, Milano, 2018; MASTROIANNI R., POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O, (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017; L. TRUCCO, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Giappichelli, Torino, 2013.

[20] L'articolo 6, par. 1 del Trattato sull'Unione europea, come modificato dal Trattato di Lisbona, recita: «*L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati*».

[21] P. PIRODDI, *art. 16 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, seconda edizione, CEDAM, Padova, 2014.

[22] S. CALZOLAIO, *Protezione dei dati personali*, aggiornamento, in *Digesto delle discipline pubblicistiche*, cot., p. 620.

base degli articoli 7A e 100A del Trattato istitutivo della Comunità europea[23] e quindi come misura di ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri, al fine della instaurazione progressiva di un mercato interno[24]. Seppure la Direttiva-madre esordisse con la proclamazione, al primo comma dell'articolo 1, del diritto alla vita privata con riguardo al trattamento dei dati personali, lasciando al secondo comma un divieto di restrizioni della circolazione dei dati medesimi, il fondamento giuridico e strategico della stessa vanno ricercati principalmente nella volontà di agevolare la libera circolazione delle merci, delle persone, dei servizi e dei capitali[25]. Il GDPR, seppure mantenendo all'articolo 1 la stessa successione («*Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati*»), fonda la sua legittimazione giuridica nell'articolo 16 del TFUE che ha ad oggetto la tutela di un diritto fondamentale, per la cui disciplina attribuisce al Parlamento europeo e al Consiglio una specifica competenza legislativa.

[23] Trattato che istituisce la Comunità europea, 11992E/TXT, in Gazzetta ufficiale n. C 224 del 31/08/1992.

[24] S. CALZOLAIO, *Protezione dei dati personali*, aggiornamento, in *Digesto delle discipline pubblicistiche*, cit., p. 619.

[25] Cfr. TCE, art. 7A, par. 2.

2.2.2. Il contesto italiano, dal vecchio al nuovo Codice della *privacy*

Il recepimento della Direttiva n. 96/45 e poi l'adeguamento al regolamento n. 2016/679 sono avvenuti in Italia attraverso l'adozione della legge n. 675/1996[26] e poi del c.d. "Codice della *privacy"* (D. lgs. n. 196/2003[27]) e infine con la modifica di quest'ultimo attraverso il D. lgs. n. 101/2018[28]. L'adozione nel nostro ordinamento della prima legge sulla *privacy* è avvenuta sotto la spinta delle scadenze europee, onde evitare il rischio che l'Italia rimanesse esclusa dal c.d. spazio *Schengen*. Di conseguenza, la legge n. 675 del 31 dicembre 1996 dovette essere più volte rimaneggiata per correggere imperfezioni ed imprecisioni dovute a una approvazione affrettata. I numerosi interventi di modifica e integrazione della legge resero dopo pochi anni necessaria una razionalizzazione delle norme prodotte, che si realizzò attraverso l'approvazione del D. lgs. n. 196 del 2003 (c.d. Codice della *privacy*), il corpus organico che di fatto ha rappresentato il riferimento unico della materia sino all'entrata in vigore del regolamento europeo n. 2016/679, il 25 maggio 2018.

Con la legge n. 163/2017, legge di delegazione europea 2016-2017, al Governo è stata delegata l'adozione di uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del GDPR[29]. Tali decreti dovevano essere adottati[30], al fine di abrogare le parti del D. lgs. n. 196/2003 incompatibili con le nuove disposizioni regolamentari, modificare

[26] legge 31 dicembre 1996, n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.*

[27] Decreto legislativo 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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).*

[28] Decreto legislativo 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).*

[29] Per una ricostruzione del percorso di adeguamento della normativa interna alla riforma ved. E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 61 ss.

[30] Su proposta del Presidente del Consiglio dei Ministri e del Ministro della Giustizia, di concerto con i ministri degli Affari esteri e della Coorperazione internazionale, dell'Economia e delle Finanze, dello Sviluppo economico e per la semplificazione e la pubblica amministrazione, acquisiti i pareri delle competenti commissioni parlamentari e del Garante.

il Codice per dare attuazione alle norme del regolamento non direttamente applicabili, coordinare le disposizioni vigenti in materia di *data protection* con quelle contenute nel GDPR, prevedere, ove opportuno, il ricorso a provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali, nell'ambito e per le finalità previsti dal regolamento, adeguare il sistema sanzionatorio penale e amministrativo vigente con la previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse[31]. La legge n. 167/2017 ha apportato le prime modifiche al d. lgs. n. 196/2003, relative a termini di conservazione dei dati di traffico telefonico, responsabilità del trattamento, riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici e funzionamento del Garante per la protezione dei dati personali. La legge di bilancio n. 205/2017[32], ha introdotto a sua volta una serie di ulteriori specifiche in materia di interesse legittimo, informativa e compiti del Garante. Con il d. lgs. 10 agosto 2018 n. 101 si è infine provveduto ad abrogare le disposizioni del d. lgs. n. 196/2003 non compatibili con il GDPR, e ad inserirne di nuove.

Diverse norme del regolamento europeo n. 2016/679 fanno infatti espresso rimando alla potestà normativa degli Stati membri per la specificazione del contenuto delle prescrizioni. Tra di esse l'articolo 6 par. 2, che consente agli Stati membri di adottare disposizioni più specifiche nei settori disciplinati dal Capo IX[33] e per quanto attiene al trattamento basato su un obbligo legale o sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, l'articolo 9 par. 4, che autorizza gli Stati membri a mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, o ancora dell'articolo 23 che prevede la possibilità, per lo Stato membro, di limitare la portata dei diritti riconosciuti agli interessati qualora tale limitazione sia necessaria e proporzionata per salvaguardare interessi collettivi quali la sicurezza nazionale, la difesa, l'indipendenza della magistratura.

Il Codice della *privacy* è risultato ampiamente rivisto e modificato dalla novella di armonizzazione che è entrata in vigore il 19 settembre 2018. *Lavorando di cesello*, il legislatore

[31] Cfr. legge 25 ottobre 2017, n. 163, art. 13 comma 3.

[32] "Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018/2020"

[33] Si tratta ad esempio della disciplina della libertà di espressione e di informazione (art. 85), dell'accesso ai documenti della pubblica amministrazione (art. 86), del trattamento di dati nell'ambito dei rapporti di lavoro (art. 88).

ha proceduto a numerosi tagli e riformulazioni, che anziché preservare l'organicità del Codice ne hanno smembrato l'impianto in maniera non uniforme, rendendo il nuovo testo, nella opinione di diversi commentatori, non organico e di non agevole lettura[34]. Occorre evidenziare come il legislatore italiano nell'intento di mantenere la veste esteriore del Codice per la protezione dei dati personali, ne abbia poi nei fatti modificato la struttura così profondamente da restituire un codice che molto poco ha ormai dell'organicità che dovrebbe avere[35].

L'articolo 1 del d. lgs. n. 196/2003 a seguito delle modifiche introdotte dal d. lgs. n. 101/2018 stabilisce che il trattamento dei dati personali deve avvenire secondo le norme del regolamento europeo n. 2016/679 e del Codice della *privacy*. Lo scopo principale della norma è dunque quello di chiarire che il Codice novellato «*forma sistema col GDPR e non vive di vita propria e autonoma*[36]». L'articolo 2, nello specificare che il Codice «*reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento*», di fatto conferma la definitiva perdita di centralità del d. lgs. n. 196/2003 nella infrastruttura normativa del sistema di *data protection* italiano[37].

[34] Evidenzia questi aspetti E. LUCCHINI GUASTALLA, in *Privacy e data protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., pp. 62-63, che compiendo una analisi dettagliata degli interventi di modifica osserva che «*Gran parte delle disposizioni del decreto privacy consistono in un intervento manipolativo sul testo del Codice privacy. Questo tipo di intervento si appunta soprattutto sulla parte III del Codice, laddove le modifiche riguardano la disciplina dei mezzi di tutela (art. 140 bis); la struttura e i compiti del Garante (artt. 153-160); impianto sanzionatorio (artt. 166-172). Le abrogazioni sono invece massicce nella parte II, relativa al trattamento dei dati in specifici settori, che si apre col nuovo articolo 45 bis del nuovo Codice privacy. Ma è nella parte I che l'intervento demolitorio del decreto privacy si manifesta in misura radicale: sono stati abrogati, infatti, i titoli dal II al VII ed è stato conservato il solo titolo I*», *Ibidem*.

[35] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 4.

[36] F. PIZZETTI, *La parte I del Codice novellato*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Giappichelli, Torino, 2021, p. 83.

[37] «*L'art. 2, infatti, proprio perché intitolato "finalità", chiarisce oltre ogni ragionevole dubbio interpretativo e applicativo che il d. lgs. n. 196/2003, come novellato dal d. lgs. n. 101/2018, è l'atto legislativo di "adeguamento" dell'ordinamento italiano al GDPR e radica la sua legittimazione e la sua ragion d'essere nell'adeguare la legislazione italiana al GDPR*», cfr. F. PIZZETTI, *La parte I del Codice novellato*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 84.

2.3 L'entrata in vigore del Regolamento europeo n. 2016/679 in materia di protezione dei dati personali.

2.3.1 I tratti essenziali della normativa

Nelle pagine precedenti si è sottolineato come l'esigenza di garantire adeguata protezione ad una consistente serie di nuove fattispecie di trattamento dei dati, unita all'evidente peso strategico della gestione e dell'utilizzo dei dati personali nello sviluppo del *Digital Single Market*, siano state il motore del decisivo passaggio dalla direttiva al GDPR. Come viene chiarito nel Considerando n. 9 del regolamento, «*la Direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione*», né ha eliminato l'incertezza giuridica e la percezione che le operazioni *online* comportino forti rischi per la protezione delle persone fisiche.

Il regolamento n. 2016/679 punta, dunque, a superare il descritto sistema di protezione dei dati personali frammentato nel territorio europeo, il quale poteva comportare rischi per la libera circolazione dei dati personali, nonché per il libero esercizio delle attività economiche e della concorrenza, anche e soprattutto in considerazione dell'ampliamento dei servizi *online* e dell'insicurezza a questi connessa [38] . L'esigenza, ricordiamolo, è quella di assicurare un'applicazione omogenea della normativa vigente, al fine di creare un clima di fiducia per lo sviluppo economico degli ambienti *online*, evitando che un quadro giuridico incerto possa costituire un freno allo sviluppo dell'economia digitale. Le richiamate considerazioni hanno contribuito alla scelta dello strumento giuridico utilizzato dal legislatore europeo. Da uno strumento di armonizzazione come la Direttiva si è passati ad un regolamento direttamente applicabile negli Stati membri, che non necessita di atti di recepimento e funge piuttosto da veicolo di uniformazione del diritto nello spazio giuridico europeo[39].

[38] G. GARDINI, *Le regole dell'informazione. L'era della post-verità*, Giappichelli, Torino, 2017, p. 327.

[39] Cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 13.

Il regolamento n. 2016/679 raccoglie ed attualizza gran parte della elaborazione dottrinale, normativa, giurisprudenziale europea in tema di protezione dei dati personali. I principi – chiave enunciati nel GDPR sono infatti rinvenibili nella Direttiva 95/46 e prima ancora nella Convenzione 108. Ma, come è stato evidenziato in dottrina, vi sono alcune novità di rilievo che pongono il GDPR in una nuova epoca di attività normativa, che tiene conto in maniera più sistematica dell'elemento tecnologico[40]. Nelle prossime pagine si tenterà, senza pretesa di esaustività, di dar conto dei contenuti del regolamento n. 2016/679. Partendo dalla delimitazione dell'ambito di applicazione della disciplina, si richiameranno i principi fondamentali. Si procederà poi ad una rassegna dei contenuti, volutamente privilegiando le regole il cui impatto sarà poi evidente nella disamina del modello di attuazione del GDPR negli enti locali (*infra*).

[40] Per una sintesi delle novità e precisazioni introdotte si veda G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 14 ss, che richiama in particolare l'introduzione di una norma sul consenso dei minori, le nuove definizioni di dato biometrico e pseudonimizzazione, le precisazioni sull'informativa, la rinnovata disciplina del diritto all'oblio, il diritto alla portabilità, le norme sul trasferimento dei dati all'estero, lo sportello unico, l'autorità capofila, il meccanismo di coerenza, nonché le regole per il foro competente, il regime di responsabilità civile, le sanzioni amministrative.

2.3.2. Il contenuto del Regolamento 2016/679

Per iniziare una panoramica sui contenuti del regolamento 2016/679 sarà opportuno definirne l'ambito di applicazione. Innanzitutto va ricordato che i principi e le regole contenuti nel GDPR sono applicabili a tutte le tipologie di trattamento, automatizzato o parzialmente automatizzato dei dati personali, al trattamento non automatizzato di dati personali ove questi siano contenuti in un archivio o siano destinati a comparirvi[41], al trattamento di dati personali effettuato dal titolare che abbia uno stabilimento nel territorio dell'Unione [42]e al trattamento di dati personali di interessati che si trovano nell'Unione, anche ove il titolare non sia stabilito nell'Unione, quando le attività di trattamento riguardino l'offerta di beni e servizi e il monitoraggio del comportamento all'interno dell'Unione (art. 3).

Il ventaglio dei soggetti pubblici e privati che ricadono entro gli estesi limiti della applicabilità del regolamento n. 2016/679 è quindi estremamente ampio, così come è ampio l'insieme dei soggetti interessati, non comparendo nel GDPR alcun riferimento al requisito della cittadinanza per poter accedere alla protezione dei propri diritti («*interessato*» è infatti, semplicemente, la «*persona fisica identificata o identificabile*[43]»).

Non sarà possibile in questa sede andare oltre una brevissima disamina dei contenuti del regolamento, mentre gli approfondimenti su taluni aspetti specifici saranno affrontati ogniqualvolta emergeranno, negli sviluppi del lavoro, elementi rilevanti in relazione alla loro declinazione nell'ambito di interesse di questa ricerca.

---

[41] Cfr. GDPR, art. 2 par. 1, fatte salve le esclusioni elencate nel par. 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 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*». Ved. L. BOLOGNINI, E. PELINO, (a cura di), *Codice della disciplina privacy*, Giuffrè Francis Lefevbre Milano, 2019, pp. 11-12.

[42] O in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico, cfr. GDPR, art. 3 par. 3. Per una disamina approfondita delle condizioni di applicazione materiale e territoriale del Regolamento 2016/679 si vedano M GRAZIADEI, *art. 2*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di)*, Codice della privacy e data protection,* Giuffrè, Milano, 2021, p.129 ss. e, *ivi*, M. CATANZARITI, art. 3, pp. 143 ss.

[43] GDPR, art. 4 par. 1 n. 1.

Nell'articolo 5 del regolamento vengono descritti i principi applicabili al trattamento dei dati personali, cioè liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, e vengono posti in capo al titolare del trattamento la responsabilità per il loro rispetto e il dovere di darne prova[44].

Queste ultime due attribuzioni, poste in capo al titolare, che insieme costituiscono il nucleo del principio di responsabilizzazione (o *accountability*), insieme ai principi di *privacy by design* e *privacy by default* rappresenta probabilmente l'innovazione più significativa introdotta nel regolamento n. 2016/679, che colloca la figura del titolare del trattamento al centro dell'intero sistema di *data protection*.

A norma dell'articolo 24 del GDPR il titolare, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà degli individui, mette in atto misure tecniche e organizzative adeguate «*per garantire ed essere in grado di dimostrare*» che il trattamento è effettuato nel rispetto del regolamento[45].

I già citati principi di *privacy by design* e *by default*[46], enunciati nell'articolo 25, prevedono che ogni nuovo trattamento di dati personali sia posto in essere tenendo in

[44] Si vedano per un commento G. MALGIERI, *art. 5* in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di)*, Codice della privacy e data protection,* cit., p. 176 ss.; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Wolters Kluwer, Milano, 2018, p. 49 ss.

[45] Per un commento alla norma ved. F. PIZZETTI, L. GRECO, *art. 24*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, cit., p. 398 ss.;

[46] GDPR, art. 25, Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita: «*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 […]*». Per un commento si veda D. FARACE, *Privacy by design e privacy by default*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 485 ss.

considerazione la protezione dei diritti degli interessati fin dalle prime fasi di progettazione. Inoltre, il titolare deve mettere in atto misure tecniche ed organizzative affinché siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento.

A ben vedere, i principi in esame costituiscono una summa dei principi di minimizzazione di limitazione della finalità, da cui discende a sua volta il principio della limitazione della conservazione [47] . Il loro inserimento nel testo del regolamento europeo n. 2016/679 sembrerebbe rispondere alla esigenza di arginare la potenziale pervasività tecnologica digitale, anticipando la tutela alla fase antecedente al trattamento, *ab origine,* e non relegandola solo ad una valutazione *ex post* dei possibili danni[48].

Nel nuovo assetto giuridico di tutela dei dati personali delineato dal GDPR, infatti, il titolare è tenuto ad effettuare una valutazione dei rischi per i diritti e le libertà delle persone fisiche che potrebbero conseguire al trattamento dei dati personali[49], e conseguentemente a determinare le misure di sicurezza da adottare[50]. Il ruolo del *data controller* si fa pertanto proattivo e non più solamente rivolto all'adempimento di regole puntualmente individuate dal regolatore. Il titolare è inoltre tenuto a monitorare l'efficacia delle misure adottate, a riesaminarle e aggiornarle qualora necessario[51].

Dalla lettura in combinato disposto dei principi appena richiamati emerge una visione integrata della protezione dei dati personali, che coinvolge necessariamente diversi profili, tra cui perlomeno quelli informatico, giuridico e organizzativo[52] , ed è espressione del c.d. approccio basato sul rischio. Sulla base del *risk-based approach* spetta infatti al titolare il compito di

[47] E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., pp. 85-86.

[48] E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice privacy*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 21.

[49] I rischi presentati dal trattamento dei dati personali sono ad esempio la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati dal Titolare, cfr. GDPR, Considerando n. 83.

[50] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 2.

[51] S. CALZOLAIO, *Protezione dei dati personali*, aggiornamento, in *Digesto delle discipline pubblicistiche*, cit., p. 630.

[52] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 18.

valutare esso stesso la presenza di rischi inerenti al trattamento, e conseguentemente di applicare misure adeguate a minimizzare il rischio, alla luce dei costi e dello stato dell'arte, della natura dei dati, dell'oggetto, del contesto e delle finalità del trattamento, dei rischi per i diritti e le libertà degli individui[53].

Il Considerando n. 76 del GDPR specifica che il titolare dovrebbe essere in grado di individuare, al termine della valutazione di tutti gli elementi, la eventuale presenza di un rischio elevato per i diritti e le libertà delle persone fisiche [54]. In tali casi, conseguenti in particolare con l'uso di nuove tecnologie[55], al titolare è richiesto, a norma dell'art. 35 del GDPR, di effettuare una valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment, DPIA*), come richiesto dall'articolo 35 del GDPR[56]. Ancora una volta è il principio di *accountability* a porre in capo al titolare il dovere di compiere tutte le valutazioni relative al trattamento dei dati personali e di agire di conseguenza. Il principio di responsabilizzazione funge quindi da meta-principio, utile a garantire la concreta attuazione degli altri principi sul trattamento dei dati[57].

Nella sua *Opinion n. 3 del 2010*, il Gruppo di lavoro Articolo 29[58] aveva proposto alla Commissione l'introduzione, nella Direttiva 95/46 del principio di *accountability*. Lo scopo di tale

[53] Cfr. GDPR, art. 32.

[54] Sui criteri di identificazione del "rischio elevato", ved. Gruppo di lavoro Articolo 29, *Linee guida concernenti la valutazione di impatto sulla protezione dei dati nenchè i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, WP248, 4 ottobre 2017; ved. anche Garante per la protezione dei dati personali, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679* - 11 ottobre 2018, docweb n. 9058979.

[55] Ad esempio i trattamenti di categorie particolari di dati su larga scala effettuati attraverso una nuova tecnologia, che espone a massicci danni da *data breach*, oppure a decisioni automatizzate che producano effetti giuridici o incidano in modo analogo sull'interessato in misura significativa a seguito di valutazioni sistematiche e globali di aspetti personali, cfr. N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 130-131.

[56] Sulla DPIA, e*x plurimis*, A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva* (artt. 32-39), in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. FINOCCHIARO (a cura di), Zanichelli, Bologna, 2017, p. 287 ss.; F. SARTORE, *La valutazione d'impatto nel GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2019, p. 333 ss.; R. TORINO, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

[57] G. GARDINI, *Le regole dell'informazione. L'era della post-verità*, cit., p. 328.

[58] Direttiva 95/46/CE, Articolo 29, *Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali*: «*1. È istituito un gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, in appresso denominato «il gruppo». Il gruppo ha carattere consultivo e indipendente. 2. Il gruppo è composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato*

innesto nella Direttiva sarebbe stato, nelle intenzioni del WP29, quello di portare la protezione dati "dalla teoria alla pratica", un modo cioè per incoraggiare i titolari del trattamento ad utilizzare strumenti più concreti ed efficaci per la protezione dei dati[59].

Già nella elaborazione contenuta nel parere in esame, il principio di *accountability* veniva declinato prevedendo in capo al titolare la responsabilità di individuare misure adeguate ed efficaci per proteggere i dati personali, e il dovere di darne evidenza[60]. Questo principio come poc'anzi ricordato è poi divenuto il cardine dell'intero sistema di protezione dei dati personali delineato nel regolamento n. 2016/679[61]. Giova sottolineare che la lista esemplificativa delle attività attraverso le quali i titolari dovrebbero dare applicazione concreta del principio di responsabilizzazione, stilata dal Gruppo di lavoro Articolo 29 ed inserita nella *Opinion n. 3/2010*, contiene la descrizione di buona parte dello strumentario oggi in uso per garantire la *compliance*

membro e da un rappresentante della o delle autorità create per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione. Ogni membro del gruppo è designato dall'istituzione oppure dalla o dalle autorità che rappresenta. Qualora uno Stato membro abbia designato più autorità di controllo, queste procedono alla nomina di un rappresentante comune. Lo stesso vale per le autorità create per le istituzioni e gli organismi comunitari. 3. Il gruppo adotta le sue decisioni alla maggioranza semplice dei rappresentanti delle autorità di controllo. 4. Il gruppo elegge il proprio presidente. La durata del mandato del presidente è di due anni. Il mandato è rinnovabile. 5. Al segretariato del gruppo provvede la Commissione. 6. Il gruppo adotta il proprio regolamento interno. 7. Il gruppo esamina le questioni iscritte all'ordine del giorno dal suo presidente, su iniziativa di questo o su richiesta di un rappresentante delle autorità di controllo oppure su richiesta della Commissione».

[59] Article 29 Data protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13 luglio 2010, p. 3.

[60] Article 29 Data protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13 luglio 2010, p. 9.

[61] L'articolo 24 del GDPR recita: «*Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità 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 dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*». Sul principio di *accountability* ved. G. MALGIERI, *art. 5* in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di)*, Codice della privacy e data protection,* cit., pp. 189-190; F. PIZZETTI, L. GRECO, *art. 24*, ivi, p. 405 ss.*;* G. FINOCCHIARO*, Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali, in* G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* cit., p. 1 ss.*;* C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato,* in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Editoriale scientifica, Napoli, 2017, p. 128 ss

al GDPR[62]. da parte dei *data controllers* di piccole e grandi dimensioni per garantire la tutela dei dati personali degli interessati[63].

Procedendo nella rapida disamina dei contenuti del regolamento n. 2016/679, meritano di essere esaminati gli articoli 6 e 9, nei quali si sostanzia il principio di liceità proclamato nell'articolo 5. Se da una parte l'articolo 6 elenca le basi giuridiche che legittimano il trattamento dei dati personali, dall'altra l'articolo 9 pone un divieto di trattamento per tutte le categorie di dati personali che, se trattate in assenza delle adeguate tutele e garanzie, potrebbero esporre l'interessato al rischio di gravi discriminazioni. Tra le basi giuridiche elencate nell'articolo 6 compaiono il consenso dell'interessato, l'esecuzione di un contratto o di misure precontrattuali, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, il perseguimento di un legittimo interesse del titolare del trattamento[64]. L'articolo 9, come poc'anzi ricordato, pone un divieto di trattamento per le categorie particolari di dati personali, ovverosia quelle idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il secondo paragrafo contiene invece una serie di discriminanti che, ove presenti, rendono legittimo il trattamento di queste tipologie di dati personali. Compaiono in

[62] Si noti che larga parte delle misure di *compliance* contenute nella lista esemplificativa del WP29 è successivamente confluita nell'articolato del GDPR.

[63] «*• Establishment of internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc); • Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects. • Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations, • Appointment of a data protection officer and other individuals with responsibility for data protection; • Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc. • Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects; • Establishment of an internal complaints handling mechanism; • Setting up internal procedures for the effective management and reporting of security breaches; • Performance of privacy impact assessments in specific circumstances; • Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc)*», cfr. Article 29 Data protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13 luglio 2010, pp. 11-12.

[64] Ved. D. POLETTI, *art. 6*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* cit., p. 191 ss.;

questo elenco il consenso esplicito dell'interessato, l'assolvimento di regole in materia di diritto del lavoro, la tutela di un interesse vitale, i trattamenti effettuati all'interno delle attività di una fondazione o associazione, i casi in cui i dati personali siano stati resi pubblici dall'interessato, i trattamenti necessari per tutelare un diritto in sede giudiziaria, i trattamenti effettuati per motivi di interesse pubblico rilevante, o per finalità di medicina preventiva o di medicina del lavoro, o per motivi di interesse pubblico nel settore della sanità pubblica, di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[65].

Il regolamento n. 2016/679 dedica un intero capo ai diritti degli interessati. Gli articoli da 12 a 22 contengono un vero e proprio decalogo di diritti azionabili, e specularmente impongono ai titolari di mettere in atto le misure necessarie a garantirne la tutela e l'esercizio. Alle norme sulla trasparenza e l'informazione seguono i diritti di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità, il diritto di opposizione e infine il divieto per il titolare di sottoporre l'interessato ad una decisione basata unicamente sul trattamento automatizzato dei dati personali che produca effetti giuridici che lo riguardano o che incida significativamente sulla sua persona[66].

Proseguendo nella rassegna dei contenuti del regolamento n. 2016/679, significative appaiono le norme che regolano l'individuazione dei c.d. ruoli *privacy*. Spetta anche in questo caso al titolare dare istruzioni a tutti i soggetti che, internamente o esternamente alla propria organizzazione, sono da lui incaricati a trattare dati personali. È quanto emerge dalla lettura dell'articolo 29 del GDPR, ove si specifica che il responsabile del trattamento o chiunque agisca sotto la sua responsabilità o sotto la responsabilità del titolare, possono trattare i dati personali solo se istruiti in tal senso dal titolare medesimo.

L'articolo 28 del regolamento n. 2016/679 regola invece tutti i casi in cui i dati personali siano trattati da soggetti estranei all'organizzazione del titolare, ma per conto di quest'ultimo.

---

[65] Ved. A. THIENE, *art. 9*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection,* cit., p. 239 ss.

[66] Si vedano, *ex plurimis*, i commentari L. BOLOGNINI, E. PELINO, (a cura di), *Codice della disciplina privacy*, cit.; R. PANETTA, (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, cit.; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit.; G.M. RICCIO, G. SCORZA, E. BELISARIO, (a cura di), *GDPR e normativa privacy. Commentario*, Wolters Kluwer, Milano, 2018.

Anche in questa ipotesi spetta al titolare individuare responsabili "esterni" che presentino garanzie sufficienti in termini di compliance al GDPR e tutela dei diritti degli interessati. Il paragrafo 3 richiede che i rapporti tra titolare e responsabile siano disciplinati da un contratto o da altro atto giuridico che contenga dettagli relativi alla materia disciplinata, alla durata, alla natura e alle finalità del trattamento, al tipo di dati trattati, alle categorie di interessati, agli obblighi e ai diritti del titolare del trattamento. Seguono alcune clausole che dovranno obbligatoriamente essere inserite nell'accordo tra titolare e responsabile, tutte finalizzate a garantire la saldezza della catena delle responsabilità per il trattamento dei dati personali e la sicurezza del trattamento stesso[67].

Il GDPR disciplina anche l'eventualità che vi siano più soggetti a determinare congiuntamente finalità e mezzi del trattamento. Nel caso di contitolarità essi dovranno determinare in modo trasparente, mediante un accordo interno – il cui contenuto essenziale sarà messo a disposizione dell'interessato - le rispettive responsabilità in merito all'osservanza del regolamento n. 2016/679, con particolare riguardo ai doveri di informazione e ai diritti dell'interessato[68].

Il legislatore europeo ha riscritto la normativa sulla protezione dei dati personali modificando in modo apparentemente limitato la forma di molte disposizioni, ma intervenendo

[67] *«[…] Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato»*, cfr. GDPR, art. 28 par. 3.

[68] Cfr. GDPR, art. 26.

molto sul piano sostanziale; così di conseguenza il quadro complessivo inevitabilmente conferisce a tutte le disposizioni un diverso significato e contenuto, benché la veste formale apparentemente sia la medesima[69]. Vi sono però alcune novità di rilievo. Una di queste è l'introduzione della figura del Responsabile per la protezione dei dati personali (*Data Protection Officer* o DPO nella, più corretta, dicitura in lingua inglese). L'inserimento, all'interno della organizzazione del titolare[70], di un profilo specifico, dotato di competenza specialistica della normativa e della prassi in materia di *data protection* compariva già nella lista redatta nel 2010 dal Gruppo di lavoro Articolo 29, ed inserita nel già citato Parere sul principio di *accountability*. E in effetti il coinvolgimento di una figura indipendente e altamente specializzata in tutte le questioni riguardanti la protezione dei dati personali (compresa la valutazione di impatto privacy[71], le violazioni di dati personali[72], i diritti degli interessati[73], i rapporti con l'Autorità di controllo[74]) bene si colloca nella sistematica rinnovata dal principio di responsabilizzazione e dall'approccio basato sul rischio. Lo conferma la clausola di chiusura contenuta nel secondo paragrafo dell'articolo 39, GDPR, specificando che il DPO dovrà eseguire i suoi compiti con un approccio incentrato sulla costante valutazione del rischio, che tenga conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti.

Come abbiamo ricordato nelle pagine che precedono, il GDPR predispone un apparato di principi e regole applicabili a persone fisiche o giuridiche, soggetti pubblici o privati, senza modulazioni nel numero e nella intensità dei requisiti di adeguamento richiesti, salvo che per

[69] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, G. FINOCCHIARO (a cura di), cit., p. 2.

[70] Obbligatorio nel caso in cui il trattamento sia effettuato da una autorità pubblica o da un organismo pubblico, escluse le autorità giurisdizionali nell'esercizio delle loro funzioni; nel caso in cui le attività principali consistano in trattamenti che richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; nel caso in cui le attività principali consistano nel trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e reati, cfr. GDPR, art. 37 par. 1.

[71] A norma dell'art. 39 par. 1 lett. c il DPO ha il compito di fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento.

[72] Nella notifica che il titolare deve inoltrare all'autorità di controllo in caso di violazione dei dati personali, esso è tenuto ad indicare il nome ed i dati di contatto del Responsabile della protezione dei dati, ex art. 33 par. 3 lett. b, GDPR.

[73] «*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti derivanti dal presente regolamento*», cfr. GDPR, art. 38 par. 4.

[74] Tra i compiti del DPO elencati nell'articolo 39 par. 1 del GDPR compaiono: d) cooperare con l'autorità di controllo e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

casi particolari[75]. Vi sono però alcune norme del regolamento europeo e del Codice della *privacy* novellato che riguardano esclusivamente trattamenti effettuati in ambito pubblico. Nel prossimo paragrafo si passeranno in rassegna tali disposizioni, al fine di evidenziare le peculiarità del modello di applicazione della normativa sulla protezione dati alla pubblica amministrazione italiana.

[75] Quali la nomina del Responsabile per la Protezione dei Dati, obbligatoria solo per i soggetti pubblici, oppure nel caso in cui le attività principali svolte dal titolare o dal responsabile comportino il monitoraggio regolare e sistematico degli interessati su larga scala, o le attività principali consistano in trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali e reati, Ved. art. 37 par. 1; si vedano, *ex plurimis*, A. AVITABILE, *Il responsabile della protezione dei dati*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, cit., p. 355 ss.; L. FEROLA, *La "nuova" figura del Responsabile della Protezione dei Dati personali e le sue caratteristiche*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, cit., p. 347 ss.; oppure la tenuta di un Registro dei trattamenti, obbligatoria per titolari del trattamento con più di duecentocinquanta dipendenti, «*a meno che il trattamento che esse effettuano non possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati […] o i dati personali relativi a condanne penali e a reati […]*», ved. L. BOLOGNINI, E. PELINO, (a cura di), *Codice della disciplina privacy*, cit., p. 226 ss..

2.3.3 Le regole per il settore pubblico

Pur essendo il regolamento europeo in materia di *data protection* una normativa generale e orizzontale, applicabile a tutti i soggetti pubblici e privati che possano essere identificati come titolari del trattamento, cionondimeno alcune delle disposizioni del GDPR sono rivolte esclusivamente al settore pubblico, e alcuni adempimenti specifici riguardano solo la pubblica amministrazione[76], mentre nell'ordinamento interno, il d. lgs. n. 101 del 2018, modificando il Codice della Privacy ha introdotto alcune specificazioni riguardanti l'ambito pubblico e corrispondenti agli spazi di intervento lasciati dal legislatore europeo agli Stati membri.

Prima di richiamare alcune di queste disposizioni, sarà necessario fare alcune precisazioni che consentano di delimitare con più chiarezza l'ambito di indagine. Innanzitutto vi è da sottolineare che, il Codice della *privacy*, nella versione antecedente alla novella del 2018, recava una bipartizione tra soggetti pubblici e privati e di conseguenza tra le regole applicabili a taluno o talaltro soggetto. A seguito della introduzione del GDPR e della revisione del Codice, non rileva più la distinzione tra soggetti pubblici e privati quanto piuttosto la finalità perseguita attraverso il trattamento[77]. Prevale un criterio oggettivo per cui la disciplina specifica del trattamento dei dati personali relativa alla esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri si applica a tutti i soggetti, a prescindere dalla qualificazione soggettiva pubblica o privata, ma solo in ragione della finalità perseguita[78]. La base giuridica prevista dall'articolo 6 lettera e) del GDPR («*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il*

[76] Restano esclusi i trattamenti effettuati dalle autorità pubbliche ai fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di minacce alla sicurezza pubblica, i quali non sono disciplinati dal GDPR (e dal d. lgs. n. 196/2003) bensì dalla Direttiva UE n. 2016/680 e dal d. lgs. n. 51/2018. Si veda, in proposito, F. PIZZETTI, *Il sistema normativo di protezione dei trattamenti di dati personali nel quadro europeo e nazionale*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 5 ss.

[77] Cfr. F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 358.

[78] Cfr. G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 203.

titolare del trattamento») può ora essere utilizzata per legittimare trattamenti di dati personali posti in essere da titolari che, pur avendo natura privatistica, sono necessari per l'esecuzione di un compito di interesse pubblico[79].

Secondariamente, occorre considerare che il regolamento non contiene una definizione di interesse pubblico, né di interesse pubblico rilevante. Modafferi ne ha ricondotto il significato alle attività svolte nell'interesse della collettività, e ricorda come nel sistema istituzionale italiano spetti al livello politico il compito di selezionare, tra i molteplici interessi privati, quelli che possano essere soddisfatti dal settore pubblico. Spetterà poi agli apparati amministrativi il dovere di attuare gli indirizzi politici e dunque di dare esecuzione alle indicazioni politiche nell'eseguire i compiti di interesse pubblico[80].

Da ultimo, è d'obbligo un *caveat* relativo alla definizione di pubblica amministrazione. Mancano infatti nel nostro ordinamento definizioni univoche e classificazioni certe[81]. Si tratta di questioni di non poco conto, considerato che l'organizzazione della pubblica amministrazione è soggetta alla riserva di legge di cui all'art. 97 della Costituzione. Nell'Unione europea si è andata affermando una logica delle geometrie variabili, che guarda più alla natura dell'interesse perseguito con il trattamento che a quella del soggetto che lo effettua, con l'effetto di poter considerare pubblico un ente solo rispetto ad alcune categorie di attività da esso svolte[82]. Occorre però tener presente che il c.d. nocciolo duro delle pubbliche amministrazioni è stato individuato nelle amministrazioni statali (ministeri, agenzie), nelle autorità indipendenti, negli enti pubblici non economici, come le università ,nelle regioni, e, per quanto interessa ai fini della presente ricerca, negli enti locali[83], che a pieno titolo possono essere utilizzati come caso di

[79] Cfr. F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 358.

[80] *Ivi*, p. 359

[81] «*In realtà il perimetro della pubblica amministrazione non è tracciato in modo netto né univoco, né rispetto agli organi di livello propriamente costituzionale, né rispetto ai soggetti privati*», cfr. M. CLARICH, Manuale di diritto amministrativo, Il Mulino, Bologna, 2017, p. 321.

[82] Cfr. F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 360.

[83] Cfr. M. CLARICH, Manuale di diritto amministrativo, cit., p. 323.

studio per indagare gli effetti della applicazione della normativa in materia di dati nelle amministrazioni pubbliche.

Venendo alle disposizioni del GDPR, è bene ricordare che alcune di esse sono specificamente rivolte ad autorità pubbliche e organismi pubblici. Ad esempio, l'art. 37, nel disciplinare la designazione del responsabile della protezione dei dati pone i trattamenti effettuati dalle autorità pubbliche e gli organismi pubblici tra quelli che richiedono la nomina obbligatoria di tale figura. L'art 86, con riferimento ai dati personali contenuti in documenti ufficiali in possesso delle autorità pubbliche e degli organismi pubblici, pone l'obbligo di conciliare il diritto di accesso e il diritto alla protezione dei dati personali.

Relativamente alle condizioni di liceità di cui all'articolo 6 all'par. 1 lettere c) ed e), il paragrafo 2 dello stesso articolo accorda agli Stati membri, nell'ambito del loro margine di discrezionalità[84], la possibilità di mantenere o introdurre disposizioni più specifiche, al fine di adeguare l'applicazione delle norme previste nel regolamento medesimo «*determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto*[85]». L'art. 2-*ter* («*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*») attua e specifica la riserva di legge di cui all'art. 6[86], precisando che la base giuridica per il trattamento dei dati comuni in ambito pubblico potrà essere costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali.

L'articolo 9 par. 2 lett. g) prevede invece che il trattamento di categorie particolari di dati effettuato per motivi di interesse pubblico rilevante si basi sul diritto dell'Unione o degli Stati membri, che sia proporzionato rispetto alla finalità perseguita, rispetti il diritto alla protezione dei dati personali e preveda misure specifiche a tutela dei diritti fondamentali degli interessati. L'art. 2-*sexies* («*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*») elenca le materie di interesse pubblico rilevante ai fini

[84] G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 202.

[85] *Ivi*, p. 196.

[86] E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., pp. 67-68.

della applicazione dell'art. 9, par. 2, lett. g), specificando che i trattamenti di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante sono ammessi se previsti dal diritto dell'Unione o da norme di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali. La norma dettaglia anche il contenuto della base giuridica, che deve specificare i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato[87]. Il comma 2 dell'art. 6-*sexies* assume l'aspetto di una sorta di norma "*omnibus*[88]" che reca un dettagliato elenco di ambiti o settori di attività, con riferimento ai quali l'interesse pubblico del trattamento si considera rilevante[89].

La questione della individuazione della base giuridica idonea a legittimare il trattamento dei dati in ambito pubblico merita qualche riflessione. Gli articoli 6 e 9 appena esaminati, elencano le basi giuridiche che rendono leciti i trattamenti dei dati personali comuni e di quelli appartenenti alle c.d. categorie particolari. Come sappiamo, per quanto attiene al settore pubblico, l'articolo 6 paragrafo 1 lettere c) ed e) stabilisce che sono leciti i trattamenti svolti per adempiere un obbligo legale, o per dare esecuzione ad un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, mentre l'articolo 9 paragrafo 2 lettera g) reca una eccezione al divieto generale di trattamento di categorie particolari di dati, nei casi in cui il trattamento sia necessario per motivi di interesse pubblico. Poiché la definizione di "interesse pubblico" è estremamente ampia ed aleatoria, già nella vigenza della direttiva 95/46 il Gruppo di lavoro art. 29 si era espresso sulla portata applicativa di questa base giuridica, chiarendo come ad un campo di applicazione potenzialmente molto vasto dovesse corrispondere una

[87] Cfr. G. MULAZZANI, *Il trattamento di categorie particolari di dati personali, necessario per motivi di pubblico interesse rilevante*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 231.

[88] F. PIZZETTI, *La parte I del Codice novellato*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 108.

[89] Ad esempio la «*tenuta degli atti e dei registri dello stato civile, […], le liste elettorali, nonché rilascio di documenti di riconoscimento*»; materie come «*cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato*»; «*obiezione di coscienza*»; «*attività sanzionatorie e di tutela in sede amministrativa o giudiziaria*»; «*attività socio-assistenziali a tutela dei minori e soggetti bisognosi*»; «*diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano*»; «*compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica*», cfr. E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 69.

interpretazione restrittiva e caso per caso del suo utilizzo. Per questa ragione nella sistematica della Direttiva-madre[90] (e del GDPR[91]), viene previsto un diritto di opposizione esercitabile dagli interessati nei casi in cui non è prevista la manifestazione del loro consenso (dunque ove la base giuridica sia l'interesse pubblico oppure il legittimo interesse[92]). Il Gruppo di lavoro Articolo 29, in un altro documento, ha chiarito che il consenso non può essere ritenuto una base giuridica idonea per il trattamento dei dati personali da parte di soggetti pubblici, in quanto potrebbe non essere stato espresso liberamente, ma piuttosto in una condizione di squilibrio di potere tra il cittadino-interessato e l'autorità pubblica-titolare del trattamento[93]. È stato peraltro osservato in dottrina che l'individuazione, per legittimare il trattamento dei dati, di basi giuridiche alternative al consenso non ha determinato una riduzione della tutela per i diritti degli interessati, in quanto i presupposti alternativi al consenso sono stati adeguatamente rafforzati da una responsabilizzazione dei titolari del trattamento e dalla definizione di un solido quadro sanzionatorio[94]. Le questioni giuridiche poc'anzi profilate stanno rivelando tutta la loro concretezza nella società datificata. Non vi è chi non veda, infatti, che la possibilità o meno di opporsi ad un trattamento dei propri dati personali come quello, pervasivo, che si realizza con la videosorveglianza delle aree pubbliche, ha innalzato i valori in gioco modificandone definitivamente la scala. Di questi epocali cambiamenti ci occuperemo nel quarto capitolo.

[90] All'articolo 14.

[91] All'articolo 21.

[92] Cfr. Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, p. 26.

[93] Ved. Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, WP 259 rev.01, 28 novembre 2017, p. 6, ove si afferma che «*è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato*». Il concetto è espresso anche nel Considerando n. 43 del GDPR.

[94] Cfr. F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 358.

2.4 Apparati amministrativi e *accountability*. Un binomio impossibile?

La *rigidità fortissima* dell'apparato amministrativo dello Stato, insieme alla necessità di modificare procedimenti e organizzazioni posti da norme di legge, quindi non suscettibili di modificazione autonoma da parte dell'amministrazione, sono stati identificati quali responsabili dei rallentamenti, quando non addirittura dei fallimenti, del processo di razionalizzazione dell'organizzazione amministrativa che negli anni Settanta era stato avviato con l'introduzione degli elaboratori elettronici negli uffici della pubblica amministrazione[95]. Anche se con fatica, l'informatica è divenuta però, negli anni successivi, un elemento fondamentale per la revisione dei procedimenti interni alle amministrazioni e, quindi, per la riorganizzazione degli apparati, in quanto l'informatizzazione comporta una organizzazione per processi e per obiettivi[96]. L'avvento di Internet ha poi semplificato le modalità di realizzazione della interoperabilità tra amministrazioni e ha consentito alle pubbliche amministrazioni di estendere notevolmente la loro capacità di raccogliere, conservare, elaborare le informazioni[97].

Oggi l'adozione di un modello organizzativo *privacy* che garantisca alle pubbliche amministrazioni la *compliance* alla normativa in materia di protezione dei dati personali può costituire uno strumento per ottimizzare i processi all'interno di una organizzazione. A differenza però di quanto potrebbe avvenire all'interno di una impresa privata, nelle amministrazioni pubbliche da un lato ogni modifica dell'organizzazione interna può realizzarsi esclusivamente all'interno delle strette maglie imposte dal principio di legalità, e dall'altro gli apparati burocratici rimangono caratterizzati da strutture, personale, prassi operative e cultura istituzionale formatesi lentamente, per stratificazioni successive, e strutturalmente poco permeabili al cambiamento[98].

---

[95] A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, cit., p. 35.

[96] F. MERLONI, *Sull'emergere della funzione di informazione nelle pubbliche amministrazioni*, in F. MERLONI (a cura di) *L'informazione delle pubbliche amministrazioni*, cit., p. 23. Sul tema ved. anche L. VIOLA, *Attività amministrativa e intelligenza artificiale*, in *Ciberspazio e diritto*, vol. 20, n. 62, 1-2/2019, p. 65 ss.

[97] F. MERLONI, *Sull'emergere della funzione di informazione nelle pubbliche amministrazioni*, in F. MERLONI (a cura di) *L'informazione delle pubbliche amministrazioni*, cit., p. 29.

[98] M. CLARICH, *Manuale di diritto amministrativo*, cit., p. 49.

Di conseguenza, l'applicazione delle regole poste dal regolamento n. 2016/679 all'interno degli apparati amministrativi sta comportando notevoli implicazioni sul piano dell'organizzazione, implicazioni che sono strettamente connesse (e proporzionate) alla quantità e alla pluralità di adempimenti richiesti ai singoli enti[99].

Ogni Pubblica Amministrazione è soggetta a vincoli legislativi e regolamentari, oltre che a procedure e prassi interne, che costituiscono l'assetto giuridico a partire dal quale deve essere elaborato un sistema di gestione della *privacy* che risponda ai requisiti posti dal regolamento europeo n. 2016/679. I modelli di *data management* elaborati nelle pubbliche amministrazioni a partire dall'adeguamento alla normativa in materia di protezione dei dati personali non potranno che essere il risultato di diverse e variabili combinazioni tra gli spazi di flessibilità e gli spazi di rigidità dell'apparato amministrativo. Nei casi di rigidità dell'apparato sarà più evidente la declinazione delle regole europee all'interno della struttura, mentre gli spazi di maggiore flessibilità consentiranno all'apparato amministrativo di evolvere verso forme più agili di gestione dei dati, tendendo per quanto possibile verso i principi di gestione dei dati contenuti nei testi normativi europei.

[99] S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, in *Diritto pubblico*, Fascicolo 2, maggio-agosto 2021, p. 635.

2.5 Il modello di applicazione del GDPR agli enti locali.

2.5.1 Peculiarità degli enti locali

La pubblica amministrazione italiana è caratterizzata da una grande varietà di enti ed organismi con differenti finalità e differenti strutture e dimensioni. Molti enti pubblici operano perseguendo singole finalità o governano settori specifici, seppure con incidenza sull'intero territorio nazionale (es. i Ministeri). Gli enti locali al contrario hanno una competenza generale, finalizzata alla cura degli interessi delle comunità e alla gestione del territorio di riferimento[100]. Il caso di studio oggetto di questa ricerca sono, come anticipato, Città metropolitane e Comuni. Ed invero proprio queste due amministrazioni locali offrono la possibilità di analizzare la complessità di elaborazione di un sistema di governo dei dati, alla luce della varietà e del volume dei dati trattati. È nostro intento dimostrare come, a partire dalla elaborazione di regole per la gestione dei dati personali, gli enti locali possono razionalizzare l'intera organizzazione delle procedure dell'ente, comprendendovi progressivamente anche la gestione di dati di ogni natura in ossequio alla legislazione in materia di dati che poi verrà analizzata.

Per quanto attiene ai Comuni l'atto normativo di riferimento è certamente il Testo unico degli enti locali, d. lgs. n. 267/2000[101], un corpo unitario di norme, organizzato e coordinato che offre una lettura coerente del sistema delle autonomie locali[102]. Nella definizione contenuta all'articolo 3, secondo comma, del codice, il Comune è l'ente locale che «*rappresenta la propria comunità, ne cura gli interessi e ne promuove lo sviluppo*». Ad esso sono attribuite autonomia statutaria [103] , normativa, organizzativa e amministrativa, nonché autonomia impositiva e

[100] Sul contenuto definitorio dell'espressione "ente locale" si veda F. STADERINI, P. CARETTI, P. MILAZZO (a cura di), *Diritto degli enti locali*, Wolters Kluwer, Milano, 2022, pp. 7-8. Secondo gli aa. «*[…] tutte le volte che non risulti, dal contesto letterale e sistematico della norma di legge in cui l'espressione è adottata, l'intenzione del legislatore di riferirsi ad una categoria di enti più ristretta e specifica, devesi interpretare l'espressione "enti locali" come comprensiva di ogni ente che operi prevalentemente su un piano locale e che sia destinato a curare interessi e perseguire fini avanti una dimensione locale*».

[101] Decreto legislativo 18 agosto 2000 n. 267, *Testo unico delle leggi sull'ordinamento degli enti locali (TUEL).*

[102] F. STADERINI, P. CARETTI, P. MILAZZO (a cura di), *Diritto degli enti locali*, cit., p. 33.

[103] «*Lo statuto, nell'ambito dei principi fissati dal presente testo unico, stabilisce le norme fondamentali dell'organizzazione dell'ente e, in particolare, specifica le attribuzioni degli organi e le forme di garanzia e di partecipazione delle minoranze, i modi di esercizio della rappresentanza legale dell'ente,*

finanziaria nell'ambito dei propri statuti e regolamenti e delle leggi di coordinamento della finanza pubblica. A norma dell'articolo 13 «*spettano al comune tutte le funzioni amministrative che riguardano la popolazione ed il territorio comunale, precipuamente nei settori organici dei servizi alla persona e alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico […]*». Il Comune svolge inoltre alcuni compiti di competenza statale, come i servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica. Tali funzioni sono svolte dal Sindaco in qualità di ufficiale del Governo[104].

Le città metropolitane, come enti di raccordo tra una città principale e piccoli centri limitrofi, con funzioni di gestione coordinata del territorio e dei servizi, sono il frutto di riflessioni e tentativi risalenti[105], anche se la comparsa nel testo costituzionale quali enti territoriali che compongono la Repubblica[106] avviene solo nel 2001 con la riforma del Titolo V[107]. La disciplina normativa delle città metropolitane è attualmente contenuta nella legge 7 aprile 2014, n. 56[108] (c.d. legge Delrio), che reca la descrizione delle finalità dell'ente e della forma di governo metropolitano. La legge Delrio ha dettato un'ampia riforma in materia di enti locali, prevedendo l'istituzione e la disciplina delle città metropolitane e la ridefinizione del sistema delle province, oltre ad una nuova disciplina in materia di unioni e fusioni di comuni[109].

---

*anche in giudizio. Lo Statuto stabilisce, altresì, i criteri generali in materia di organizzazione dell'ente, le forme di collaborazione fra comuni e province, della partecipazione popolare, del decentramento, dell'accesso dei cittadini, alle informazioni e ai procedimenti amministrativi, lo stemma e il gonfalone e quanto ulteriormente previsto dal presente testo unico***»**, cfr. d. lgs. n. 267/2000, art. 6 comma 2.

[104] Ved. TUEL, art. 14.

[105] Per una ricostruzione si veda Y. GUERRA, *Il ruolo delle città metropolitane alla luce della sentenza n. 240 del 2021: governance metropolitana e funzioni*, in *Forum di Quaderni costituzionali*, 2/2022, pp. 114-117.

[106] Articolo 114 della Costituzione italiana: «*La Repubblica è costituita dai Comuni, dalle Province, dalle Città metropolitane, dalle Regioni e dallo Stato. I Comuni, le Province, le Città metropolitane e le Regioni sono enti autonomi con propri statuti, poteri e funzioni secondo i principi fissati dalla Costituzione*».

[107] Approvata con l. cost. n. 3/2001. Sulla costituzionalizzazione delle Città metropolitane, ved. G. MOBILIO, *Le Città metropolitane. Dimensione costituzionale e attuazione statutaria*, Giappichelli, Torino, 2017, p. 74 ss.

[108] legge 7 aprile 2014 n. 56, *Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni.*

[109] L. VANDELLI, P. BARRERA, P. TESSARO, C. TUBERTINI, *Città metropolitane, province, unioni e fusioni di comuni : la legge Delrio, 7 aprile 2014, n. 56 commentata comma per comma*, Maggioli, Santarcangelo di Romagna, 2014; A. STERPA (a cura di), *Il nuovo governo dell'area vasta : commento alla legge 7 aprile 2014, n. 56 Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni, c.d. legge Delrio aggiornato al d.l. 24 giugno 2014, n. 90 convertito con modificazioni dalla l. 11*

Con le Città metropolitane[110], il legislatore intendeva istituire enti di area vasta dotati di competenze soprattutto strategiche, programmatorie e di coordinamento[111]. A queste competenze si sono però dovute affiancare necessariamente funzioni operative, gestionali e di amministrazione diretta "ereditate" dalle Province[112]. Le finalità istituzionali indicate dalla legge n. 56/2014 (art. 1 comma 2) riguardano la cura dello sviluppo strategico del territorio metropolitano, la promozione e la gestione integrata dei servizi, delle infrastrutture e delle reti di comunicazione di interesse della Città metropolitana, la cura delle relazioni istituzionali afferenti al proprio livello, ivi comprese quelle con le città e le aree metropolitane europee.

Alle finalità si aggiunge l'elenco delle funzioni di adozione del piano strategico, pianificazione territoriale generale, organizzazione dei servizi pubblici di interesse generale, mobilità e viabilità, promozione e coordinamento dello sviluppo economico e sociale, promozione e coordinamento dei sistemi di informatizzazione e digitalizzazione[113]. Ulteriori funzioni possono essere attribuite dallo Stato o dalle regioni, in base ai princìpi di sussidiarietà, differenziazione e adeguatezza.

Dall'intreccio tra funzioni e finalità emerge l'intenzione di istituire un ente che ha la sua ragion d'essere nello sviluppo strategico del territorio e nella promozione integrata di servizi e

agosto 2014, n. 114, Jovene, Napoli, 2014; F. FABBRIZZI, G.M. SALERNO (a cura di), *La riforma delle autonomie territoriali nella legge Delrio*, Jovene, Napoli, 2014.

[110] Sulle Città metropolitane, R. DANIELIS (a cura di), *La città metropolitana: sfide, rischi e opportunità*, EUT, Trieste, 2016; A. LONGO, L. CICIRELLO, *Città metropolitane e pianificazione di area vasta*, Franco Angeli, Milano, 2015; A. LUCARELLI, *La città metropolitana. Ripensare la forma di stato ed il ruolo di regioni ed enti locali: il modello a piramide rovesciata*, in *federalismi.it*, 25 giugno 2014; D. MONE, *Città metropolitane. Area, procedure, organizzazione del potere, distribuzione delle funzioni*, in *federalismi.it*, 9 aprile 2014; A. PATRONI GRIFFI, *Le città metropolitane nel guado costituzionale*, in *federalismi.it*, 6 luglio 2016; L. SALVIA, *Pianificazione strategica e indirizzo politico nelle Città metropolitane alla luce della riforma "Delrio" (legge 56 del 2014)*, in *Osservatorio costituzionale* – AIC, 2, 2016; A. SIMONCINI, G. MOBILIO, *L'identità delle Città metropolitane attraverso i loro Statuti: sintomi di una sindrome "bipolare"?*, in *Le Regioni*, 2016; G.F. FERRARI (a cura di), *Nuove province e Città metropolitane*, Giappichelli, Torino, 2016; L. VANDELLI, *Città metropolitane*, in *Enciclopedia del diritto*, Annali IX, Giuffrè, Milano, 2016; G. TARLI BARBIERI, *Le Città metropolitane: il quadro generale e la forma di governo*, in G.F. FERRARI (a cura di), *Nuove province e Città metropolitane*, Giappichelli, Torino, 2016.

[111] Sulle Città metropolitane nel sistema costituzionale italiano: G. MOBILIO, *Le Città metropolitane. Dimensione costituzionale e attuazione statutaria*, cit.; M.R. RICCI, *La città metropolitana nell'ordinamento giuridico italiano. Percorsi istituzionali e profili di criticità*, Il Mulino, Bologna, 2020.

[112] F. STADERINI, P. CARETTI, P. MILAZZO (a cura di), *Diritto degli enti locali*, cit., p. 101.

[113] Sulle funzioni delle Città metropolitane ved. G. MOBILIO, *Le Città metropolitane. Dimensione costituzionale e attuazione statutaria*, cit., pp. 303-429. Ved. anche F. PIZZETTI, *La riforma degli enti territoriali. Città metropolitane, nuove province e unione di comuni. legge 7 aprile 2014, n. 56 (legge "Delrio")*, Giuffrè, Milano, 2015, pp. 83-92.

reti di comunicazione[114]. Alle città metropolitane si applicano, ove compatibili, le disposizioni in materia di comuni del Testo Unico sull'ordinamento degli Enti Locali (il già citato d. lgs. n. 267/2000) e le disposizioni della legge n. 131/2003 (cd. 'legge La Loggia') sulla potestà normativa degli enti locali. Il sindaco metropolitano è di diritto il sindaco del comune capoluogo. Egli ha la rappresentanza dell'ente, convoca e presiede il consiglio metropolitano e la conferenza metropolitana, sovrintende al funzionamento dei servizi e degli uffici e all'esecuzione degli atti ed esercita le funzioni attribuite dallo statuto; ha potere di proposta per ciò che attiene al bilancio dell'ente.

Come emerge chiaramente dalla breve rassegna appena proposta, gli enti locali si distinguono rispetto ad altri enti pubblici per la varietà delle materie trattate. Ma essi ben possono ben differenziarsi anche tra di loro, per la molteplicità delle configurazioni che ciascun ente locale può assumere al variare delle caratteristiche del territorio, dell'economia, della popolazione. Questa osservazione ha una ricaduta diretta ed evidente nella disciplina *privacy*.

Ciò emerge con particolare chiarezza ove si richiamino i principi-cardine del GDPR, come l'approccio basato sul rischio, l'*accountability* e la *privacy by design*. Nella applicazione del GDPR emergono infatti moltissime questioni rispetto alle misure tecniche e organizzative adeguate che gli enti locali, in qualità di titolari del trattamento, dovrebbero di volta in volta porre in essere in ossequio a tali principi. Quanto appena affermato sarà più comprensibile grazie ad un esempio. I Considerando nn. 75 e 76 del GDPR, insieme all'articolo 35, impongono al titolare del trattamento (dunque all'ente locale), di svolgere una analisi del rischio e, in caso di rischio elevato, una più approfondita valutazione di impatto sulla protezione dei dati personali[115]. In tali casi è previsto che venga svolta una valutazione di impatto *privacy* (DPIA). Dalla lettura del Considerando 75 possono essere tratti elementi che il titolare deve tenere in considerazione per effettuare una valutazione. I rischi per i diritti e le libertà delle persone fisiche possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare, se il trattamento può comportare discriminazioni, furto o usurpazione di identità,

[114] F. PIZZETTI, *La riforma degli enti territoriali. Città metropolitane, nuove province e unione di comuni. legge 7 aprile 2014, n. 56 (legge "Delrio")*, cit., p. 9. Sulle finalità e le funzioni della Città metropolitana ved. anche F. STADERINI, P. CARETTI, P. MILAZZO (a cura di), *Diritto degli enti locali*, cit., p. 102 ss.

[115] A norma dell'art. 35 par.1, un trattamento che preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattate categorie particolari di dati o dati relativi a condanne penali e reati; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali di un vasto numero di interessati.

Vi sono poi ipotesi, individuate dal GDPR, in cui la DPIA deve essere svolta in base ad una presunzione di elevata rischiosità del trattamento. Tra di esse compare la «*sorveglianza sistematica su larga scala in una zona accessibile al pubblico*[116]». Si tratta di una eventualità piuttosto diffusa e comune, in quanto possono ricadere entro questa fattispecie sia la videosorveglianza che il servizio di *free wi-fi*. Emerge in questo caso la necessità di valutare il concetto di "larga scala", in quanto elemento dirimente per considerare un trattamento ad alto rischio e quindi effettuare una valutazione d'impatto *privacy*. Le Linee guida del Gruppo di lavoro art. 29 sui Responsabili della protezione dei dati[117] forniscono un elenco di fattori utili a valutare se un trattamento possa essere considerato "su larga scala". Tali fattori sono: il numero dei soggetti interessati dal trattamento, in termini assoluti oppure espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto del trattamento; la durata, ovvero la persistenza dell'attività di trattamento; la portata geografica dell'attività di trattamento.

Dunque, la analisi del rischio (e del rischio elevato), prodromica alla DPIA, non potrà non tener conto di elementi peculiari di ogni singola realtà in cui si trattino dati personali. A seconda del trattamento valutato, l'area di riferimento potrebbe essere una porzione di un Comune, come ad esempio il centro storico, o una zona industriale, oppure al contrario l'intero territorio

[116] GDPR, art. 35 par. 3 lett. c.

[117] Gruppo di lavoro Articolo 29, *Linee guida sui responsabili della protezione dei dati*, WP 243 rev. 01, 5 aprile 2017.

di una Unione di Comuni. E ancora, il trattamento potrebbe riguardare un servizio gestito da una specifica direzione di un singolo ente, oppure una prestazione fornita da più enti consorziati. Con evidenti conseguenze sulla titolarità (o contitolarità) del trattamento. Le geometrie possono essere innumerevoli, così come le "soluzioni *privacy*" che di volta in volta debbono essere elaborate dai titolari del trattamento.

Gli adempimenti richiesti agli enti locali per adeguare la propria attività alle regole di protezione dei dati personali sono numerosi e toccano ambiti e livelli diversi nell'albero organizzativo[118]. L'adeguamento di un ente locale alle regole poste dal GDPR, specialmente – ma non solo – per quanto attiene alla catena delle responsabilità e delle autorizzazioni al trattamento dei dati personali, non può prescindere, ad esempio, dall'analisi dell'organigramma e delle attribuzioni di ciascun soggetto in esso compreso.

Infatti, chiunque tra i soggetti facenti parti dell'organizzazione del titolare (o del responsabile) abbia accesso ai dati personali non può trattarli se non dietro precisa istruzione da parte del titolare medesimo[119]. Tale regola, letta in combinato disposto con la definizione di "terzo" contenuta nell'art. 4 par. 1 n. 10 del GDPR, fornisce una indicazione fondamentale per la realizzazione di un modello di gestione *privacy*. "Terzo" è il soggetto diverso dall'interessato, dal titolare, dal responsabile e dalle persone autorizzate al trattamento dei dati, è un soggetto, cioè, escluso dalla catena della responsabilità per il trattamento dei dati personali[120]. L'intera sequenza delle responsabilità deve infatti fluire senza soluzione di continuità, e deve essere definita, a cura del titolare, prima che il trattamento dei dati personali abbia inizio. In questo quadro diviene centrale la ricognizione delle mansioni e delle attribuzioni di ciascuna persona fisica, in modo tale che ciascuno, sulla base delle categorie di dati personali effettivamente

[118] Ad esempio l'aggiornamento delle informative riferite ad ogni singolo trattamento, arricchite dalle specificazioni richieste dagli articoli 13 e 14 del GDPR; la nomina (con contestuale assegnazione delle istruzioni) dei soggetti del trattamento; la sottoscrizione di *data transfer agreement* con enti o organizzazioni situati all'estero, con cui si intrattengono rapporti giuridici che implicano anche lo scambio di dati; la tenuta e il costante aggiornamento del registro dei trattamenti, cfr. S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, cit., p. 636.

[119] Cfr. GDPR, art. 29.

[120] Ved. anche *European Data Protection Board*, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 luglio 2021, pp. 28-29.

trattate, possa ricevere dal titolare un atto di nomina (in qualità di persona autorizzata al trattamento o di responsabile) e precise istruzioni.

La procedura di *compliance* appena delineata evidenzia l'importanza, per sviluppare un saldo sistema di gestione dei dati personali, della adesione e corrispondenza dei ruoli *privacy* con gli incarichi che i vari soggetti ricoprono all'interno dell'ente locale. Il Sindaco, i dirigenti, e tutti gli altri dipendenti dell'ente locale (dunque appartenenti all'organizzazione del titolare) nonché alcune categorie di soggetti esterni (società partecipate, consulenti, fornitori di servizi…) per trattare legittimamente i dati personali del Comune o della Città metropolitana debbono essere istruiti in tal senso, oltre che legittimati da un atto di nomina, in mancanza del quale sarebbero qualificati "terzi[121]".

È il diritto amministrativo a delineare e disciplinare l'inquadramento giuridico dei soggetti che rivestono i differenti ruoli all'interno di un apparato pubblico. Per quanto riguarda gli enti locali, le attribuzioni dirigenziali sono regolate innanzitutto dall'articolo 107 del d. lgs. n. 267/2000. Questa norma stabilisce che «*Spetta ai dirigenti la direzione degli uffici e dei servizi secondo i criteri e le norme dettati dagli statuti e dai regolamenti*» (comma 1).

Spettano inoltre ai dirigenti tutti i compiti, compresa l'adozione degli atti e provvedimenti amministrativi che impegnano l'amministrazione verso l'esterno (comma 2). Il comma 3 attribuisce ai dirigenti tutti i compiti di attuazione degli obiettivi e dei programmi definiti con gli atti di indirizzo, tra i quali rilevano in particolare, ai fini della presente disamina, la stipulazione dei contratti, l'assunzione di impegni di spesa, gli atti di amministrazione e gestione del personale, i provvedimenti di autorizzazione, concessione o analoghi.

Il d. lgs. n. 150/2009 ha modificato la disciplina della dirigenza pubblica «*per conseguire la migliore organizzazione del lavoro e assicurare il progressivo miglioramento della qualità delle*

[121] «*In assenza di una formale designazione come incaricati del trattamento, i dipendenti delle pubbliche amministrazioni che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto alle amministrazioni stesse, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento. Tale designazione è, infatti, indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti dell´amministrazione titolare del trattamento (v. art. 19 della legge n. 675/1996)*», cfr. Garante per la protezione dei dati personali, 23 maggio 2000, in Bollettino n. 13, pag. 21, doc. web n. 40229.

prestazioni erogate al pubblico[122]». Il dirigente è divenuto così responsabile della gestione delle risorse umane e della quantità e qualità delle prestazioni dei dipendenti[123]. L'articolo 17 del d. lgs. n. 165/2001 prevede, inoltre che per specifiche e comprovate ragioni di servizio i dirigenti possano delegare, per un periodo di tempo determinato, alcune delle competenze comprese nelle loro funzioni. Alla luce delle citate attribuzioni in materia di gestione del personale e di nomina di soggetti delegati, sui dirigenti grava il compito di dare la corretta collocazione ad ogni nuovo rapporto giuridico di cui sia responsabile; detto altrimenti, ad ogni modifica dell'organigramma dovrà corrispondere un adeguamento del sistema di gestione dei dati personali, innanzitutto attraverso l'aggiornamento della catena dei ruoli *privacy*.

Merita infine di essere evidenziato come l'articolo 110 del TUEL preveda la possibilità che incarichi di funzioni dirigenziali siano affidati mediante contratti a tempo determinato anche al di fuori della dotazione organica dell'ente[124]. È questa una fattispecie in cui le regole del diritto amministrativo e la normativa in materia di *data protection* sembrano confliggere, in quanto il soggetto nominato dirigente, estraneo all'organizzazione del titolare, parrebbe dover essere nominato responsabile esterno. In caso contrario però i dirigenti nominati secondo questa procedura sarebbero gli unici soggetti ad essere inquadrati (e nominati) come se facessero parte dell'organizzazione del titolare, pur senza essere incardinati nell'ente locale.

Gli esempi di cui si è dato conto dovrebbero aver chiarito in che misura l'applicazione dei principi-cardine del GDPR richieda la creazione di un sistema amministrativo di gestione in cui ciascuna componente del sistema agisce in modo coordinato e coerente rispetto all'intera organizzazione[125]. Gli enti locali hanno la necessità di elaborare dei modelli organizzativi capaci di garantire il rispetto delle norme in materia di protezione dati. Tale elaborazione deve però tener conto della struttura dell'ente medesimo e delle regole amministrative che ne disciplinano il funzionamento e lo svolgimento dei compiti istituzionali, prima fra tutte la disciplina contenuta nella legge n. 241/1990 sul procedimento amministrativo. Altrettanto impattante all'interno della pubblica amministrazione è la normativa relativa alla trasparenza amministrativa, che in

[122] Decreto legislativo 27 ottobre 2009, n. 150, *Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttivita' del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*, art. 37.

[123] F. STADERINI, P. CARETTI, P. MILAZZO (a cura di), *Diritto degli enti locali*, cit., p. 237.

[124] Sul punto ved. *Ivi*, pp. 238-239.

[125] S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, cit., p. 639.

più casi arriva a confliggere con la sfera di riservatezza tutelata dalla normativa sui dati personali. Occorre dunque elaborare soluzioni organizzative che ottimizzino la *compliance* senza costituire un freno all'attività amministrativa[126].

Gli enti locali hanno uno strumento privilegiato attraverso il quale predisporre un modello organizzativo *privacy* calibrato sulla realtà specifica. Si tratta del regolamento[127]. Attraverso di esso Comuni e Città metropolitane individuano i ruoli *privacy* (e suddividono così le responsabilità), delineano le regole per il corretto e sicuro trattamento dei dati personali, stabiliscono quali siano le procedure da attivare in caso di violazione dei dati (per un attacco *hacker*, o per un guasto al *server*…). Il governo dei dati avviene attraverso questo strumento-principe.

[126] Sull'impatto dell'applicazione del GDPR nella organizzazione delle PA e nell'attività amministrativa ved. S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione,* cit., che propone delle modalità di organizzazione che tengano conto della complessità giuridica risultante dalla coesistenza di diverse leggi applicabili nel medesimo ambito, senza per questo appesantire ulteriormente la già complessa rete delle procedure in essere.

[127] L'art. 7 del TUEL attribuisce agli enti locali il potere di adottare regolamenti nelle materie di propria competenza ed in particolare per l'organizzazione e il funzionamento delle istituzioni e degli organismi di partecipazione, per il funzionamento degli organi e degli uffici e per l'esercizio delle funzioni. A seguito della riforma del Titolo V la Costituzione italiana prevede che «*I Comuni, le Province e le Città metropolitane hanno potestà regolamentare in ordine alla disciplina dell'organizzazione e dello svolgimento delle funzioni loro attribuite*» (art. 117, comma 6).

2.5.2 Caso di studio: il Regolamento per la protezione dei dati personali della Città metropolitana di Firenze

Il regolamento sulla protezione dei dati personali della Città metropolitana di Firenze approvato con Delibera del Consiglio Metropolitano n. 53 del 23/06/2021 (d'ora in avanti, il regolamento *privacy*) costituisce un esempio di elaborazione di un modello organizzativo *privacy* all'interno di un ente locale. Esso costituisce altresì un modello di governo dei dati. L'oggetto del regolamento *privacy* è la disciplina delle misure organizzative e dei processi interni di attuazione del regolamento europeo n. 2016/679 e del d. lgs. n. 196/2003 relative al trattamento di dati personali per finalità istituzionali della Città Metropolitana. Con un approccio molto simile a quello prescelto per il Codice della *privacy*, anche il regolamento in esame viene concepito come uno strumento volto ad agevolare l'adeguamento dell'ente al GDPR, che rimane la normativa di riferimento. Lo si desume dalla espressa dichiarazione della finalità, contenuta nel primo articolo, ma anche nel richiamo ai principi fondamentali del trattamento operato nell'articolo 2 e nella clausola di raccordo contenuta nell'articolo 4, che rinvia alle definizioni contenute nel GDPR. Nelle prossime righe procederemo ad una ricognizione dettagliata dei contenuti dell'articolato.

Il regolamento *privacy* è suddiviso in una Premessa e in tre parti, rispettivamente dedicate a: "Soggetti e nomine", "Compiti e funzioni", "Procedure". Esso, come specificato nell'articolo 1, poc'anzi richiamato, disciplina le misure organizzative ed i processi interni di attuazione del GDPR e del Codice della *privacy*, relativamente al trattamento dei dati personali effettuato per il perseguimento delle finalità istituzionali della Città metropolitana. Nel secondo paragrafo viene specificato quali siano le attività istituzionali, cioè quelle previste dalla legge, dallo statuto e dai regolamenti, quelle esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente, quelle svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente, quelle disciplinate da un contratto con i soggetti interessati. Per tutti i trattamenti di dati personali effettuati dall'ente nello svolgimento delle attività non sussumibili nelle finalità istituzionali in senso stretto (es. sondaggi di rilevamento del gradimento rispetto ad alcuni servizi) la base giuridica viene individuata nel consenso. L'articolo 1 si chiude con una clausola generale che rinvia, per tutto quanto non espressamente disciplinato nel regolamento, alla

normativa vigente in materia di *data protection*, oltre che ai provvedimenti dell'Autorità indipendente italiana e del Comitato europeo.

Il secondo articolo richiama i principi fondamentali della normativa in materia di dati personali, quali liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione. La Città metropolitana si impegna ad adottare misure tecniche e organizzative adeguate ad impedire il verificarsi di violazioni di dati personali[128] . Dopo aver richiamato i principali rischi attraverso un rimando al Considerando n. 75 del GDPR, la Città metropolitana si impegna a promuovere al suo interno attività di sensibilizzazione e di formazione e aggiornamento del personale, collegando tali attività al duplice scopo di garantire la protezione dei dati personali e di migliorare la qualità dei servizi offerti ai cittadini.

L'articolo 3, a norma degli artt. 9 par. 2 lett. g e 2-*sexies* del Codice della *privacy* specifica quali siano le materie rispetto alle quali la Città metropolitana effettua trattamenti di categorie particolari di dati[129]. Si tratta infatti di ipotesi nelle quali viene superato il divieto generale di trattamento delle categorie particolari di dati personali.

[128] Regolamento privacy, Articolo 2: «*La Città Metropolitana di Firenze adotta le misure tecniche e organizzative adeguate per impedire il verificarsi di violazioni dei dati personali, intese quali violazioni della sicurezza che possano comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'ente*».

[129] Regolamento privacy, art. 3: «*A norma degli Artt. 9 par. 2 lett. g del GDPR e 2 sexies del Codice della Privacy, la Città metropolitana di Firenze effettua trattamenti di categorie particolari di dati personali per motivi di interesse pubblico rilevante nelle seguenti materie:*

- *le attività attinenti alla tenuta delle liste elettorali;*
- *le attività finalizzate all'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nonché dirette all'esercizio del mandato degli organi rappresentativi;*
- *le attività finalizzate all'applicazione della disciplina relativa alla documentazione dell'attività istituzionale;*
- *le attività finalizzate all'instaurazione ed alla gestione dei rapporti di lavoro sia in ordine all'espletamento degli adempimenti previsti in relazione al trattamento economico e giuridico, sia in materia sindacale, di igiene e sicurezza del lavoro;*
- *le attività dirette all'applicazione, anche tramite i concessionari del servizio, delle disposizioni in materia di tributi in relazione ai contribuenti, ai sostituti e ai Responsabili d'imposta, nonché in materia di deduzioni e detrazioni;*
- *le attività finalizzate all'applicazione della disciplina in materia di rapporti con le organizzazioni di volontariato;*
- *le attività svolte in conformità di leggi o di regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.*

L'art. 4 contiene una ulteriore clausola di raccordo con il GDPR rinviando *in toto* al contenuto delle definizioni ivi contenute, che vengono utilizzate con il medesimo significato nel regolamento della Città metropolitana.

La parte del regolamento dedicata ai "Soggetti e nomine" costituisce uno snodo fondamentale della costruzione del modello di attuazione del GDPR nella Città metropolitana. Infatti, dopo aver richiamato nella prima parte i principi fondamentali della materia e le definizioni così come utilizzate nella legge-madre e poi specificato quali siano le basi giuridiche e le finalità che rendono legittimi i trattamenti, dall'articolo 5 in avanti vengono richiamati tutti i c.d. ruoli *privacy* definiti nel GDPR, plasmando tali definizioni in modo che possano aderire adeguatamente alla organizzazione dell'apparato amministrativo dell'ente e ai soggetti che con esso interagiscono. Così il titolare del trattamento è individuato nella Città metropolitana di Firenze, nella persona del sindaco metropolitano pro tempore, soggetto responsabile per decisioni sulle finalità e modalità del trattamento. E' bene ricordare, in proposito, che il Garante per la protezione dei dati personali ha precisato che «*qualora il trattamento sia effettuato nell´ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l´entità nel suo complesso (ad esempio, la società, il ministero, l´ente pubblico, l´associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all´esterno (ad esempio, l´amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)*». [130] Il titolare rappresenta il vertice di un sistema ramificato in cui le responsabilità per il trattamento dei dati personali vengono capillarmente tracciate attraverso atti giuridici in vengono stabilite le responsabilità di ciascun soggetto giuridico e gli atti di autorizzazione al trattamento per le persone fisiche.

L'ipotesi della contitolarità, disciplinata dall'art. 26 del GDPR viene declinata nel modello metropolitano nei casi di esercizio associato di funzioni e servizi e nei casi di compiti la cui gestione è affidata alla Città metropolitana da enti ed organismi statali e regionali[131]. I contitolari

Sono considerati trattamenti effettuati per motivi di interesse pubblico rilevante tutti quelli posti in essere dalla Città metropolitana di Firenze nelle materie indicate dall'art. 2 sexies comma 2 del Codice della Privacy».

[130] Garante per la protezione dei dati personali, Titolare, responsabile, incaricato - Precisazioni sulla figura del 'titolare', 9 dicembre 1997, doc. web. n. 39785.

[131] *«[…] è molto frequente che più amministrazioni si trovino a intervenire nell'ambito del medesimo trattamento di dati personali. Tale circostanza fa sì che si instauri una pluralità di relazioni fra*

debbono chiarire tramite accordo interno i rispettivi ruoli e i rapporti con gli interessati che non debbono necessariamente essere condivisi equamente, ma possono seguire criteri di allocazione specificamente ritagliati sull'obiettivo di ciascuno[132]. L'art. 6 comma 3 individua nella pubblicazione nel sito istituzionale la modalità adeguata per portare alla conoscenza degli interessati il contenuto essenziale dell'accordo di contitolarità.

A fronte della scelta del GDPR di disciplinare esclusivamente i rapporti giuridici del titolare del trattamento con soggetti esterni alla sua organizzazione, che trattano dati per suo conto (responsabili esterni ex art. 28 GDPR), la declinazione del regolamento europeo nella struttura organizzativa della Città metropolitana ha comportato la scelta di disciplinare i ruoli dei responsabili interni e di quelli esterni, in modo da rispettare l'organigramma interno all'ente ed ottimizzare le scelte organizzative al fine di massimizzare la protezione dei dati personali. A tale fine il regolamento *privacy* prevede che i dirigenti della Città metropolitana siano nominati responsabili interni, ciascuno per la funzione di propria competenza.

Nell'articolo 7 viene individuato anche lo strumento di nomina: "*I responsabili interni sono designati dal Sindaco metropolitano con il decreto di attribuzione delle funzioni dirigenziali*". La norma prevede che i responsabili posseggano i requisiti (adeguati conoscenza specifica, esperienza, capacità ed affidabilità) che vengono assicurate a seguito di adeguata formazione. Inoltre i nomi dei responsabili interni vengono pubblicati nella sezione Amministrazione trasparente del sito istituzionale. Il raccordo è evidentemente con l'articolo 107 e l'articolo 109 del TUEL. La norma appena descritta riveste particolare importanza per comprendere la sistematica dell'intero regolamento *privacy*. Infatti emergono la logica della razionalizzazione delle procedure (la nomina dei responsabili interni avviene attraverso il decreto di attribuzione delle funzioni dirigenziali), l'utilizzo virtuoso di strumenti disciplinati da altre normative (la pubblicazione dei nominativi nella sezione Amministrazione trasparente) e la sistematica sottesa all'interno articolato, ovvero l'applicazione dei principi cardine della normativa di protezione dati. Invero le caratteristiche richieste ai responsabili interni, insieme

i diversi soggetti che intervengono sui trattamenti, connotando questi ultimi in un senso che si potrebbe definire plurisoggettivo», cfr. S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, cit., p. 643.

[132] N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data protection officer*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 132.

alla previsione delle attività di formazione, costituiscono la declinazione del principio di *accountability*, per cui il titolare adotta misure adeguate a ridurre il rischio.

Anche l'articolo 8, relativo alla nomina di responsabili esterni, segue la medesima logica di razionalizzazione delle procedure e di declinazione del GDPR sulle caratteristiche dell'amministrazione locale. Vi si specifica infatti che «*Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o altri strumenti giuridici dalla legge con cui è affidata a tali soggetti esterni la gestione di attività e servizi per conto della Città metropolitana, è prevista espressamente la nomina degli stessi soggetti affidatari quali responsabili esterni del trattamento dei dati personali connessi alle attività istituzionali affidate*». In questi casi, spetta al titolare assicurarsi che il responsabile utilizzi misure adeguate rispetto al tipo di trattamento che deve porre in essere[133].

I dipendenti nello svolgimento delle proprie mansioni sono nominati incaricati al trattamento. La nomina avviene da parte del responsabile interno della propria unità organizzativa (cioè il dirigente nominato ex artt. 107 e 109 del TUEL), e sulla base del principio della *privacy by design* avviene in sede di predisposizione degli atti di micro-organizzazione, facendo riferimento alle attività di trattamento indicate nel registro dei trattamenti.

Dalla lettura dell'articolo 9 si può cogliere il collegamento tra le mansioni assegnate al dipendente, la corrispondente nomina *privacy* e le attività di trattamento che debbono essere elencate nell'apposito registro predisposto a norma dell'art. 30 GDPR. Oltre al richiamo all'attività di formazione, appare centrale il terzo comma, nel quale vengono disciplinati gli aspetti informatici dell'accesso ai dati da parte dei dipendenti dell'ente, in particolare nei casi di cessazione del servizio o cambio di mansioni. Il responsabile dei Servizi Informativi viene incaricato di predisporre «*una modalità operativa che assicuri l'accesso informatico dell'incaricato ai soli dati personali necessari a svolgere le mansioni riportate nell'atto di nomina. In particolare, provvede ad una mappatura di tutte le autorizzazioni all'accesso informatico ai dati dell'ente, che viene aggiornata a seguito di ogni modifica degli atti di incarico. A tal fine, i*

[133] Egli infatti è responsabile anche nel caso in cui non siano state preventivamente effettuate tutte le verifiche necessarie in ordine all'adeguatezza delle misure tecniche ed organizzative utilizzate, cfr. N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data protection officer*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 137.

responsabili interni competenti comunicano al responsabile dei Sistemi Informativi ogni modifica relativa alle mansioni dei dipendenti che comporti una variazione nelle attività di trattamento dei dati personali a cui gli stessi sono autorizzati». L'articolo 10 chiarisce che la qualifica di interessati riguarda non solo i cittadini metropolitani, ma tutte le persone a cui i dati personali si riferiscono: dipendenti dell'ente, non residenti, turisti, fruitori dei servizi *online*, in perfetta aderenza a quanto indicato nel GDPR che nel Considerando n. 1 ricorda che «*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*».

L'articolo 11 descrive la figura del responsabile della protezione dei dati personali, nominato con decreto motivato del Sindaco metropolitano e scelto nella compagine dirigenziale o esternamente all'ente. L'articolo disciplina le ipotesi di incompatibilità dell'incarico (il DPO interno può ricoprire altri ruoli «*purchè non generino conflitti di interesse con la sua funzione*»). L'articolo 12 disciplina la nomina dell'Amministratore di Sistema, in ossequio ai provvedimenti del Garante del 27.11.2008 e 25.6.2009 e ss.mm.ii.. Vi si stabilisce che la nomina viene effettuata dal Dirigente dei Sistemi Informativi e che dovrà fornire supporto ed assistenza al DPO.

Alla assegnazione dei ruoli privacy segue l'attribuzione nella seconda parte del regolamento *privacy*, di compiti e funzioni.

Vale la pena di evidenziare come il modello organizzativo *privacy* della Città metropolitana di Firenze preveda una suddivisione a cascata delle responsabilità di organizzazione, supervisione e controllo. Il titolare dirama le direttive ed effettua verifiche periodiche sul rispetto delle istruzioni impartite ai responsabili. Ai responsabili interni viene invece affidato il compito di svolgere tutte le attività di competenza del titolare nel proprio ambito di competenza, in ossequio all'art. 107 del TUEL che assegna ai dirigenti la capacità di impegnare l'ente verso l'esterno.

Infatti, i responsabili interni si occupano di effettuare le nomine dei dipendenti appartenenti al proprio ufficio come incaricati al trattamento, vincolandoli alla riservatezza e curandone la formazione; si occupa di adempiere gli obblighi di informazione degli interessati, facendo così in modo che le informative somministrate siano dettagliate e pertinenti rispetto ad ogni singolo ambito di attività dell'ente; nomina i responsabili esterni e stipula accordi per l'accesso alle banche dati per l'attività di pertinenza del proprio ufficio; individua ed attua, insieme al titolare del trattamento, misure adeguate per garantire la sicurezza dei trattamenti;

collabora con il titolare del trattamento per dare seguito alle richieste per l'esercizio dei diritti degli interessati, relative a trattamenti di dati personali posti in essere nel proprio ufficio; compila la sezione di competenza del proprio ufficio del registro dei trattamenti di cui all'art. 30 del GDPR della Città metropolitana di Firenze; cura la pubblicazione nel sito della Città metropolitana di Firenze del contenuto essenziale degli accordi di contitolarità di propria competenza; riferisce al Titolare del trattamento e al DPO ogni violazione di dati personali di cui viene a conoscenza senza ritardo e li assiste nel procedimento di notifica della violazione al Garante; fornisce assistenza al titolare del trattamento per le comunicazioni all'interessato di violazione dei dati personali nei casi previsti dall'articolo 34 GDPR; nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, sentito il DPO, effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (*Data Protection Impact Assessment*, DPIA), ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del trattamento medesimo.

Per quanto riguarda i responsabili esterni del trattamento, il regolamento *privacy* fa rinvio all'articolo del 28 del GDPR ma si specificano aspetti pratici quali le modalità di comunicazione al titolare, i termini per la comunicazione di una violazione dati, la restituzione o cancellazione dei dati alla fine del rapporto.

Nella terza parte del regolamento, dedicata alle procedure, l'art. 19 disciplina la tenuta e l'aggiornamento del registro dei trattamenti. Le regole di tenuta del documento vanno anche in questo caso declinate sull'apparato e sulla suddivisione organizzativa dell'ente, e devono rispondere alla necessità di svolgere e periodicamente aggiornare una analisi capillare di tutti i flussi di dati afferenti all'amministrazione.

Il regolamento *privacy* specifica che il registro, in formato digitale, è conservato presso la Segreteria generale dell'ente e deve essere aggiornato almeno con cadenza annuale. La compilazione di ciascuna sezione, corrispondente alle varie Direzioni in cui la Città metropolitana è suddivisa, è affidata al responsabile interno competente. L'adeguamento dell'apparato amministrativo alle regole in materia di protezione dati personali, così come delineate nel regolamento 2016/679 e nel Codice della *privacy* novellato, costituisce uno straordinario strumento di razionalizzazione di ogni singola Pubblica Amministrazione. Infatti la normativa

prevede il controllo del ciclo di vita del dato personale, dal momento della raccolta, attraverso le varie possibilità di trattamento, fino alla conservazione e cancellazione dello stesso. Questo controllo avviene attraverso la corretta applicazione dello strumentario *privacy* previsto nel GDPR. Il registro dei trattamenti, previsto dall'articolo 30 del GDPR, può rappresentare lo strumento di raccordo di tutto il sistema. Esso prevede che il titolare componga un elenco di tutti i trattamenti dei dati personali effettuati nella propria organizzazione, specificando per ciascuno di essi quale sia la base giuridica che legittima il trattamento, quali le finalità, oltre a specificare termini di conservazione, eventuali trasferimenti all'estero dei dati, misure approntate per garantire la sicurezza dei dati, eventuali destinatari dei dati stessi.

Come il regolamento stesso invita a fare, il registro dei trattamenti può essere arricchito di più informazioni rispetto a quelle minime indicate nella norma. Si tratta di un processo virtuoso che dovrebbe consentire, via via, al titolare di ottenere una mappatura completa dei trattamenti, dei soggetti coinvolti, delle basi normative che li legittimano, dei tempi massimi di conservazione. Poiché la maggioranza dei dati trattati negli enti locali è di natura personale la compliance al GDPR impone una ricognizione di quasi tutti i flussi di dati. Se si aggiunge a questo che anche i nomi di eventuali professionisti coinvolti, i recapiti contenenti riferimenti a persone fisiche, i nomi di referenti all'interno della PA o nelle Società private che a vario titolo operano con la Pubblica Amministrazione sono dati personali, restano al di fuori del registro pochissime tipologie di trattamento.

C'è di più. Riguardando ogni trattamento di dati personali che avviene all'interno dell'organizzazione del titolare, la mappatura di tali trattamenti riguarderà sia le attività che l'ente svolge all'interno delle sue finalità istituzionali, sia l'organizzazione interna dell'ente medesimo. Cioè a dire che la spinta alla razionalizzazione dei processi e delle procedure che viene come conseguenza della mappatura di tutti i trattamenti di dati personali, riguarderà necessariamente sia l'attività di indirizzo politico (gestione dei dati personali del Consiglio e della Giunta, oltre che delle sedute, provvedimenti ecc), sia l'organigramma dell'ente (alle mansioni di ogni impiegato dell'ente debbono corrispondere istruzioni precise sui trattamenti di dati personali che lo stesso è autorizzato a svolgere), sia l'attività amministrativa ordinaria (procedimenti amministrativi, obblighi di trasparenza, bandi e gare…), sia l'erogazione di servizi (asili nido, trasporto pubblico, mense scolastiche, anagrafe…), sia la realizzazione di lavori pubblici (edilizia pubblica, opere di restauro, infrastrutture…).

Come si può facilmente intendere, la ricognizione di tutti i trattamenti di dati personali svolti all'interno di un ente, e la sistematizzazione di tali informazioni all'interno di un registro, consente di avere una visione di insieme non solo sui trattamenti di dati personali, ma sull'intera attività di un ente locale. L'obbligo di svolgere un tale adempimento costringe l'amministrazione a raccogliere informazioni per colmare eventuali lacune rispetto ai flussi di dati, in particolare in merito ai tempi di conservazione. Parafrasando le parole che Alberto Predieri ebbe ad utilizzare parlando della introduzione degli elaboratori elettronici nell'amministrazione dello Stato, possiamo riferirci agli strumenti di compliance al GDPR, ed in particolare al Registro dei trattamenti affermando che *la razionalizzazione* da essi *imposta porta innanzitutto alla conoscenza del reale funzionamento delle organizzazioni e dei procedimenti vigenti. Ad essa consegue la loro riconsiderazione, che deve essere effettuata già nello studio per l'analisi dei processi e la loro tendenziale unificazione, imposta dalla razionalità del sistema informativo che può portare a semplificare taluni processi, ad abolirne taluni segmenti e, al limite l'intero processo, quando si costati che anziché automatizzarlo esso deve essere abolito*[134].

Tra le procedure disciplinate, oltre alla tenuta del registro dei trattamenti, vi è la procedura da seguire in caso di violazione dei dati personali. Innanzitutto viene disciplinata la catena delle comunicazioni: l'incaricato che venga a conoscenza di un *data breach* ne dà comunicazione al responsabile del proprio ufficio o, se la violazione riguarda un trattamento non afferente al proprio ufficio, al DPO. Il responsabile deve riferire al titolare, che provvederà alle eventuali comunicazioni al Garante e agli interessati, mentre la tenuta del registro delle violazioni viene affidata al DPO.

L'articolo 20 contiene la procedura per la corretta predisposizione e somministrazione delle informative[135] e deve essere letto in combinato disposto con gli articoli 14 e 16. Infatti il responsabile interno, con l'aiuto degli impiegati assegnati al suo ufficio, garantisce che gli interessati ricevano idonea informativa per i trattamenti afferenti al suo ambito di competenza. L'ultimo paragrafo contiene una clausola di raccordo con la compilazione del registro dei trattamenti: ai trattamenti mappati all'interno del registro, ed aggiornati in base a un criterio di competenza, corrispondono gli atti di nomina degli incaricati alle singole mansioni di ufficio che

[134] A. PREDIERI, *Gli elaboratori elettronici nell'amministrazione dello Stato*, cit., p. 36.

[135] Sugli obblighi di informazione in capo alle PA cfr. S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, cit., p. 640.

comportino il trattamento dei dati personali, e il contenuto delle informative fornite agli interessati, sempre suddivise per area tematica.

La presentazione di una istanza di esercizio dei diritti degli interessati innesca un procedimento amministrativo che presuppone la definizione previa di un adeguato assetto organizzativo idoneo a gestire e curare l'istanza[136]. Per questa ragione il regolamento *privacy* prevede tutti i passaggi amministrativi volti a rispondere alla richiesta; come è stato osservato, la predeterminazione dei criteri in base ai quali individuare gli organi chiamati ad attivarsi per rispondere alle richieste degli interessati si dà attuazione ai principi di imparzialità e di *privacy by design* e *by default*[137]. Nello specifico, la procedura per la gestione dei diritti degli interessati pone in capo al dirigente dell'URP il compito di predisporre e mettere a disposizione degli interessati la modulistica per l'esercizio dei diritti. L'apposito registro contenente tutte le richieste e compilato e conservato a cura dell'URP.

Il modello di applicazione del GDPR nella Città metropolitana prevede dunque una suddivisione di compiti e delle responsabilità basata su due direttrici: da una parte la struttura dell'organigramma, in modo da poter attraverso una serie di procedure garantire che tutti gli adeguamenti siano correttamente eseguiti e monitorati, senza lacune o aree prive di regolamentazione e dall'altra la costante e completa mappatura dei trattamenti dei dati personali dell'ente, effettuata attraverso l'aggiornamento sistematico del Registro dei trattamenti, contenente tutte le informazioni di cui all'art. 30 del GDPR.

L'articolo 22 del regolamento *privacy* è una norma molto densa, che contiene le procedure relative alla sicurezza dei trattamenti. Esso prevede la suddivisione in diversi livelli di attribuzioni. Il dirigente dei Sistemi Informativi è responsabile per la sicurezza informatica. Il titolare garantisce la sicurezza fisica dei luoghi attraverso la verifica della presenza di misure anti-incendio, la registrazione degli accessi fisici, l'installazione di infissi ignifughi e dotati di serratura. Ciascun responsabile interno si accerta che nel suo ufficio siano applicati sistemi di autenticazione per l'utilizzo dei dispositivi, sistemi di autenticazione con diversi livelli di visibilità, idonei sistemi di protezione degli archivi cartacei.

[136] S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, cit., p. 645.

[137] *Ivi*, p. 659.

Di notevole rilievo la disposizione dell'art. 23, nella quale si rileva un altro punto di raccordo tra la normativa e le procedure del diritto amministrativo e il diritto della protezione dati personali. Invero la norma contiene un rinvio, per quanto attiene alla conservazione e cancellazione dei dati, a quanto indicato nel massimario di scarto dell'ente. Viene precisato che gli incaricati hanno il dovere di distruggere i fogli di lavoro necessari allo svolgimento delle mansioni d'ufficio, al termine delle operazioni che ne hanno richiesto l'utilizzo. Un ulteriore raccordo con un'altra normativa di assoluta rilevanza per la pubblica amministrazione è contenuto nell'art. 24 ove si precisa che «*La Città metropolitana di Firenze tratta i dati personali contenuti in atti e documenti amministrativi che devono essere pubblicati nel sito istituzionale dell'ente secondo quanto previsto dal regolamento in materia di accesso documentale, civico e generalizzato e dalla normativa vigente in materia di trasparenza amministrativa*». La norma di chiusura del regolamento afferma che la Città metropolitana di Firenze sostiene e promuove ogni strumento di sensibilizzazione rispetto al consolidamento della protezione dei dati personali e per il miglioramento della qualità dei servizi offerti ai cittadini metropolitani.

Il regolamento sulla protezione dei dati personali della Città metropolitana appena esaminato costituisce un punto d'arrivo nella elaborazione di un modello organizzativo *privacy* all'interno degli enti locali. Esso tiene conto delle peculiarità dell'ente, dei fini istituzionali che lo stesso persegue così come indicati dalla legge; tiene conto, inoltre, della necessità di applicare altre normative specifiche e in parte di segno opposto, come quella sulla trasparenza amministrativa e sull'accesso. In tal senso vengono inseriti corretti rimandi e clausole di coordinamento. Infine il regolamento contiene la declinazione di principi e regole posti dal GDPR nella accezione più adeguata alla Città metropolitana. Attraverso la enucleazione di un modello organizzativo *privacy* si può verificare come una parte consistente dei dati che vengono trattati dall'ente è sottoposta, in tutto il suo ciclo vitale, a regole e procedure che ne garantiscono il trattamento secondo legge, e che garantiscono i diritti e le libertà delle persone fisiche cui i dati si riferiscono.

2.6 Alcune considerazioni sul GDPR come ausilio al *data management* negli enti locali

Il regolamento sulla protezione dei dati personali della Città metropolitana di Firenze costituisce l'intelaiatura del sistema di gestione privacy dell'ente locale e rappresenta al contempo un modello applicativo del GDPR in una pubblica amministrazione. Infatti, il regolamento *privacy* offre almeno tre differenti livelli di lettura. Rappresenta il passaggio obbligato dalla lettera del regolamento europeo 2016/679 alla pratica, rispetto alla quale ad ogni adempimento corrisponde una procedura in cui debbono essere esplicitati soggetti responsabili, tempi di azione, modalità di esecuzione; rappresenta secondariamente la declinazione del GDPR all'interno di un apparato solido, rigido, ancorato alla legge che ne definisce in dettaglio finalità, limiti, modalità di funzionamento. Il modello applicativo del GDPR, dunque, in questo caso si muove entro due assi: da una parte la valutazione del rischio e la scelta di misure adeguate da parte del titolare del trattamento, dall'altra le regole e gli apparati amministrativi, non passibili di modifiche o aggiustamenti se non per via legislativa.

Con il conseguente accrescimento del valore strategico di strumenti come i Regolamenti, i decreti di attribuzione delle funzioni, gli atti di micro-organizzazione. Quest'ultima osservazione appare essenziale per comprendere in che misura e con quale pervasività la regolazione europea del trattamento dei dati abbia modificato apparati e prassi consolidati, e sottoposti a riserva di legge dall'articolo 97 della Costituzione[138]. Il terzo livello di lettura del regolamento, che rileva nella economia del presente lavoro in maniera particolare, riguarda l'effetto di razionalizzazione nel governo dei dati dell'ente che viene impresso grazie all'applicazione del regolamento in materia di dati personali. Sappiamo infatti che la stragrande maggioranza dei dati in possesso degli enti locali è costituita da dati personali. Molto spesso nella realtà dei *Big Data* e degli algoritmi, dati personali e non personali sono difficilmente scindibili. Come si vedrà nel prossimo capitolo, il regolamento 2019/1807 sui dati non personali prevede che in caso di insiemi di dati misti prevalga l'applicazione delle regole del GDPR.

[138] «*I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione*», Costituzione italiana, art. 97, comma 1.

Ciò significa che il patrimonio informativo di una Città metropolitana sarà in gran parte costituito da dati il cui trattamento sarà disciplinato dal regolamento *privacy*. Ebbene, la sistematica dell'articolato poc'anzi esaminato consente di seguire e verificare l'intero ciclo di vita dei dati personali raccolti e trattati nell'ente, dal momento della somministrazione delle informative, sino alla cancellazione in ossequio alle regole del massimario di scarto, passando attraverso tutte le attività tipiche dell'ente, rispetto alle quali i trattamenti sono tutti mappati nell'apposito registro e sottoposti alle responsabilità di incaricati, responsabili, e del titolare. Il rispetto delle procedure e dei termini individuati nel GDPR e nel regolamento *privacy* offre alla Città metropolitana un formidabile strumento di razionalizzazione e di governo del patrimonio informativo.

Quanto appena descritto vale per ciascun titolare del trattamento, pubblico o privato, così come la spinta alla razionalizzazione dell'organizzazione vale in entrambi gli ambiti. Come è noto, però, mentre il settore privato non è soggetto a vincoli di nessun genere e nei casi più virtuosi società private hanno colto l'opportunità che il GDPR ha posto loro dinnanzi per rivedere tutti i processi aziendali, alleggerirli, eliminare duplicazioni e passaggi farraginosi, nel settore pubblico il rispetto di norme di legge e l'impossibilità per la singola amministrazione di intervenire, se non ad un livello superficiale, di fatto riducono la possibilità che gli effetti ottenuti siano di impatto notevole. Infatti, oltre alle leggi che disciplinano l'azione amministrativa, il procedimento amministrativo, i documenti amministrativi ecc, anche la parte di norme che attiene alla digitalizzazione della pubblica amministrazione (primo fra tutti il CAD), pur imponendo decisi passi in avanti per quanto attiene alla amministrazione digitale, alla digitalizzazione, al passaggio al *cloud*, alla valorizzazione del patrimonio informativo pubblico, anch'essa costituisce un ulteriore *layer* di regole da rispettare. Con il risultato che il funzionario amministrativo che intenda rivedere l'organizzazione del proprio ente dovrà progressivamente verificare il rispetto del diritto amministrativo "analogico", l'adempimento di quanto contenuto nel Codice dell'amministrazione digitale, e poi applicare il principio di *accountability* come descritto del GDPR alla complessa e stratificata macchina amministrativa risultante da queste norme. Risultato questo non agevole da ottenere, ma comunque possibile, come mostrano esempi virtuosi, quale la Città metropolitana di Firenze.

Anche grazie alla collaborazione con il Dipartimento di Scienze Giuridiche dell'Università di Firenze, la Città metropolitana ha intrapreso un percorso di adeguamento al GDPR che ha

preso le mosse da una intensa attività di formazione del personale. Successivamente, attraverso una costante opera di sostegno dell'Unità *privacy* e con il supporto del DPO ciascuna direzione ha effettuato una ricognizione di tutti i trattamenti di dati personali effettuati al proprio interno e li ha inseriti all'interno del *format* di registro scelto per tutto l'ente. In questa fase di compilazione sono emersi numerosissimi nodi "materiali", quali duplicazioni di documenti cartacei e digitali, mancanza di un termine per la cancellazione dei dati, tendenza alla conservazione "per sicurezza", e ancora più numerosi nodi giuridici, come la differenza tra documenti e informazioni (cioè tra dati inseriti in documenti e dati strutturati e conservati in apposite banche dati)[139], la difficoltà tecnica di stabilire se un dato sia anonimizzato oppure no, la gestione delle richieste di accesso documentale, civico, generalizzato, l'imputabilità di trattamenti di dati personali ad interi uffici piuttosto che a singole persone fisiche, l'identificazione dei trattamenti rientranti nelle finalità dell'ente, posti in essere per interesse pubblico, e di quelli invece che richiedono il consenso dei cittadini come base giuridica. Il lungo percorso di compilazione del registro dei trattamenti ha consentito di individuare tutte le figure coinvolte, titolari, contitolari, responsabili, incaricati, e di poter verificare la sussistenza degli atti giuridici di nomina; anche le informative sono state tutte riviste sulla base dei trattamenti emersi e delle informazioni ad esso collegate; infine, l'ente ha elaborato il proprio regolamento *privacy*, contenente gli esiti dell'approfondito percorso di revisione appena descritto.

L'evolvere continuo della Società digitale verso forse sempre maggiori di commistione della vita analogica e di quella datificata, gli strabilianti avanzamenti della ricerca e della innovazione tecnologica, in particolare nel campo dell'Intelligenza artificiale, la competizione economica globale, l'avanzare sulla scena di soggetti non statali dotati di un controllo talmente esteso della comunicazione, dell'informazione e dei servizi da essere definiti "poteri privati", seduti allo stesso tavolo degli Stati, in ragione della loro capacità di determinare, in base alle scelte operate, la disponibilità o meno di un servizio per i cittadini, o il corretto svolgimento (o meno) della vita democratica (*in primis* attraverso la formazione dell'opinione pubblica) , sono gli elementi fattuali che il diritto deve descrivere e regolare, e costituiscono il contesto in cui i soggetti pubblici devono agire. Il questo scenario, la protezione delle persone fisiche rispetto al

[139] «*Da meri archivi mantenuti staticamente su supporti cartacei, le informazioni in mano pubblica, organizzate e strutturate digitalmente, hanno assunto nel loro complesso la rinnovata veste dinamica di banche dati*», cfr. G. CARULLO, *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, cit., pp. 184-185.

trattamento dei propri dati personali appare di fondamentale importanza, e al contempo rappresenta la base valoriale e giuridica su cui edificare la necessaria architettura normativa con la quale governare la realtà e i suoi fenomeni, nei rapporti internazionale come nella amministrazione delle città. Questa è la strada intrapresa dall'Unione europea, alla cui strategia digitale è dedicato il prossimo capitolo.

CAPITOLO 3 – LA STRATEGIA DIGITALE EUROPEA

3.1 Il quadro normativo (cenni)

Di fronte al sempre crescente impatto dei *Big Data* nella società e nell'economia, l'Unione europea si è dapprima dotata di alcuni atti normativi che hanno regolato il trattamento dei dati personali e non personali nella realtà digitale. Tra questi il c.d. Pacchetto Protezione Dati, pubblicato in Gazzetta Ufficiale dell'Unione europea il 4 maggio 2016 (costituito dal regolamento n. 2016/679 sul trattamento dei dati personali e dalla direttiva n. 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati[1]), il successivo regolamento n. 2018/1807 sui dati non personali, il regolamento sulla cybersicurezza (Reg. n. 2019/881). La direttiva n. 2019/1024, sostituendo direttiva 2003/98/CE e la direttiva 2013/37/UE ha ridisegnato il quadro relativo all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

Nel 2020 la Commissione europea ha inserito le iniziative appena citate in un contesto più ampio ed organico, una vera e propria strategia digitale europea. La definizione di un complesso apparato di norme, relative all'utilizzo dei dati, comporta per tutti i soggetti coinvolti una attenta verifica di obblighi ed opportunità. Infatti la realizzazione del disegno tratteggiato dalla Commissione rappresenta un deciso passo in avanti per lo sviluppo del Mercato Unico europeo e per l'intera società, che potrà giovare dei benefici della innovazione basata sui dati.

L'analisi delle linee essenziali della strategia digitale europea e dei suoi principali prodotti normativi consentirà di avere una visione d'insieme che sia prodromica alle riflessioni sulla *governance* dei dati da parte degli enti locali. Nei successivi paragrafi, dunque, si procederà

[1] «*Obiettivo principale della direttiva è innalzare la garanzia della privacy dei cittadini quando interviene un trattamento dati per motivi giudiziari e di polizia, ma anche facilitare notevolmente lo scambio e l'uso delle informazioni utili per il contrasto a fenomeni come criminalità e terrorismo. Essa si presenta quindi come lex specialis rispetto al Regolamento generale sulla protezione dei dati, di cui declina principi e obblighi con riguardo allo specifico contesto delle attività di polizia giudiziaria*», cfr. G. GARDINI, *Le regole dell'informazione. L'era della post-verità*, cit., p. 332.

ad una rassegna dei principali documenti ed atti normativi europei in materia di dati. Si cercherà altresì di evidenziare gli aspetti più rilevanti e peculiari che differenziano la disciplina del settore pubblico da quella generale.

3.2 La strategia europea per i dati

Il documento "*A European Strategy for Data*[2]" pubblicato il 19 febbraio 2020, espone in maniera compiuta l'approccio europeo alla *global data economy*. L'Europa può divenire un modello di riferimento per una società in cui i dati siano sfruttati per adottare decisioni migliori ed aumentare così la competitività delle imprese di tutte le dimensioni e per rispondere alle sfide sociali, climatiche, ambientali, contribuendo allo sviluppo di società più sane, prospere e sostenibili[3].

A differenza del modello statunitense, in cui le scelte sono lasciate in mano al settore privato, senza che vi sia un freno alle concentrazioni in capo a pochi soggetti economicamente potentissimi, e del modello cinese caratterizzato dalla sorveglianza governativa e dalla presenza delle *Big Tech*, con scarse garanzie per i cittadini, l'Unione propone una *European way* caratterizzata dal bilanciamento tra il massimo utilizzo dei dati per lo sviluppo economico del Mercato Unico da una parte, e da altissimi standard etici, di privacy, di *safety* and *security* dall'altra[4]. L'essere umano rimane al centro del progetto europeo di sviluppo digitale, all'interno di una strategia che promuova il valore dei dati nella plurima dimensione personalistica, economica e sociale[5]. L'obiettivo è quello di creare uno spazio unico europeo di dati, in cui il diritto dell'UE sia applicato con efficacia, all'interno del quale le imprese abbiano accesso «*a una quantità pressochè infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore*[6]».

Perché questo si realizzi è necessario consolidare un clima di fiducia da parte dei cittadini nei confronti delle innovazioni basate sui dati, e un contesto politico attraente e favorevole, che

[2] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020.

[3] *Ivi*, pp. 1-3.

[4] *Ivi*, p. 4.

[5] Ved. A. MORETTI, *Il valore dei dati nell'European Data Strategy: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022, p. 108.

[6] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020, p. 5.

favorisca l'aumento dei dati conservati ed elaborati nell'Unione europea. Il primo ostacolo per raggiungere questo obiettivo è individuato nella frammentazione normativa che caratterizza le regole di un settore che, invece, per crescere e divenire competitivo, necessita di azioni comuni che rafforzino il mercato interno. Iniziative dei singoli Stati dovrebbero essere sostituite da *progressi comuni*[7] rispetto ad alcune criticità individuate dalla Commissione.

La prima tra queste è l'effettiva disponibilità dei dati, il cui valore risiede nel loro utilizzo e riutilizzo. Il documento programmatico contiene quindi innanzitutto una analisi delle tipologie di flussi. Essi possono realizzarsi nella condivisione dei dati tra PA e imprese, e viceversa, nella condivisione tra imprese e nella condivisione tra autorità pubbliche. In particolare, mentre l'utilizzo dei dati del settore pubblico da parte delle imprese è garantito da politiche consolidate dell'Unione, si evidenzia che i dati del settore privato disponibili per l'utilizzo da parte del settore pubblico non sono ancora sufficienti affinché possano essere valorizzati in termini di miglioramento delle politiche e dei servizi pubblici[8]. Altre criticità sono individuate, nel documento, negli squilibri di potere tra *Big Tech* e piccole e medie imprese (ove queste ultime abbiano difficoltà ad accedere ai dati), nella necessità di sopperire alla carenza di competenze digitali della popolazione e nel necessario potenziamento degli strumenti in mano alle persone fisiche per poter controllare i propri dati. Rileva infine la voce relativa alla necessità di predisporre approcci e strutture di *governance* per l'utilizzo dei dati che ne consentano il massimo sfruttamento. Sul versante tecnico emerge la necessità di migliorare i meccanismi di interoperabilità, la qualità dei dati scambiati (intesa come struttura, autenticità e integrità, la cui assenza potrebbe compromettere il valore dei dati stessi), le infrastrutture, la sicurezza cibernetica.

Le azioni che caratterizzano la strategia europea come delineata dalla Commissione si basano su quattro pilastri. Il primo di questi è la condivisione intersettoriale di dati per favorirne il loro massimo riutilizzo. Per fare questo sono previsti diversi interventi, anche legislativi (tra cui l'adozione di una legge sui dati), ispirati ad un approccio flessibile alla *governance*, che consenta lo sviluppo di ecosistemi vivaci, dinamici e vividi[9]. La Commissione non sposa l'approccio di una normativa dettagliata *ex ante*, che rischierebbe di appesantire il sistema in assenza di

[7] *Ivi*, p. 7.
[8] *Ivi*, p. 7 ss.
[9] *Ivi*, p. 13.

informazioni certe rispetto ai possibili sviluppi tecnologici.

Piuttosto si punta a *rafforzare la sovranità tecnologica europea per l'economia agile basata sui dati*, attraverso una serie di investimenti in dati, infrastrutture tecnologiche, interoperabilità. La strategia punta inoltre sulla alfabetizzazione, per ampliare il serbatoio di talento digitale[10] con la formazione di specialisti digitali e con il supporto alle PMI nello sviluppo di capacità specifiche per renderle capaci di sfruttare appieno le opportunità derivanti da *data-based business models.*

La grande novità proposta con la strategia europea è la creazione di *data spaces* tematici. Dalla possibilità di far circolare i dati ed estrarre da essi valore, innovazione, benefici per la collettività dipende l'espansione del *Digital Single Market*. La Commissione europea propone di realizzare questo effettivo cambio di marcia con un sistema di *pools* di dati, suddivisi in aree tematiche in modo che ogni settore possa trovare regole adeguate, e al contempo i singoli *spaces* possano comunicare tra di loro per massimizzare il flusso di dati, con il superamento dei limiti legati ai *data silos*. Questa suddivisione per settori tematici dovrebbe contribuire a superare la frammentazione[11], considerata un grave rischio per lo sviluppo del Mercato unico, agevolando la condivisione di dati personali e non personali omogenei all'interno di aree regolamentate da norme comuni elaborate per quegli spazi. Nelle parole della Commissione: «*Such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of common rules developed for the space* [12]».

[10] *Ivi*, p. 23.

[11] Nella Relazione per i due anni di applicazione del GDPR la Commissione denuncia quanto sia complesso sviluppare attività economiche/commerciali transfrontaliere, in particolare relative a tecnologie, innovazione e *cybersecurity*, a fronte di una ancora evidente differenziazione delle normative nazionali su aspetti di grande rilevanza pratica per le aziende, quali ad esempio il consenso dei minori in relazione ai servizi della società dell'informazione e il regime di trattamento di particolari categorie di dati, cfr. Commissione europea, *Communication from the Commission to the European Parliament and the Council "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation",* COM(2020) 264 final, 24 giugno 2020.

[12] Commissione europea, *Communication from the Commission to the European Parliament, The Council, The European economic and social Committee and the Committee of the Regions "A European strategy for data*" cit., p. 16.

3.3 La strategia digitale in azione. Il nuovo quadro regolamentare europeo per i dati

Come abbiamo visto, condizione necessaria per lo sviluppo della *data-driven economy* è la disponibilità e la libera circolazione di enormi quantità di dati[13]. Per garantire la fruibilità della materia prima al variegato insieme di attori di questo sviluppo (cittadini, imprese, professionisti, università…) l'Unione ha delineato una serie di interventi per agevolare l'apertura e la circolazione dei dati personali e non personali, e poi la disponibilità di quantità sempre maggiori di dati, con modalità tali da assicurare il rispetto dei diritti.

[13] Sulla libera circolazione dei dati, *ex plurimis*: M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato Concorrenza Regole*, 2/2019, p. 293 ss.; R. PANETTA, (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2007; R. PANETTA, (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, cit.; S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Rivista critica di diritto privato*, 1984.

3.3.1 La libera circolazione dei dati

L'obiettivo di agevolare il libero flusso dei dati personali e non personali nello spazio giuridico europeo, che l'Unione mira a raggiungere principalmente attraverso il GDPR e il regolamento n. 2018/1807, è esplicitato nel Considerando 10 di quest'ultimo, il quale chiarisce che «*A norma del regolamento (UE) 2016/679, gli Stati membri non possono limitare o vietare la libera circolazione dei dati personali all'interno dell'Unione per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento di dati personali. Il presente regolamento sancisce il medesimo principio di libera circolazione all'interno dell'Unione per i dati non personali […]. Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati. […]».*

I due Regolamenti sulla libera circolazione dei dati personali e non personali rispondono all'esigenza di superare la frammentazione normativa nello spazio giuridico europeo, ed al contempo di ingenerare un clima di fiducia, presupposti entrambi irrinunciabili per lo sviluppo del Mercato Unico Digitale[14].

Nel regolamento n. 2016/679 il Considerando 13 chiarisce che «*Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. […]*». L'importanza di regole comuni è riaffermata nel Considerando 7 del regolamento n. 2018/1807, ove si afferma che «*Un unico insieme di regole per tutti i partecipanti al mercato costituisce un elemento essenziale per il corretto funzionamento del mercato interno, affinché siano garantite la certezza del diritto e la parità di*

[14] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Costruire un'economia dei dati europea"*, 10 gennaio 2017, p. 5 ss.

condizioni all'interno dell'Unione. Al fine di rimuovere gli ostacoli agli scambi ed evitare distorsioni della concorrenza derivanti da divergenti normative nazionali, nonché per prevenire il probabile insorgere di ulteriori ostacoli e distorsioni significative, è necessario adottare norme uniformi applicabili in tutti gli Stati membri».

Il Considerando 7 del GDPR fa invece riferimento all'importanza di creare «*il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno*», declinando quel *principio di fiducia* che rappresenta il criterio interpretativo di base e l'obiettivo ultimo che giustifica la stretta connessione che nell'articolo 1[15] lega la tutela dei dati alla garanzia della loro libera circolazione[16].

Il regolamento n. 2018/1807[17], c.d. FFD (*Free Flow Data Regulation*) pone regole volte a garantire la libera circolazione dei *non-personal data*, finalizzate principalmente ad eliminare gli ostacoli alla libera circolazione, primi fra tutti gli obblighi di localizzazione introdotti dagli Stati membri[18].

Relativamente al tema della circolazione dei dati personali e non personali nello spazio giuridico europeo, è bene mettere in luce una conseguenza della espansione del fenomeno della *Big data Analytics* e della comparsa di software di Intelligenza artificiale. Infatti l'evoluzione tecnologica ha reso ormai macchinoso ed obsoleto il processo di separazione dei dati in categorie. Molto spesso tale attività, seppure realizzabile in una fase di ricognizione *ex ante* dei *dataset*, diviene di poca utilità *ex post*, ovvero a seguito del trattamento degli stessi dati con strumenti di analisi ed Intelligenza artificiale. L'utilizzo di algoritmi applicati ad un volume immenso di dati consente di estrarre o anche di prevedere informazioni personali, a volte partendo da *dataset* di informazioni non personali, correlati con altri *dataset* di differente

[15] La norma, dopo aver precisato che scopo del GDPR è proteggere i diritti e le libertà fondamentali degli individui, con particolare riferimento alla protezione dei dati personali, chiarisce che «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*».

[16] Cfr. F. PIZZETTI, *Intelligenza artificiale, protezione dei dati e regolazione*, Giappichelli, Torino, 2018, p. 170.

[17] *Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*.

[18] L'articolo 4 del regolamento FFD vieta agli Stati di introdurre obblighi di localizzazione che impongano di effettuare il trattamento sul territorio dello Stato o ostacolino il trattamento in un altro Stato membro.

origine e contenuto[19]. In questo contesto la distinzione tra dato personale e dato non personale, dunque, è sempre meno realizzabile[20], e la possibilità di una applicazione di regimi giuridici differenti a tipologie diverse di dati, sempre meno probabile. La possibile difficoltà nella separazione tra i due insiemi di dati è stata già prevista dal legislatore europeo, che all'art. 2 par. 2 del regolamento n. 1807/2018 precisa che qualora i dati personali e non personali all'interno di un *dataset* siano indissolubilmente legati, resta impregiudicata l'applicazione del GDPR.

[19] Autorità per le Garanzie nelle Comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 14.

[20] Cfr. Ibidem, Executive Summary, p. 7.

3.3.2 La disponibilità dei dati

Oltre ad introdurre atti normativi volti a garantire la libera circolazione dei dati personali e non personali, l'Unione ha compiuto passi significativi anche rispetto alla progressiva apertura e al riutilizzo del patrimonio informativo del settore pubblico. In questo solco si colloca certamente la direttiva n. 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico[21], emanata al fine di «*sfruttare appieno il potenziale dell'informazione del settore pubblico a vantaggio dell'economia e della società europee»*[22]in quanto «*l'informazione del settore pubblico rappresenta una fonte straordinaria di dati in grado di contribuire a migliorare il mercato interno e lo sviluppo di nuove applicazioni per i consumatori e le persone giuridiche. L'utilizzo intelligente dei dati, ivi compreso il loro trattamento attraverso applicazioni di intelligenza artificiale, può trasformare tutti i settori dell'economia*[23]*».*

Con il fine di allargare il bacino dei dati pubblici accessibili utilizzabili, il *Data Governance Act*[24] integra oggi la direttiva n. 2019/1024, stabilendo regole per il riutilizzo, a determinate condizioni, dei dati detenuti da enti pubblici che siano soggetti a diritti di terzi[25]. Si tratta dei dati protetti per motivi di riservatezza commerciale, riservatezza statistica, protezione della proprietà intellettuale, protezione dei dati personali[26]. Anche in questo caso la scelta dello

[21] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[22] Direttiva n. 2019/1024, Considerando 4.

[23] Direttiva n. 2019/1024, Considerando 9. La varietà di informazioni che il settore pubblico raccoglie, produce, riproduce e diffonde è richiamata nel Considerando 8. Si tratta di «informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione».

[24] *Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Data Governance Act).* Tra i commenti ved. F. COLAPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *I post di AISDUE, Focus "Servizi e piattaforme digitali*", n. 3, 5 maggio 2021; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, Anno 2022, Fascicolo 4, in particolare p. 978 ss..

[25] Si tratta dei dati protetti per motivi di riservatezza commerciale, riservatezza statistica, protezione della proprietà intellettuale, protezione dei dati personali Cfr. Data Governance Act, art. 3 par. 1.

[26] Cfr. Regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto di governance dei dati), COM(2020) 767 final, art. 3.

strumento normativo è ricaduta sul regolamento, per favorire un'applicazione uniforme delle regole.

Il *Data Governance Act* mira a promuovere la disponibilità ed il migliore utilizzo dei dati[27] in favore di nuovi soggetti economici e attori pubblici. L'obiettivo è quello di contrastare le *Big Tech* in ottica pro-concorrenziale, e al contempo consentire la definizione degli indirizzi politici sulla base – anche -di quelle informazioni[28]. Questo scopo può essere ottenuto attraverso diversi meccanismi trai i quali la condivisione tra imprese dietro compenso, l'azione di intermediari per la condivisione[29], per mezzo del consenso per scopi altruistici[30].

Certamente di rilievo sotto il profilo dell'incremento dei dati a disposizione del settore pubblico ai fini del miglioramento delle politiche e delle attività amministrative, è l'introduzione nel DGA di una ipotesi di utilizzo di dati messi a disposizione dagli interessati su base volontaria, per perseguire obiettivi di interesse generale[31]. Tra gli obiettivi di interesse generale elencati nel Considerando 45 compaiono l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione nella realizzazione di statistiche, il miglioramento delle politiche e dei servizi pubblici, il sostegno alla ricerca scientifica. Sempre il citato Recital propone la predisposizione, all'interno degli Stati membri, di sistemi e strumenti tali da agevolare l'espansione della pratica della donazione dei dati sulla base del consenso informato. A tal fine l'articolo 25 prevede l'elaborazione di un modello europeo di consenso all'altruismo dei dati che permetta si presenti con un formato uniforme in tutti gli Stati membri[32]. Il Data Governance Act prevede anche la possibilità di costituire e registrare organizzazioni senza scopo

[27] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale,* in *Studi parlamentari e di politica costituzionale*, 209, 1° semestre 2021, p. 40.

[28] S. SCAGLIARINI, *Identità digitale e tutela della privacy*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit. p. 365.

[29] «*Negli intenti del legislatore unionale, la nuova governance europea dei dati incentrata sugli intermediari, configurati come soggetti indipendenti tanto dai titolari dei dati quanto dagli utenti dei dati, potrà facilitare l'emergere di ecosistemi basati sui dati affidabili e agevolmente fruibili*», cfr. D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law and Technologies*, 1/2022, p. 52.

[30] *Ibidem*.

[31] Ved. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., in particolare p. 986 ss.; A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale,* cit., p. 44.

[32] Si veda in proposito European Data Protection Board, European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 Marzo 2021, pp. 38-39.

di lucro che svolgano attività di altruismo dei dati, destinatarie di obblighi di trasparenza e di obblighi specifici posti a tutela dei diritti degli interessati e dei titolari dei dati[33].

Mentre da una parte l'apertura, da parte della PA, di dati con restrizioni dovute alla tutela della proprietà intellettuale, della privacy o di altri diritti di terzi sui dati sembra in prima battuta agevolare il settore privato, rappresentando piuttosto un onere per quello pubblico, dall'altra parte l'altruismo dei dati sembra rivolto più ad agevolare il settore pubblico nella raccolta dei dati. A questo potrebbe aggiungersi, se il *Data Act* dovesse arrivare in porto come l'attuale proposta, il potere delle autorità pubbliche di acquisire d'imperio i dati per ragioni eccezionali di necessità.

La proposta di *Data Act* nasce come abbiamo ricordato poc'anzi in seno alla Strategia europea per i dati al fine di porre regole armonizzate per l'equo accesso ai dati, in modo da poterne distribuire il valore. Nella relazione di presentazione dell'atto si fa riferimento al valore dei dati che è concentrato nelle mani di poche società, mentre la maggior parte dei dati non è utilizzata a causa di scarsa fiducia, incentivi economici contrastanti e ostacoli tecnologici[34]. Appare dunque centrale il tema della equità e della redistribuzione del valore derivante dai dati tra tutti gli attori della società digitale. Questo testo legislativo appare particolarmente rilevante in quanto viene in rilievo la necessità che anche la Pubblica Amministrazione divenga *recipient* di dati. Si ricalibra quindi un assetto in cui lo sviluppo del Mercato unico, obiettivo centrale della strategia europea, ha portato a concentrare l'attenzione verso forme sempre più allargate di apertura dei dati pubblici per il riutilizzo. Non si era invece prestata attenzione alla necessità per il settore pubblico di avere più informazioni a disposizione – tra cui certamente quelle estraibili

[33] Data Governance Act, artt. 17 ss.

[34] *Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (legge sui dati), COM(2022) 68 final*, Relazione, p. 1.

dai dati di operatori privati[35] – per adempiere in modo più efficiente ai compiti assegnati dalla legge ad ogni autorità/organismo[36].

La legge sui dati vuole rispondere alla esigenza di garantire flussi di dati più ampi ed equi tra impresa e impresa, tra PA e Pa, tra impresa e PA e viceversa. Per quanto attiene la condivisione di dati tra imprese, il *Data Act* mira ad evitare che le Piccole e Medie Imprese rimangano vittime di situazioni di squilibrio e accettino accordi contrattuali che non garantiscono loro un accesso adeguato ai dati, a causa delle asimmetrie nel potere negoziale o nelle conoscenze.

Per quanto attiene alla condivisione di dati B2G (*Business to Government*), nella proposta di *Data Act* viene disciplinato un istituto di "espropriazione forzata" dei dati di operatori privati da parte di organismi pubblici, nei casi di "necessità eccezionale". Tali sono considerati i dati che servono a prevenire o gestire una emergenza pubblica o a contribuire alla ripresa dopo tale emergenza, posto che la richiesta deve essere limitata nel tempo e nella portata (una sorta di principio di proporzionalità della richiesta). La terza ipotesi contemplata è che la mancanza di dati impedisca alla pubblica autorità di svolgere un compito di interesse pubblico stabilito dalla legge, ove il soggetto pubblico non possa reperire tali dati a prezzi di mercato, né attraverso gli strumenti legislativi in vigore o da adottare. Infine viene considerata la eventuale riduzione dell'onere amministrativo che graverebbe sull'attore pubblico nel caso in cui dovesse reperire i dati altrimenti che attraverso l'"espropriazione". A fronte dell'obbligo di messa a disposizione dei dati da parte dei soggetti privati, la legge sui dati prevede una serie di regole che il richiedente dovrà rispettare. L'articolo 17 elenca il contenuto minimo essenziale per inoltrare una richiesta. Essa dovrà specificare quali dati sono richiesti, quale sia lo scopo della richiesta, l'uso che si farà dei dati e il tempo di utilizzo. Inoltre l'autorità pubblica richiedente

[35] Relativamente ai dati già in possesso della pubblica amministrazione, nell'ordinamento italiano l'articolo 50 del CAD disciplina la condivisione dei dati tra diverse pubbliche amministrazioni e tra di esse e soggetti privati. La norma specifica che i dati delle pubbliche amministrazioni debbono essere raccolti, conservati, resi disponibili e accessibili, entro i limiti posti dalla normativa *privacy* e nel rispetto delle leggi e dei regolamenti, compresa la legislazione europea sul riutilizzo. Il secondo comma chiarisce che i dati in possesso di una amministrazione debbono essere messi a disposizione di altre PA quando siano necessari per adempiere a compiti istituzionali (senza peraltro che il trasferimento da un sistema informativo ad un altro modifichi la titolarità del dato e del trattamento, come specificato nel comma 3-*bis*). Il comma 2-*bis* specifica che le PA possono, entro l'ambito delle proprie funzioni istituzionali, procedere all'analisi dei propri dati, anche in combinazione con quelli detenuti da altri soggetti pubblici, e secondo le modalità individuate da AgiD.

[36] Si tornerà su questo aspetto nelle Conclusioni.

dovrà indicare la base giuridica della richiesta e dimostrarne l'eccezionalità, oltre che il termine entro il quale i dati debbono essere resi disponibili. Il secondo paragrafo specifica che la richiesta dovrà essere espressa in termini chiari, coincisi e comprensibili, che deve essere proporzionata in termini di granularità, volume e frequenza, e riguardare se possibile dati non personali; essa deve rispettare le finalità legittime del titolare dei dati, e lo stesso titolare dovrà essere informato delle eventuali sanzioni per la mancata messa a disposizione. L'articolo 19 impone agli enti pubblici che hanno ricevuto i dati a seguito della richiesta di non utilizzare i dati in modo incompatibile con lo scopo per il quale sono stati richiesti, di mettere in atto misure tecniche e organizzative adeguate a tutelare i diritti e le libertà degli interessati, di distruggere i dati non appena non saranno più necessari, informandone il titolare. La messa a disposizione dei dati per rispondere ad una emergenza pubblica non prevede il pagamento di alcun corrispettivo. Il compenso non potrà superare i costi tecnici ed organizzativi sopportati dal titolare per rispondere alla richiesta[37].

Insieme all'altruismo dei dati disciplinato nel *Data Governance Act*, l'obbligo di messa a disposizione svolge la funzione di riequilibrio tra il costante aumento della massa di dati – e dunque di valore – in possesso di pochi, grandi operatori privati, e la scarsità di dati privati a disposizione del settore pubblico[38].

La proposta di regolamento sull'Intelligenza artificiale completa la rassegna proposta. L'impatto di una normativa siffatta, quando verrà approvata, sarà certamente significativo ed avrà dei risvolti applicativi importanti per gli attori privati del sistema economico ma anche per i soggetti pubblici, in quanto fruitori di sistemi di IA. Infatti molte delle declinazioni dell'innovazione tecnologica e nel settore pubblico e, vedremo, nell'amministrazione degli enti locali, ricadono oggi nelle fattispecie che emergono dall'*Artificial Intelligence Act*. Si profilano dunque numerose questioni applicative e di coordinamento con il restante apparato regolamentare, in particolar modo quello relativo alla gestione dei dati, essendo, dati ed algoritmi, le due componenti essenziali dell'economia e della società digitale.

[37] Proposta di Data Act, art. 20.

[38] *Ivi*, p. 3: *«[…] la Commissione presenta una proposta di normativa sui dati con l'intento di garantire un'equa ripartizione del valore dei dati tra gli operatori dell'economia dei dati e di promuovere l'accesso ai dati e il relativo utilizzo*».

3.4 La proposta per la regolazione dell'Intelligenza artificiale in Europa

La proposta di regolamento sull'Intelligenza artificiale presentata il 21 aprile 2021[39] pone «*regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di Intelligenza artificiale nell'Unione*» (art. 1 lett. a)). Si tratta di un testo normativo complesso, caratterizzato dalla compresenza di istanze volte allo sviluppo dell'industria e del mercato e di un'impostazione di fondo che mette saldamente al centro la persona e i suoi diritti fondamentali[40].

L'articolo 3 n. 1) introduce la definizione di "*sistema di intelligenza artificiale*[41]". Seguono le regole per l'utilizzo delle diverse tipologie di sistemi di IA. Il legislatore ha svolto una valutazione *a priori* sui rischi di danno per la salute, la sicurezza e di impatto negativo sui diritti fondamentali e attribuito a ciascun livello di rischio una disciplina via via meno stringente[42]. Si

[39] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (legge sull'Intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM(2021) 206 final.

[40] Si vedano CASONATO C., MARCHETTI B., *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di Intelligenza artificiale*, in *Biolaw Journal - Rivista di BioDiritto* n. 3/2021, p. 415 ss.; MANTELERO A., *Sulle regole AI l'Europa sceglie approccio "industriale": luci e ombre*, in *AgendaDigitale*, 27 aprile 2021; SIMONCINI A., *Verso la regolamentazione della Intelligenza artificiale. Dimensioni e governo*, in *BioLaw Journal – Rivista di BioDiritto*, vol. 2, 2021; il volume *La via europea per l'Intelligenza artificiale*, a cura di C. CAMARDI, Wolters Kluwer CEDAM, Milano, 2022, ed in particolare i contributi G. MAZZINI, S. SCALZO, *The proposal for the Artificial Intelligence Act: considerations around some key concepts*, pp. 21-52; G. RESTA, *Cosa c'è di "europeo" nella proposta di Regolamento UE sull'Intelligenza artificiale?*, pp. 53-74; V. PAGNANELLI, *Il settore pubblico alla sfida dell'Intelligenza artificiale*, pp. 157-184; G. FINOCCHIARO, *La proposta di Regolamento sull'Intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, pp. 215-237; A. SIMONCINI, *Quale modello per la regolazione dell'Intelligenza artificiale? L'Europa al bivio*, pp. 239-265; P. STANZIONE, *La via europea all'Intelligenza artificiale*, pp. 513-518.

[41] «*Un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*», cfr. Proposta di Regolamento sull'IA, art. 3 num. 1).

[42] «*Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di intelligenza artificiale, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA*», cfr. Proposta di regolamento sull'IA, Considerando 14. Sull'adozione dell'approccio basato sul rischio negli atti regolatori europei ved. G. DE GREGORIO., P.

passa infatti dal rischio massimo, che ove presente in determinati sistemi di Intelligenza artificiale ne prevede la proibizione, alla ampia categoria dei sistemi ad alto rischio, per i quali è prevista una disciplina molto articolata, ai sistemi a rischio medio, destinatari di obblighi minimi, fino ai sistemi di Intelligenza artificiale considerati privi di rischi, per i quali non viene predisposto alcun tipo di regolazione all'interno dell'articolato.

I sistemi di Intelligenza artificiale proibiti sono descritti nell'articolo 5[43]. L'AIA vieta l'utilizzo di tecniche subliminali che possano distorcere il comportamento di una persona in

DUNN, *Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA*, https://assets.ctfassets.net/iapmw8ie3ije/5EuxLPaUIsgGt7R6PgeuFK/c9269e55e10bb2a7a0b392624c08f4d0/De_Gregorio_Dunn_My_Data_is_Mine__1_.pdf .

[43] *Articolo 5*

1. Sono vietate le pratiche di intelligenza artificiale seguenti:

a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;

iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

2. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), tiene conto dei seguenti elementi:

a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema;

modo da provocare ad essa o ad altri un danno fisico o psicologico, i sistemi che sfruttano le vulnerabilità dovute all'età o alla disabilità di uno specifico gruppo di persone, i sistemi utilizzati dalle autorità pubbliche per classificare l'affidabilità delle persone in base al loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale ottenuto abbia come conseguenza il trattamento pregiudizievole o sfavorevole di determinate persone o gruppi di persone in contesti sociali non collegati ai contesti in cui i dati sono stati originariamente raccolti, o un trattamento pregiudizievole o sfavorevole ingiustificato o sproporzionato rispetto al comportamento sociale delle persone oggetto di valutazione o rispetto alla gravità di tale condotta.

L'ultima categoria di trattamenti vietati riguarda l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini di attività di contrasto[44].

b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali.

3. Per quanto riguarda il paragrafo 1, lettera d), e il paragrafo 2, ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso.

L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2.

4. Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, lettera d), e ai paragrafi 2 e 3. Tale Stato membro stabilisce nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, lettera d), compresi i reati di cui al punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

[44] Per una riflessione sul rapporto tra l'utilizzo del riconoscimento biometrico a fini di polizia in spazi accessibili al pubblico e le modalità del controllo statuale si veda G. SOANA, *Intelligenza artificiale e architettura del controllo. Una riflessione sull'utilizzo delle tecnologie di riconoscimento facciale basate su IA negli spazi pubblici*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, cit., p. 197 ss.

Questo ultimo divieto è però corredato da una serie di significative eccezioni, che rendono lecito porre in essere queste pratiche altrimenti vietate. Si tratta dei casi di ricerca mirata di potenziali vittime di reato, compresi i minori scomparsi, della prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità delle persone o di un attacco terroristico, del rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o sospettato di reato nel quadro di esecuzione del mandato di arresto europeo, nel caso in cui il reato sia punibile con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

Il paragrafo 2 dell'articolo 5 prosegue introducendo dei criteri di valutazione della opportunità e necessità di utilizzo di un sistema di identificazione biometrica in tempo reale, quali la natura della situazione che dà luogo al possibile utilizzo, e la gravità, la probabilità, e l'entità del danno in caso di mancato utilizzo, e d'altro canto le conseguenze in termini di gravità, probabilità ed entità per i diritti e le libertà delle persone interessate. La norma prevede inoltre che vengano rispettate le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare con riguardo alle limitazioni temporali, geografiche e personali.

Il terzo paragrafo prevede che l'utilizzo di sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico a fini di contrasto debba comunque essere autorizzato preventivamente dall'autorità giudiziaria o da un'autorità amministrativa indipendente, a seguito di richiesta motivata e salvo motivi di urgenza debitamente giustificata. Infine, il paragrafo 4 consente agli Stati membri di autorizzare in tutto o in parte l'utilizzo dei sistemi di identificazione appena descritti, predisponendo, nel diritto interno, regole di dettaglio che disciplinino tutte le fasi dell'utilizzo, dalla richiesta alle attività di controllo.

L'articolo 6[45] definisce i sistemi di IA c.d. *ad alto rischio*, prevedendo che un sistema ricada in tale fascia di rischio ove siano presenti entrambe le seguenti condizioni: che il sistema

[45] *Articolo 6 - Regole di classificazione per i sistemi di IA ad alto rischio*

1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;

b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato

sia destinato ad essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II, e che il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.

Oltre ai sistemi di Intelligenza artificiale che possono essere inseriti nella categoria in quanto rispondenti alle condizioni appena descritte, la proposta di regolamento individua una serie enumerata e fissa di sistemi di IA, suddivisi in settori elencati nell'allegato III, che sulla base di una valutazione svolta anch'essa *a priori* sono da considerarsi sempre ad alto rischio[46]. I settori

---

o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

46 *L'articolo 7 attribuisce alla Commissione il potere di aggiornare l'elenco attraverso l'adozione di atti delegati a norma dell'articolo 73: Articolo 7 - Modifiche dell'allegato III*

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare l'elenco di cui all'allegato III aggiungendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati ai punti da 1 a 8 dell'allegato III;

b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, che è, in relazione alla sua gravità e alla probabilità che si verifichi, equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.

2. Nel valutare, ai fini del paragrafo 1, se un sistema di IA presenti un rischio di danno per la salute e la sicurezza o un rischio di impatto negativo sui diritti fondamentali equivalente o superiore al rischio di danno presentato dai sistemi di IA ad alto rischio di cui all'allegato III, la Commissione tiene conto dei criteri seguenti:

a) la finalità prevista del sistema di IA;

b) la misura in cui un sistema di IA è stato usato o è probabile che sarà usato;

c) la misura in cui l'uso di un sistema di IA ha già causato un danno alla salute e alla sicurezza o un impatto negativo sui diritti fondamentali o ha suscitato gravi preoccupazioni in relazione al verificarsi di tale danno o impatto negativo, come dimostrato da relazioni o da prove documentate presentate alle autorità nazionali competenti;

d) la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e capacità di incidere su una pluralità di persone;

e) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo dipendono dal risultato prodotto da un sistema di IA, in particolare perché per motivi pratici o giuridici non è ragionevolmente possibile sottrarsi a tale risultato;

f) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto all'utente di un sistema di IA, in particolare a causa di uno squilibrio di potere, conoscenza, situazione economica o sociale o età;

sono i seguenti: identificazione e categorizzazione biometrica delle persone fisiche, gestione e funzionamento delle infrastrutture critiche, istruzione e formazione professionale, occupazione, gestione dei lavoratori e accesso al lavoro autonomo, accesso a prestazioni e servizi pubblici e privati essenziali e fruizione degli stessi, attività di contrasto, gestione della migrazione, dell'asilo e del controllo delle frontiere, amministrazione della giustizia e processi democratici.

Il Titolo III pone una disciplina molto dettagliata, che prevede numerosi adempimenti e obblighi cui i soggetti coinvolti a vario titolo nel funzionamento dei sistemi ad alto rischio debbono adeguarsi. Compaiono infatti regole per i fornitori, per i fabbricanti di prodotti, per i rappresentanti autorizzati, per gli importatori, per i distributori e regole per gli utenti.

Il capo II è interamente dedicato ai requisiti cui il sistema *high risk* deve essere conforme. Innanzitutto, è previsto un sistema di gestione dei rischi, ovvero «*un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un aggiornamento costante e sistematico*[47]». L'articolo 10[48] prevede e regola la *governance* dei dati

g) la misura in cui il risultato prodotto con un sistema di IA è facilmente reversibile, considerando non facilmente reversibili i risultati che hanno un impatto sulla salute o sulla sicurezza delle persone;

h) la misura in cui la legislazione vigente dell'Unione prevede:

i) misure di ricorso efficaci in relazione ai rischi presentati da un sistema di IA, ad esclusione delle richieste di risarcimento del danno;

ii) misure efficaci per prevenire o ridurre sostanzialmente tali rischi.

[47] art. 9 par. 2.

[48] *Articolo 10 - Dati e governance dei dati*

1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5.

2. I set di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di governance e gestione dei dati. Tali pratiche riguardano in particolare:

a) le scelte progettuali pertinenti;

b) la raccolta dei dati;

c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione;

d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;

e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;

f) un esame atto a valutare le possibili distorsioni;

g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere

di addestramento, convalida e prova. Seguono norme sulla documentazione tecnica, la conservazione delle registrazioni, la trasparenza e fornitura di informazioni agli utenti, la sorveglianza umana, l'accuratezza, robustezza e cybersicurezza.

I sistemi considerati a rischio limitato, ovvero quelli destinati ad interagire con le persone fisiche, quelli che operano un riconoscimento delle emozioni o una categorizzazione biometrica e quelli che generano o manipolano contenuti digitali che assomigliano a persone o altri oggetti, luoghi od entità che potrebbero apparire falsamente autentici o veritieri, fornitori e utenti sono sottoposti ad obblighi di trasparenza, a norma dell'art. 52[49].

usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi.

4. I set di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

5. Nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

6. Per lo sviluppo di sistemi di IA ad alto rischio diversi da quelli che utilizzano tecniche che prevedono l'addestramento di modelli si applicano adeguate pratiche di gestione e governance dei dati, al fine di garantire che tali sistemi di IA ad alto rischio siano conformi al paragrafo 2.

[49] *Articolo 52 - Obblighi di trasparenza per determinati sistemi di IA*

1. I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. Gli utenti di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica, che sono autorizzati dalla legge per accertare, prevenire e indagare reati.

3. Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente.

Tuttavia il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

Non sussiste nemmeno tale obbligo invece per tutti i restanti sistemi di Intelligenza artificiale che non rientrano in nessuna delle categorie indicate nell'AIA, che pertanto sono considerati a rischio minimo e perciò non bisognosi di alcun tipo di regolazione.

È certamente vero che l'utilizzo di sistemi di Intelligenza artificiale nel settore pubblico potrebbe fornire occasioni per migliorare l'efficienza, l'efficacia e la trasparenza della Pubblica amministrazione[50]. Non possono però essere taciuti però i gravi rischi di compromissione di diritti fondamentali che possono derivare da un utilizzo non regolamentato di tecnologie per loro natura capaci di giungere a livelli di pervasività senza precedenti. La suddivisione in categorie di rischio delle differenti tecnologie che viene proposta dall'AIA mira a garantire livelli crescenti di protezione, sino ad arrivare ai divieti di utilizzo, dinanzi a *software* via via più pericolosi.

Il regolamento non prevede una suddivisione tra disciplina per il settore pubblico e disciplina per il settore privato. Questa scelta metodologica mira ad ancorare l'applicazione di determinate regole ad una concreta valutazione del rischio connesso all'utilizzo di uno specifico sistema di IA. Occorre evidenziare però come il regolamento sull'IA, pur non contenendo formalmente una disciplina *ad hoc* per il settore pubblico, di fatto ne ponga una nella sostanza. Due su quattro tra i divieti posti dall'articolo 5 sono rivolti ad autorità pubbliche (l'attività di *social scoring* di cui al par. 1 lett. c) e l'identificazione biometrica remota "in tempo reale" a fini di contrasto di cui al par. 1 lett. d)). Lo stesso divieto non vale per i privati. Inoltre, molti degli utilizzi che ricadono nella qualificazione "ad alto rischio" possono essere ricondotti alle finalità perseguite dalle pubbliche autorità.

Scorrendo l'Allegato III si evince che la maggior parte dei sistemi ad alto rischio, per cui è prevista una disciplina di *compliance* molto articolata, sono riconducibili ad attività poste in essere nel settore pubblico. Basti pensare ai «*sistemi di IA destinati ad essere utilizzati come componenti di sicurezza nella gestione del traffico stradale e nella fornitura di acqua, gas,*

4. I paragrafi 1, 2 e 3 lasciano impregiudicati i requisiti e gli obblighi di cui al titolo III del presente regolamento. Sul diritto di conoscere la natura dell'interlocutore ved. C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, Maggio 2019, p. 101 ss.

[50] Cfr. M. TRAPANI, *GDPR e Intelligenza artificiale: i primi passi tra governance, privacy, trasparenza e accountability*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 319 ss..

riscaldamento ed elettricità», ai sistemi di IA utilizzati «*per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica*», o ancora ai sistemi utilizzati per inviare servizi di primo soccorso stabilendo al contempo la priorità. Si pensi ancora alle già citate attività di contrasto, tra cui, ad esempio, i sistemi utilizzati dalle autorità per individuare i c.d. *deep fake*.

Pare ripetersi, con l'introduzione dell'AIA, lo schema emerso in conseguenza dell'entrata in vigore del GDPR, cioè il "doppio binario" tra settore pubblico e privato, ove il settore pubblico vede applicata una disciplina molto più rigida e caratterizzata da molte più prescrizioni, il più delle volte soggette ad integrazioni a livello nazionale (come nel caso delle norme introdotte con il d. lgs. 101/2018 di modifica del Codice della privacy), e da interventi delle autorità di controllo nazionali[51].

Il risultato rischia di essere nuovamente la frammentazione normativa e regolamentare che costantemente mina e limita lo sviluppo del Mercato Unico, e che proprio la scelta di intervenire nel settore dell'Intelligenza artificiale con un regolamento piuttosto che con una Direttiva voleva scongiurare[52]. Nella relazione di accompagnamento alla proposta si legge infatti che «*la scelta di un regolamento come atto giuridico è giustificata dalla necessità di un'applicazione uniforme delle nuove regole, come la definizione di IA, il divieto di talune pratiche dannose consentite dall'IA e la classificazione di taluni sistemi di IA. L'applicabilità diretta di un regolamento, conformemente all'articolo 288 TFUE, ridurrà la frammentazione giuridica e faciliterà lo sviluppo di un mercato unico per sistemi di IA leciti, sicuri e affidabili*[53]».

Inoltre nel panorama attuale del sistema giuridico europeo la Pubblica Amministrazione si trova all'interno di un reticolo di norme ed adempimenti di *compliance* cui attenersi. Basti pensare, oltre all'*Artificial Intelligence Act*, al GDPR, al regolamento FFD, alla direttiva sul riutilizzo dell'informazione nel settore pubblico, al *Data governance act*, cui si aggiungerà la

[51] Sul punto sia consentito rinviare a V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *Osservatorio sulle fonti*, 2/2021, p. 783 ss., ove sottolineo come, anche nelle decisioni del Garante, la medesima tipologia di trattamento viene autorizzata nel caso di titolari del trattamento privati, e vietata per titolari pubblici.

[52] SIMONCINI A., *Quale modello per la regolazione dell'Intelligenza artificiale? L'Europa al bivio*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, cit., pp. 246-247.

[53] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (legge sull'Intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, Relazione, COM(2021) 206 final.

legge sui dati. Questa prospettiva pone le PA di fronte ad una sfida molto impegnativa, specie ove ad un aumento del numero e della complessità degli adempimenti non corrisponda un eguale rafforzamento dei mezzi organizzativi, finanziari, delle competenze e degli investimenti adeguati a gestire tale complessità.

Un esempio di questa complessità derivante dall'applicazione congiunta di più normative all'utilizzo dei sistemi di Intelligenza artificiale riguarda la catena di soggetti coinvolti nella regolazione dell'utilizzo di sistemi di IA. Numerose sono le figure il cui ruolo viene descritto e regolato nell'AIA: produttore, fornitore, distributore, utente. Parallelamente alla catena delle responsabilità sui sistemi di IA dovrà essere identificata la filiera dei ruoli *privacy* (titolari, responsabili, incaricati, oltre che DPO). A ciascuna delle figure appena descritte com'è noto la normativa attribuisce, con diversi gradi di intensità, compiti e responsabilità. Nel complesso reticolo degli apparati amministrativi, ed in quello ancora più complesso che racchiude anche i rapporti degli enti pubblici con fornitori e partner esterni alla pubblica amministrazione, questo si dovrà tradurre in nomine, contratti, policies che consentano di risalire in ogni circostanza la catena delle responsabilità.

L'utilizzo di algoritmi di *machine-learning*[54] e *deep-learning*[55] potrebbe aumentare ulteriormente la complessità di un processo di per sé semplice. Infatti questi sistemi di Intelligenza artificiale sono caratterizzati da una complessità tecnologica tale da impedire, in elaborazioni complesse e concatenate di accedere alle modalità di funzionamento[56]. La

[54] Apprendimento automatico: «*un algoritmo di apprendimento automatico è in grado di imparare dai dati e di costruire un modello per ogni specifico problema che gli si presenta. In altre parole, i vari algoritmi "addestrano" un modello che rappresenta l'essenza della capacità di risolvere quel problema. […] Da un insieme di dati di partenza noti (il dataset), il nostro obiettivo è trovare un modello che sia in grado di elaborarne correttamente di nuovi, non ancora conosciuti o persino non ancora avvenuti*», cfr. F. M. DE COLLIBUS, *L'era delle macchine che apprendono*, in *Limes, Rivista italiana di geopolitica*, 12/2022, pp. 17-18.

[55] Apprendimento profondo: «*L'idea di base è che i neuroni artificiali possano dividersi in tanti strati non immediatamente visibili (hidden layer, strati nascosti), ciascuno dei quali calcola uno stato intermedio: la somma di questi livelli dà origine al risultato finale di output. La fase di addestramento di tale rete neurale artificiale consiste nel determinare i pesi corretti dei singoli neuroni nel contesto della rete globale in cui si trovano*», ivi, p.23.

[56] Cfr. Council of Europe study DGI(2017)12, *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, p. 38. Ved. anche A. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, cit., p. 295.

mancanza di totale trasparenza sulle singole fasi di trattamento dei dati e sui singoli *output* dei *software* utilizzati con ogni probabilità renderà più difficoltosa l'individuazione dei centri di imputazione della responsabilità. Si aggiunga la necessità appena richiamata per la PA di rivolgersi all'esterno per forniture e servizi, specie nel settore tecnologico. A questa circostanza consegue in primo luogo l'esigenza di dotare la PA di competenze interne altamente specializzate, in grado di trarre il maggiore vantaggio dall'utilizzo delle innovazioni tecnologiche e al contempo di governarne l'impatto nella organizzazione interna delle mansioni e delle responsabilità. Un esempio potrebbe meglio chiarire la urgenza per le PA di assicurarsi personale competente: appare evidente che gli enti pubblici dovranno essere in grado di redigere bandi di gara volti ad individuare soggetti idonei a garantire il rispetto del composito quadro regolatorio delineato poc'anzi.

Se è vero che la prima regolazione in materia di sistemi di Intelligenza artificiale è ancora in fase di proposta, è pur vero che applicazioni pratiche su *software* basati su algoritmi avanzati, che sono alimentati da dati personali, sono già in funzione da tempo e sono passati al vaglio del Garante per la protezione dei dati personali. Infatti l'utilizzo degli algoritmi nel settore pubblico è evoluto nel tempo verso una sempre più stringente tendenza alla profilazione del cittadino/contribuente/lavoratore/utente del Servizio Sanitario Nazionale, per le più svariate finalità. Questa tendenza ad un controllo più pervasivo, da realizzarsi grazie alle potenzialità dei trattamenti automatizzati, ha costretto l'Autorità ad incrementare la sua attività di sorveglianza.

Con il provvedimento del 25 marzo 2021[57] l'Autorità si è pronunciata sul c.d. *sistema SARI Real Time*, che ove fosse stato utilizzato, avrebbe consentito di analizzare in tempo reale i volti ripresi da telecamere installate in aree geografiche predeterminate, confrontandoli con una banca dati predefinita (*watch-list*) contenente un massimo di 10.000 volti. Il sistema, sottoposto alla valutazione dell'Autorità dal Ministero dell'Interno - Dipartimento di Pubblica Sicurezza, attraverso un algoritmo di riconoscimento facciale avrebbe individuato corrispondenze tra i volti e avrebbe di conseguenza generato un *alert* per richiamare l'attenzione degli operatori sul *match* tra il soggetto ripreso e uno dei profili contenuti nell'archivio di riferimento.

[57] Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time* - 25 marzo 2021, docweb n. 9575877.

Il Garante nell'esprimere un parere su tale proposta ha chiarito che "*il sistema in argomento realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di polizia; ancorché la valutazione d'impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno l'identificazione di una persona in luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella "watch-list*".

Nell'ordinamento italiano mancano disposizioni normative specifiche che consentano tale tipo di trattamento che per le sue caratteristiche determina una forte interferenza con la vita privata delle persone interessate, pertanto, il Garante esprime parere negativo rispetto al trattamento sottoposto al suo vaglio.

Molto significativo appare il passaggio del provvedimento in cui l'Autorità sottolinea come con il trattamento biometrico di tutte le persone che circolano in uno spazio pubblico si determini "*una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui*". Infatti, l'impiego di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione dei reati dovrebbe avvenire solo ove strettamente necessario, in modo proporzionato alle finalità e con le dovute garanzie.

Il sistema di identificazione biometrica progettato dal Dipartimento di Pubblica Sicurezza sembrerebbe rientrare in quanto previsto dall'articolo 5 par. 1 lett. d) dell'AIA ed essere pertanto vietato[58]. La fattispecie descritta rientra infatti nella descrizione dell'utilizzo di *sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto.* Nonostante il divieto esplicito di utilizzo di tali sistemi, la stessa disposizione contiene un elenco di esimenti che rendono legittimo l'uso dell'identificazione biometrica in

[58] L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico è vietato solo nel caso in cui esso sia a fini di attività di contrasto. La motivazione di tale ulteriore restrizione risiederebbe nella necessità di evitare che, sottoposta a sorveglianza costante, la popolazione possa essere indirettamente limitata nell'esercizio della libertà di riunione e di altri diritti fondamentali; inoltre, l'immediatezza dell'impatto e l'impossibilità di eseguire ulteriori controlli e correzioni aumenterebbe il rischio per i diritti e le libertà delle persone fisiche, Cfr. Proposta di Regolamento sull'IA, Considerando 18.

tempo reale per attività di contrasto se questo è necessario per la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi[59], che potrebbe pertanto legittimare il trattamento automatizzato di dati biometrici a fini di identificazione in tempo reale.

Si potrebbe allora, erroneamente, pensare che il limite sovente incontrato da parte di autorità pubbliche nel tentativo di introdurre soluzioni tecnologiche basate sull'utilizzo di sistemi di Intelligenza artificiale, spesso soggetto a battute d'arresto per la mancanza di una base giuridica idonea a rendere lecito il trattamento automatizzato di dati personali, potrebbe essere superato con l'adozione del testo definitivo dell'*Artificial Intelligence Act*. Il Considerando n. 41 dell'AIA offre delle indicazioni dirimenti. In primo luogo, vi si chiarisce che la circostanza che un sistema di IA sia classificato come ad alto rischio secondo i parametri del regolamento non rende l'utilizzo di tale *software* automaticamente lecito, ma al contrario esso dovrà essere conforme al resto della legislazione, compresa quella sulla *data protection*. In secondo luogo, e ancora più importante, il Considerando 41 specifica che l'AIA non dovrebbe esser considerato quale fondamento giuridico per il trattamento di dati personali, comprese le categorie particolari[60].

Da una attenta analisi della proposta di regolamento emerge dunque chiaramente come i due Regolamenti (GDPR e AIA) non siano complementari, e che anzi l'applicazione di entrambe le normative potrebbe in futuro sollevare questioni interpretative e di coordinamento, specie nel settore pubblico.

La rassegna normativa appena svolta ci ha consentito di definire ulteriormente il quadro delle regole applicabili ai dati (e ai sistemi di Intelligenza artificiale che li utilizzano) entro il quale soggetti pubblici e attori privati debbono collocarsi ad agire. Per quanto attiene all'oggetto di questa ricerca, l'applicazione, nello spazio urbano, dell'apparato regolatorio che si sta delineando, appare utile per decodificare e dare una chiave di lettura ai fenomeni di sviluppo

[59] Cfr. Proposta di regolamento sull'IA, art. 5 par. 1 lett. d) punto i).

[60] «*Il fatto che un sistema di IA sia classificato come ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia necessariamente lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità ai requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale. Il presente regolamento non dovrebbe essere inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali*».

delle c.d. *smart cities.* Infatti, in assenza di una cornice normativa unitaria, tali progetti stanno evolvendo in modo non sempre ordinato. Di conseguenza i processi di ammodernamento e miglioramento dei servizi e dell'amministrazione subiscono rallentamenti o sono comunque più difficoltosi, in quanto gli amministratori sono frenati dalla incertezza sulla individuazione delle regole da applicare a nuove fattispecie e nuovi rischi, in un quadro in continua evoluzione[61]. Nel prossimo capitolo si cercherà di dare conto del percorso che gli enti locali, con diversi gradi di intensità, stanno percorrendo verso la trasformazione in città intelligenti.

[61] Cfr. S. RANCHORDAS – A. KLOP, *Data-driven regulation and governance in smart cities,* University of Groningen Faculty of Law Legal Studies Research Paper Series No. 7/2018, p. 21, «*Moreover, smart cities also do not always have specific or flexible legal frameworks that can embed their novel policies and match the new urban reality and their needs. […] the lack of a specific legal framework for smart cities can delay or impede some of their initiatives, including data-driven regulation and governance*».

CAPITOLO 4 – LA GOVERNANCE DEI DATI NELLA CITTA' INTELLIGENTE

4.1 Smart cities, tra forma e sostanza

Alcuni autori sostenevano, già alcuni anni fa, che il termine *smart city* sarebbe ben presto incorso in obsolescenza: «*Smart city is still an evolving field, with many projects still alive; however, it is expected that the term itself will soon lose its relevance and will be superseded by a new label with new agendas, interests and technologies*[62]*».* Così non è stato, ed anzi studi ed iniziative aventi ad oggetto proprio la concretizzazione di questa idea hanno visto in tempi recenti una nuova fase di sviluppo. Da ultimo uno studio del Parlamento europeo ha individuato le caratteristiche principali di una *smart city*, che ruotano tutte attorno all'idea dell'uso della tecnologia per una migliore gestione della città, che porti benefici ai cittadini, alle imprese, agli amministratori pubblici e che sia orientato alla sostenibilità sociale ed ambientale[63]. Anche nel documento "*A European Strategy for Data* [64]" di cui ci siamo occupati nel capitolo precedente la Commissione ricorda come i dati siano la linfa vitale dello sviluppo economico, e come possano rendere possibile «*un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici*», oltre a costituire un fondamentale elemento «*per far fronte alle sfide sociali, climatiche e ambientali, contribuendo allo sviluppo di società più sane, più*

[62] cfr. K. S. WILLIS, A. AURIGI, *Digital and Smart cities*, Routeledge, London-New York, 2018, p. 16.

[63] «*In particular, seven distinct features of smart cities can be highlighted: 1. Broad use of ICT as the core element of smart cities as they connect infrastructure and services as well as increase the quality of life of city residents; 2. Use of technologies and innovation to improve well-being; 3. A business-friendly environment with a sense of cooperation and consultation between authorities, industry and communities; 4. Openness through the idea of a smart city as an open innovation platform to foster the empowerment of citizens and communities; 5. Real-time monitoringand the use of data for city management; 6. Citizen empowerment as smart cities encourage programs aiming to increase social learning and education, and strengthen social capital; 7. Sustainability as smart cities also aim to create socially and environmentally sustainable cities by reducing the negative impacts of human activity*», cfr. European Parliament, Panel for the Future of Science and Technology (STOA), *Social approach to the transition to smart cities*, Febbraio 2023, p. 5.

[64] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020.

prospere e più sostenibili[65]». Nonostante i riferimenti più o meno espliciti a questa ideale città tecnologica ed innovativa, non esiste ad oggi una accezione condivisa di *smart city*. Dietro al label "*Smart city*" si sommano decine di diverse definizioni della Città intelligente. Alcune di esse si basano sugli obiettivi che la città si pone di raggiungere, altre sui servizi implementati, oppure sull'uso più o meno massiccio delle nuove tecnologie nella fase di elaborazione di nuove politiche o ancora sulla partecipazione dei cittadini alla vita della comunità[66]. Ed in effetti l'aggettivo "*smart*" può essere attribuito ad un ventaglio amplissimo di applicazioni concrete, che spaziano dai sistemi di video-sorveglianza (anche biometrica[67]), alle *smart grids* in grado di controllare i consumi e regolare l'utilizzo dell'energia elettrica, ai sensori che rilevano l'inquinamento atmosferico, ai sistemi integrati di *smart mobility*, sino alla prenotazione di prestazioni sanitarie[68]. A questi ambiti "tradizionali" si sono aggiunte di recente numerose altre declinazioni delle c.d. soluzioni *smart*, diffusesi rapidamente per rispondere a esigenze e bisogni contingenti. La pandemia di Covid-19, e poi il riaffacciarsi prepotente degli scenari bellici alle porte dell'Unione europea, hanno imposto cambiamenti repentini[69] e talvolta drastici di abitudini, prassi, equilibri consolidati per decenni, accelerando il percorso di ripensamento delle strategie globali e locali[70], sino ad intaccare la dimensione urbana e le modalità di erogazione

[65] Cfr. Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020, p. 3.

[66] Per una rassegna, E. FERRERO, *Le smart city nell'ordinamento giuridico*, in Il foro amministrativo, 4/2015, p. 1267 ss.; ved. anche B. MURGANTE, G. BORRUSO, *Smart cities: un'analisi critica delle opportunità e dei rischi*, in GEOmedia, n. 3/2013; V. MOSCO, *The Smart City in a Digital World*, Emerald Publishing Limited, 2019; K. LOFGREN, C. W. R. WEBSTER, *The value of Big Data in government: The case of 'smart cities'*, in *Big Data & Society*, January–June 2020, pp. 1–14; S. RANCHORDAS – A. KLOP, *Data-driven regulation and governance in smart cities,* cit., p. 1 ss.

[67] Cfr. C. BUZZACCHI, *Le smart cities tra sicurezza delle tecnologie e incertezza della dimensione democratica*, in C. BUZZACCHI, P. COSTA, F. PIZZOLATO (a cura di), *Technopolis. La città tra mediazione giuridica e profezia tecnologica*, Giuffrè Francis Lefebvre, Milano, 2019, p. 89 ss.

[68] Nelle Smart cities *«[…] i cittadini attraverso un'applicazione presente nei propri smartphones hanno accesso in tempo reale ai dati sul traffico, sui parcheggi disponibili, sulla qualità dell'aria, sui tempi di attesa dei mezzi pubblici, sulle farmacie di turno aperte, sul numero dei pazienti presenti nel pronto soccorso. Tutto ciò grazie a sensori interconnessi, i quali trasmettono le proprie rilevazioni ad un server centrale che elabora e rende disponibili le informazioni ai propri utenti*», ved. A. SOLA, *Utilizzo dei big data nelle decisioni pubbliche tra innovazione e tutela della privacy*, in MediaLaws, 24 dicembre 2020.

[69] Cfr. P. COSTANZO, *Lo "Stato digitale"*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 13.

[70] Si vedano, per tutti, i volumi *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, a cura di A. PAJNO, L. VIOLANTE, Il Mulino, Bologna, 2021; in particolare il contributo di A. PATANE', *Democrazia rappresentativa durante la pandemia: il ruolo dei consigli regionali*, Vol. I, p. 269 ss.

dei servizi: la crisi energetica ad esempio ha richiesto una gestione "intelligente" dei consumi, in gran parte nelle mani delle amministrazioni locali[71].

Forse proprio in ragione della varietà di forme che la Città intelligente può assumere, ad oggi non esiste un quadro normativo specifico che ne tratteggi la disciplina, come emerge dagli esiti del *report* di cui ci occuperemo nel prossimo paragrafo.

[71] La trasformazione digitale della pubblica amministrazione ha modificato «*la struttura del sistema di produzione e distribuzione dell'energia, dando la stura a sistemi locali di produzione e di regolamentazione, "agevolando la gestione collettiva ed economica di produzione e di consumo attraverso reti intelligenti"*», cfr. F.F. PAGANO, *Pubblica amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit. pp. 301-311.

4.2 Il Report del Parlamento europeo sull'utilizzo dell'IA nei contesti urbani

Il 30 luglio 2021 la Commissione per lo sviluppo regionale (REGI) del Parlamento europeo ha pubblicato i risultati di una ricerca su Intelligenza artificiale e sviluppo urbano[72]. Si tratta di uno studio che esamina il ruolo dell'Intelligenza artificiale nelle città e il suo impatto sulla coesione socioeconomica e territoriale all'interno delle aree urbane e tra di esse. Esso evidenzia potenzialità e rischi dell'applicazione delle tecnologie di Artificial Intelligence nei contesti urbani, e offre al contempo una ricognizione delle esperienze e delle politiche già in essere, oltre ad indicare il percorso che l'Unione europea dovrebbe seguire per favorire un approccio territoriale all'AI nel contesto urbano. Lo studio sottolinea come l'AI, combinata con altre tecnologie digitali come i *Big Data*, *l'Internet of Things*, il *cloud*, e le infrastrutture di telecomunicazione possa sfruttare al meglio l'enorme mole di dati prodotti nello svolgimento della vita cittadina. Tra i vantaggi legati all'utilizzo dell'Intelligenza artificiale nel contesto urbano la ricerca elenca il miglioramento dei profili di gestione, il sostegno al processo decisionale, lo sviluppo di nuovi servizi, la creazione di nuove opportunità economiche. I principali ambiti di applicazione dell'Intelligenza artificiale nelle *smart cities* che lo studio elenca sono l'amministrazione locale, la sanità, la sicurezza, la mobilità e l'energia. Inoltre, l'AI viene intesa come mezzo per favorire l'efficienza, migliorare la *governance* e promuovere impegno democratico e sostenibilità ambientale.

La ricerca evidenzia però anche i principali rischi che sono connessi all'implementazione di sistemi di Intelligenza artificiale nei contesti urbani. Tra di essi vengono elencati i danni per la tutela della vita privata, dovuti alla inaccuratezza nella gestione dei dati personali, le possibili discriminazioni o le decisioni sbagliate che possono essere frutto di algoritmi di cui non si può conoscere e comprendere la logica, oltre che i rischi per l'economia ed in particolare per la possibile perdita dei posti di lavoro. Rispetto all'impatto dell'utilizzo dell'Intelligenza artificiale nella dimensione socioeconomica e territoriale nei contesti urbani, lo studio evidenzia due tipi di rischi. Il primo legato al realizzarsi di discriminazioni a scapito delle fasce più vulnerabili della

[72] European Parliament, *Artificial Intelligence and Urban Development*, Study Requested by the REGI Committee Luglio 2021.

popolazione, con riflessi sulla coesione economica e sociale all'interno della città, il secondo connesso invece alla possibile perdita di coesione tra città diverse, o tra le città e le zone rurali, ove potrebbero crearsi situazioni di divario digitale (ad esempio tra realtà che sono in grado di implementare soluzioni di AI ed altre realtà meno "intelligenti").

Sul fronte delle esperienze già in essere, lo studio evidenzia come, salvi rari casi rappresentanti da città avanzate e di grandi dimensioni, vi siano ancora risultanze insufficienti per una valutazione circostanziata degli effetti della applicazione dell'Intelligenza artificiale nei contesti urbani. Valutazioni più attendibili potranno essere svolte quando l'utilizzo di questi sistemi innovativi sarà comune su larga scala. Il report si occupa anche di definire quali dovrebbero essere le principali attribuzioni in capo alle autorità pubblica, al fine di ridurre i rischi per i cittadini e potenziare al massimo i benefici dell'AI nel contesto urbano. Le condizioni minime che dovrebbero essere garantite toccano concetti-chiave del lessico della economia e della società digitale: accesso ai dati, interoperabilità, quadri giuridici e governance adeguati, ma anche capacità amministrativa, competenze specifiche, oltre che la garanzia della effettiva partecipazione dei cittadini allo sviluppo delle *smart cities* basate sull'AI.

Dal report emerge chiaramente come l'enorme mole di dati prodotti nello svolgimento della vita cittadina possa essere sfruttata al meglio attraverso l'applicazione ai *Big Data* di una combinazione di mezzi e tecnologie (*Artificial Intelligence,* infrastrutture telco, *cloud*…). Le applicazioni concrete spaziano dalla sanità, alla sicurezza, alla mobilità, all'energia, fino ad incidere sul miglioramento dei profili di gestione della città, sul *policy-making*, sullo sviluppo di nuovi servizi, sulla creazione di nuove opportunità economiche.

Il report della Commissione REGI ha evidenziato come l'azione strategica dell'Unione europea non abbia posto una attenzione specifica allo sviluppo dell'Intelligenza artificiale nelle *smart cities*, rispetto alle quali non esistono riferimenti normativi e regolamentari *ad hoc*[73]. La già citata recente pubblicazione dello studio *Social approach to the transition to smart cities* da parte del Parlamento europeo[74], conferma che il tema tende ad essere affrontato non

[73] Secondo E. SPILLER, «*la disciplina di settore spesso consiste in una sorta di* patchwork *in cui si tenta di assemblare gli istituti necessari alla realizzazione di diversi progetti*», cfr. *Citizens in the loop? Partecipazione e Smart city*, in *La città e la partecipazione tra diritto e politica*, F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), Giappichelli, Torino, 2019, p. 289..

[74] European Parliament, Panel for the Future of Science and Technology (STOA), *Social approach to the transition to smart cities*, Febbraio 2023.

attraverso interventi legislativi quanto piuttosto mediante studi tematici, finalizzati alla elaborazione e condivisione di buone pratiche e alla proposta di *policy options*[75].

[75] Si vedano in proposito i capitoli 3 e 4 dello studio, p. 30 ss..

4.3 La città come ecosistema digitale. Una chiave di lettura (e di regolazione) per le *smart cities*

Alla luce di quanto sin qui emerso, ed in particolare della mancanza di un quadro regolatorio specifico per le *smart cities*, vorremmo proseguire il percorso intrapreso all'inizio di questo contributo, applicando quello che abbiamo definito come metodo *data-driven*. Vorremmo di conseguenza ricondurre le *smart cities* entro una griglia di regole applicabili a fattispecie anche differenti – come differenti sono i "modelli" di Città intelligente [76] – ma accomunate dalla presenza di due caratteristiche essenziali, cioè la digitalizzazione e l'uso delle nuove tecnologie, in particolare l'Intelligenza artificiale [77]. La città "funziona" in quanto le persone che la popolano [78], gli enti pubblici, le società private, in diversa misura si fanno attori e fruitori di un ecosistema digitale [79].

La componente datificata della Città [80], insieme ai sistemi di Intelligenza artificiale utilizzati per estrarne conoscenza, sono dunque i due riferimenti rispetto ai quali diviene

[76] Uno degli approcci definitori descrive la *smart city* come «*un sistema di sviluppo che si caratterizza per un insieme di strategie di pianificazione urbanistica tese all'ottimizzazione e all'innovazione dei servizi pubblici allo scopo di mettere in relazione le infrastrutture materiali delle città con il capitale umano, intellettuale e sociale di chi le abita in ragione del ricorso diffuso alle nuove tecnologie della comunicazione, della mobilità e dell'efficienza energetica*», v. F.F. PAGANO, *Pubblica amministrazione e innovazione tecnologica*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., pp. 311-312. A parere di chi scrive, sebbene la descrizione proposta sia condivisibile, una impostazione incentrata sulle finalità o sui settori di sviluppo della Città intelligente rischia di escluderne *a priori* alcune declinazioni non appartenenti alla casistica dei primi "prototipi" di *smart city* ma invece oggetto di implementazione grazie al progredire dei progetti.

[77] Lo sviluppo di una *smart city* dipende infatti dalla disponibilità di ingenti quantità di dati, costantemente aggiornati e provenienti da diverse fonti, insieme alla capacità di elaborazione di tali dati attraverso tecniche di *data mining* oltre che dalla possibilità di utilizzo della stessa "materia prima" per addestrare sistemi di apprendimento automatico, anche ad un livello "profondo" (*deep-learning*), basato su interconnessioni che riproducono le reti neurali del cervello umano. J. BURREL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & Society* 3 (2016), 1, pp. 1-12.

[78] Non solo cittadini ma anche turisti, pendolari, *city-users*.

[79] La Commissione Europea nella Comunicazione "*Costruire un'economia dei dati europea*" afferma che i dati sono diventati una risorsa essenziale, e l'analisi dei dati offre potenzialità enormi in vari campi, tra cui lo sviluppo delle *smart cities*, cfr. Commissione Europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - "Costruire un'economia dei dati europea"*, COM(2017) 9 final, 10 gennaio 2017.

[80] «*Smart city solutions generate huge volumes of data, that could be structured or unstructured, originating from a variety of disparate sources and potentially requiring real-time analysis*», cfr. T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, in *The International Archives*

possibile individuare le coordinate normative imprescindibili a partire dalle quali ogni *Smart city* è chiamata a definire il proprio modello di *governance.* Basandosi sul combinato disposto delle norme, principalmente di matrice europea, che disciplinano la raccolta, l'utilizzo, il riutilizzo, la condivisione e la conservazione dei dati, personali e non personali (che nel capitolo precedente abbiamo passato in rassegna) ogni Città[81], più o meno "intelligente" può organizzare i flussi di dati nel modo più adeguato al conseguimento dei propri fini, riconfigurando servizi, prevedendo problemi, anticipando bisogni[82], e garantendo al contempo il rispetto dei diritti e delle libertà di tutti gli attori che popolano l'ecosistema digitale urbano.

Del resto, gli amministratori pubblici sono in grado di raccogliere nell'area urbana enormi e variegate quantità di dati generati o raccolti da infrastrutture e servizi pubblici, da sensori posizionati su edifici, aree di passaggio, pali della luce, dai *devices* dei cittadini collegati alle reti *wi-fi* e così via. È proprio grazie alla analisi dei dati raccolti che gli amministratori possono monitorare i fenomeni urbani e prendere decisioni basate sui dati, cioè sulle informazioni catturate in tempo reale[83]. Per un ente locale può non essere semplice gestire grandi quantità di dati, e utilizzare in sinergia vecchie e nuove modalità di raccolta, conservazione e finanche di analisi dei dati, in modo da trarne rapidamente informazioni utili e fruibili. Dunque, la disponibilità di una infrastruttura e di *policies* idonee a governare i flussi di dati, e a definire i ruoli dei soggetti coinvolti nella predisposizione e nella fruizione dei servizi (cioè a dire gli attori dell'ecosistema digitale urbano) può essere determinante per la trasformazione di una città in *smart city*[84].

of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLVIII-4/W5-2022, p. 130.

[81] Tutti i riferimenti alla Città o alla *Smart city* contenuti in questo elaborato devono intendersi come riferiti alla dimensione territoriale e alla definizione giuridica del Comune come definito dal Testo Unico degli Enti Locali, d. lgs. n. 267/2000. Urbano riflette sulla mancanza, nel nostro ordinamento, di una definizione giuridica della "città", cfr. G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, cit., pp. 463-468.

[82] F COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, cit., p. 48.

[83] J. WANG, D. QUE NGUYEN, T. BONKALO, O. GREBENNIKOV, *Smart governance of urban data*, *E3S Web of Conferences* 301, 05005 (2021), p.5; S. RANCHORDAS – A. KLOP, *Data-driven regulation and governance in smart cities,* cit., p. 6.

[84] T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, cit., p. 131.

A questo punto della riflessione si inserisce il secondo caso di studio oggetto di questa dissertazione. Il Comune di Milano, con la deliberazione della Giunta comunale n. 620 del 22/05/2020 ha infatti approvato le Linee di indirizzo per l'adozione del modello di Architettura d'impresa (*Enterprise Architecture*) e per il governo dell'Ecosistema Digitale Urbano. Si tratta di un ambizioso progetto per la realizzazione di una infrastruttura informatica e giuridica che consenta al Comune di governare la variegata e imponente mole di dati che quotidianamente fluisce nel territorio urbano della città di Milano. I flussi di dati molto spesso non sono coordinati, e gran parte del valore che potrebbe essere prodotto e sfruttato attraverso l'analisi dei dati viene disperso. Il Comune di Milano ha invece interesse ad allargare la propria base conoscitiva per elaborare politiche migliori, allineando il ciclo dei dati a quello delle decisioni. Costituire un ecosistema regolato consentirà poi, a maggior ragione, di favorire la condivisione e il riutilizzo dei dati anche da parte degli altri attori dell'ecosistema medesimo. È necessario quindi un approccio coordinato che tenga conto dei ruoli e delle esigenze della pubblica amministrazione, dei fornitori di servizi (società partecipate o aziende private), delle università e degli enti di ricerca, dei cittadini, dei pendolari, dei *city-users*. Per quanto attiene al percorso di ricerca oggetto di questo contributo, il progetto milanese potrebbe essere considerato quale caso di studio come modello di *data governance*. Per *data governance* si intende infatti una combinazione di politiche, procedure, ruoli e responsabilità, in cui vengono stabilite regole di ingaggio, poteri decisionali e responsabilità per la gestione efficace delle risorse informative[85].

[85] T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, cit., p. 130.

4.4. Caso di studio: l'Ecosistema digitale urbano del Comune di Milano

La Città di Milano da molti anni interpreta in maniera innovativa il concetto di *smart city*, conciliando innovazione ed inclusione, affiancando gli investimenti in infrastrutture, *open data*, interoperabilità e connettività *wi-fi* ad interventi volti a dare spazi, servizi ed occasioni di crescita per quei soggetti che contribuiscono a rendere più vivibile e fruibile la città. Con la delibera del 22 maggio 2020 la Giunta comunale ha approvato il progetto di realizzazione del c.d. Ecosistema Digitale Urbano, del quale in questo paragrafo passeremo brevemente in rassegna i contenuti.

Il progetto di Ecosistema Digitale Urbano si prefigge di intervenire nella città in modo sistematico per sviluppare servizi digitali accessibili a tutti i cittadini e alle imprese in ambiti quali la mobilità e i trasporti, la raccolta differenziata, la sicurezza urbana, il decoro urbano e verde pubblico, il turismo, l'istruzione e la formazione alle nuove tecnologie, la partecipazione ai processi decisionali della città e del quartiere, l'incubazione di nuove imprese e di nuovi modelli di *business* legati al territorio.

Il ruolo del Comune di Milano nello sviluppo di questo progetto viene chiarito sin dalle premesse. Infatti, l'ente locale si pone quale soggetto attivo nella erogazione dei servizi ma anche, e soprattutto, quale soggetto detentore del ruolo di governo del sistema[86]. Per garantire l'efficace gestione del patrimonio informativo comunale debbono essere promossi *standard* e regole per favorire un modello riconosciuto di trasformazione digitale (a questo fine il Comune ha applicato i principi della c.d. *Enterprise Architecture* [87]). Nella delibera di sottolinea l'importanza che l'ecosistema sia aperto a soggetti sia pubblici che privati, in quanto l'apporto

[86] L'amministrazione comunale «*ha il compito di vigilare sulle iniziative pubbliche e private in modo che non siano in conflitto, ma si sviluppino armonicamente in un ecosistema strutturato, coordinato e interoperabile*», cfr. Comune di Milano, *Deliberazione della Giunta comunale n. 620 del 22/05/2020*, *Approvazione delle linee di indirizzo per l'adozione del modello di Architettura d'Impresa (Enterprise Architecture) del Comune di Milano e per il governo dell'Ecosistema Digitale Urbano*, p. 2.

[87] «*L'Enterprise Architecture è la descrizione della struttura di un'organizzazione, dei sui processi operativi, dei sistemi informativi a supporto, dei flussi informativi, delle tecnologie utilizzate, delle localizzazioni geografiche e dei suoi obiettivi. Attraverso la conoscenza architetturale di una organizzazione complessa, quale un'impresa, è possibile: regolare l'evoluzione strategica del parco applicativo, i processi di crescita ed efficientamento, controllare i rischi operativi, garantire la qualità di dati e processi e verificare la conformità alle normative»*, cfr. Relazione tecnico-illustrativa, p. 7.

delle iniziative imprenditoriali viene considerato fondamentale. L'Ecosistema Digitale Urbano dovrà essere caratterizzato da alti livelli di integrazione e di interoperabilità dei sistemi informativi in modo che sia i privati che gli enti pubblici e le loro società partecipate possano offrire soluzioni digitali[88]. Dunque, l'adozione del modello di Architettura d'impresa consentirà al Comune di Milano di garantire una *governance* unitaria sui processi di trasformazione digitale, nel rispetto dei principi in materia di *privacy*, trasparenza e accessibilità di dati, e con protocolli interoperabili e l'adozione di *standard* specifici ed unitari, che saranno inseriti nei bandi e capitolati d'appalto.

La valorizzazione di dati prodotti negli spazi pubblici della città costituisce un obiettivo primario del progetto in esame. Invero la molteplicità di dispositivi connessi, nonché di servizi forniti da operatori pubblici e privati, dà origine, nell'area urbana di Milano, ad una produzione massiva di dati – non solo di dati ambientali, ma anche di dati relativi ai comportamenti di migliaia di cittadini – che possono essere considerati *beni comuni*, capaci di generare un valore economico e di ricerca. L'obiettivo del Comune è far sì che l'accesso a questo valore, al quale già attingono le Big Tech, sia consentito anche a realtà più piccole, cittadini, associazioni, al Comune stesso mediante opportune *policy* promosse dall'amministrazione comunale ed elaborate al fine di preservare la *privacy* e gli interessi commerciali degli operatori privati.

Non sfuggirà a questo punto che il modello di gestione dei dati del Comune di Milano, finalizzato – anche – a favorire una più equa distribuzione del valore dei dati, agevolando l'accesso agli stessi anche da parte di attori meno potenti dei *Big Players*, si pone sullo stesso solco della proposta di *Data Act* in discussione nell'Unione europea. La legge sui dati, infatti, si pone gli stessi obiettivi di ridistribuzione del valore ed equità nelle possibilità di accesso ai dati.

La relazione tecnico-illustrativa che accompagna la delibera n. 620/2020, illustra e circostanzia quanto in essa tratteggiato. Innanzitutto, vengono individuati tre principali soggetti che sono protagonisti della forte spinta all'innovazione che caratterizza il Comune di Milano. Sono i cittadini (che privilegiano i servizi digitali, l'integrazione con nuove tecnologie come i dispositivi mobili e l'opportunità di svolgere operazioni senza recarsi agli sportelli), le imprese

[88] Tra i servizi che possono essere offerti tramite iniziative imprenditoriali si fa riferimento alle soluzioni di *sharing mobility*, mentre gli esempi di servizi offerti dai soggetti pubblici riguardano la Open *wi-fi*, la videosorveglianza, le colonnine di ricarica dei veicoli elettrici, i sensori ambientali.

(che competono per offrire servizi innovativi e per evolvere su nuovi modelli di business) e l'Amministrazione comunale, che, in questo contesto, come anticipato, ricopre due ruoli differenti. Da una parte è soggetto attivo nell'erogazione di servizi digitali ai cittadini e alle imprese, dall'altra riveste un ruolo di governo.

Il modello di Architettura d'impresa è inteso come ponte strategico fra la Direzione Sistemi Informativi e tutte le altre direzioni, in modo che tutte le nuove progettualità o i cambiamenti rilevanti che abbiano impatto sullo sviluppo di sistemi informativi siano validati a livello di governo centrale. Il modello di Ecosistema Digitale Urbano elaborato dal Comune di Milano si articola poi su quattro direttrici: gli attori, le infrastrutture, i servizi digitali e gli ambiti di applicazione.

Gli attori sono individuati in: Comune di Milano, cittadini e *city-users* (lavoratori, pendolari e turisti), imprese (specie quelle in cui l'ICT ha un ruolo rilevante), i *freelancers* (liberi professionisti, specie del settore IT…), i *civic hackers* (ovverosia i cittadini attivi nei processi partecipati, che impiegano le proprie competenze per trovare nuove soluzioni sulla base dei dati e dei servizi digitali resi pubblici, suggerire nuove connessioni e nuove necessità, nel quadro di un dialogo costruttivo con la PA), le associazioni e il terzo settore, altri enti pubblici che svolgono attività nel Comune di Milano (ad esempio la Regione Lombardia, la Città metropolitana di Milano, l'Agenzia delle Entrate, la Camera di Commercio, l'INPS, il Tribunale di Milano ecc.)[89].

La *policy* di condivisione elaborata per l'Ecosistema[90] è finalizzata a fornire un indirizzo tecnologico uniforme per i soggetti operanti sul territorio e al contempo ad incentivare la condivisione regolamentata dei flussi tra quegli stessi soggetti. Il Comune di Milano utilizza per il proprio Ecosistema Digitale Urbano *standard* di interoperabilità tecnologica, glossari di dati e ontologie definiti a livello nazionale dal Piano Triennale per l'Informatica nella Pubblica

[89] Relazione tecnico-illustrativa, p. 18. Ved. W. OOMS, M. C. J. CANIËLS, N. ROIJAKKERS, D. COBBEN, *Ecosystems for smart cities: tracing the evolution of governance structures in a dutch smart city initiative*, in *International Entrepreneurship and Management Journal* (2020) 16, p. 1226: «*Smart city governance needs to work with (and affect) processes at various levels: national and local policies, corporate strategies of the firms involved, academic leadership at the universities that partner in the initiatives, and so on*».

[90] Servizi e dati debbono essere condivisi attraverso interfacce applicative (API) *standard*.

Amministrazione[91]. Il Gruppo di coordinamento trasversale costituito all'interno dell'ente determina la *governance* del sistema definendo le strategie e gli interventi necessari.

Le coordinate per la realizzazione del progetto delineato nella Delibera n. 620/2020 rivestono particolare interesse in quanto attraverso la definizione di soggetti, ruoli, responsabilità e regole l'ente locale *costituisce* un modello di convivenza per tutti gli attori dell'ecosistema digitale. Le regole per il governo dei dati si rivelano dunque strumenti utili per descrivere, e poi gradualmente disciplinare, tutte le manifestazioni della inafferrabile *smart city*[92].

Prima di concludere su questo caso d'uso, per completezza, pare opportuno ricordare che di pari passo con la digitalizzazione dei servizi e la creazione di un ecosistema digitale necessariamente cambia la città nella sua componente materiale. Rodotà ci ricordava già nel 1997 che i servizi molto spesso non si risolvono nell'informazione, e non perdono la loro concretezza, per cui la localizzazione fisica resta essenziale. Dunque «*l'intreccio tra dematerializzazione di taluni servizi […] e il permanere di un ineliminabile aggancio al territorio tradizionalmente inteso impone una ristrutturazione sempre più marcata dell'intera rete dei servizi, con riflessi evidenti sull'organizzazione e sull'idea stessa di città*[93]».

[91] Ved. supra, par. 1.3.2.

[92] «*Smart city governance, is identified as a key driving force to enable smart city development*», cfr. W. OOMS, M. C. J. CANIËLS, N. ROIJAKKERS, D. COBBEN, *Ecosystems for smart cities: tracing the evolution of governance structures in a dutch smart city initiative*, cit., p. 1226.

[93] S. RODOTA', *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Bari, 1997, p. 129.

4.5 Dal *data management* alla *data governance*

La delibera n. 620/2020 del Comune di Milano adotta un modello di *data governance* per il contesto urbano digitalizzato. Esso prevede infatti una combinazione di politiche, procedure, ruoli e responsabilità, in cui vengono stabilite regole di ingaggio, poteri decisionali e responsabilità per la gestione efficace delle risorse informative[94]. Questo caso di studio ci consente di osservare quali sono in concreto le differenze tra il modello di *data management* che può essere costruito sulla base delle indicazioni che si possono trarre dalle regole di *compliance* al regolamento europeo 2016/679 in materia di protezione dei dati personali, e modelli più ampi di governo dei dati, che racchiudano al loro interno la disciplina di un intero sistema digitale, che riguardi i flussi di tutte le tipologie di dati, i numerosi attori coinvolti nel loro trattamento e l'attribuzione dei poteri decisori in merito alla valorizzazione del patrimonio informativo.

Quel che si vuole evidenziare è che il processo di adeguamento al GDPR, e quindi di mappatura e razionalizzazione di tutti i flussi di dati e delle ramificazioni all'interno di un apparato amministrativo, costituisce uno *step* fondamentale e prodromico allo sviluppo di sistemi più complessi di *governance* dei dati *tout court*. Per chiarire questo punto sarà bene richiamare le definizioni di *data management* e *data governance*.

Mentre per *data management* si intende l'insieme di regole e *policies* che regolano la gestione dei dati all'interno di una organizzazione[95], il concetto di *data governance* comprende e supera quello di *data management*. Infatti, oltre alla gestione del patrimonio informativo, come abbiamo avuto modo di osservare, il modello di *data governance* proposto determina la distribuzione del potere e regola i rapporti tra i vari soggetti che interagiscono in un determinato contesto[96](nel nostro caso di studio, nell'Ecosistema Digitale Urbano). Gli ecosistemi delle città

[94] T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, cit., p. 130.

[95] *Data management* is *«the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets*», cfr. M. AL-RUITHE, E. BENKHELIFA, K. HAMEED, *A systematic literature review of data governance and cloud data governance*, in *Personal and Ubiquitous Computing* (2019) 23:839–859, p. 841.

[96] *Data governance* is «*the exercise of authority, control, and shared decisionmaking (planning, monitoring, and enforcement) over the management of data assets*», cfr. M. AL-RUITHE, E. BENKHELIFA, K. HAMEED, *A systematic literature review of data governance and cloud data governance*, cit., p. 841.

intelligenti, a differenza di altre organizzazioni "privatistiche" si prestano agevolmente ad una lettura "costituzionale", in quanto, ad esempio, includono nelle loro dinamiche i cittadini, considerati attori al pari degli altri soggetti (la pubblica amministrazione, le aziende, le università…). Gli ecosistemi digitali urbani inoltre sono più orientati alla realizzazione di servizi, in quanto i loro obiettivi principali riguardano la trasformazione della vita degli individui e il miglioramento del benessere della società [97], e le relazioni che in essi si creano sono potenzialmente più durature rispetto ad altre forme di collaborazione, in quanto gli attori dell'ecosistema perseguono obiettivi comuni e non sempre passibili di essere raggiunti in tempi brevi, a causa della loro complessità. Infine, negli ecosistemi, è più probabile che i partner si impegnino nella strategia congiunta e nella creazione e appropriazione di valore condiviso a livello di sistema piuttosto che a livello individuale[98].

Il tentativo di analisi della *smart city* nella sua componente digitale ci ha consentito di individuare una serie di norme e regole che, disciplinando le modalità di trattamento e condivisione dei dati, rappresentano l'intelaiatura dei sistemi di governo dei dati che gli enti locali debbono progressivamente costruire. Ma va sottolineato il modello appena descritto potrebbe essere applicato ad ogni livello di governo, premessa una fase "costituente" in cui vengano identificati i poteri, i ruoli, le regole. Ad esempio, a livello di area vasta, la Città metropolitana potrebbe individuare regole di governo dei dati all'interno della propria funzione di coordinamento dei sistemi di informatizzazione e digitalizzazione, realizzando il modello di *smart landscape* evocato nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021. Un raccordo tra gli enti locali su più ampia scala sarebbe sicuramente auspicabile, a fronte del debole esercizio da parte dello Stato della funzione di coordinamento informativo, informatico e statistico di cui al secondo comma dell'articolo 117 della Costituzione, che, unito alla tendenza delle pubbliche amministrazioni a conservare la propria autonomia organizzativa, ha contribuito alla creazione di quelle che sono state definite "*dodicimila città-Stato*

[97] «*A data governance framework designed specifically for smart cities, will enable the city to extract the most possible value from its data assets, thereby supporting decision-making processes, improving operational efficiency and ensuring regulatory compliance, for the ultimate purpose of improving the quality of life of its citizens, visitors and businesses alike*», cfr. T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, cit., p. 134.

[98] W. OOMS, M. C. J. CANIËLS, N. ROIJAKKERS, D. COBBEN, *Ecosystems for smart cities: tracing the evolution of governance structures in a dutch smart city initiative*, cit., p. 1229.

digitali[99]*"*[100]. È utile ricordare che nella Comunicazione della Commissione europea "*Bussola per il digitale 2030: il modello europeo per il decennio digitale*[101]*"* l'interoperabilità[102] a tutti i livelli di governo e tra i servizi pubblici viene indicata come strategia di interazione tra cittadini, pubbliche amministrazioni e istituzioni democratiche. In continuità con quello *statement* si pone la successiva Comunicazione "*Collegare i servizi pubblici, sostenere le politiche pubbliche e garantire benefici pubblici Verso un'"Europa interoperabile"*[103]*"* nella quale la Commissione esordisce affermando che «*I servizi pubblici digitali interoperabili sono essenziali per digitalizzare con successo il mercato unico dell'Unione europea*[104]». Non è priva di pregio, alla luce di quanto appena ricordato, la scelta del Comune di Milano di inserire nella architettura dell'Ecosistema Digitale Urbano uno *standard* di interoperabilità tecnologica che dovrà essere utilizzato da tutti gli attori dell'ecosistema medesimo[105].

[99] L. ATTIAS, *Audizione davanti alla Commissione parlamentare sulla semplificazione*, 20 marzo 2019.

[100] F.F. PAGANO, *Pubblica Amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 305.

[101] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM/2021/118 final, 9 marzo 2021.

[102] Intesa, nella definizione contenuta nel Codice dell'Amministrazione Digitale, come 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 (ved. d. lgs. n. 82/2005, art. 1 comma 1 lett. dd).

[103] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa al rafforzamento della politica del settore pubblico in materia di interoperabilità "Collegare i servizi pubblici, sostenere le politiche pubbliche e garantire benefici pubblici Verso un'"Europa interoperabile"*", 18 novembre 2022.

[104] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa al rafforzamento della politica del settore pubblico in materia di interoperabilità "Collegare i servizi pubblici, sostenere le politiche pubbliche e garantire benefici pubblici Verso un'"Europa interoperabile"*", 18 novembre 2022, p. 2.

[105] Cfr. *supra*, par. 4.4.

4.6 La necessità di un fondamento costituzionale dei modelli di *governance* dei dati

Nel concludere il capitolo dedicato alla *governance* dei dati nella *smart city* occorre sottolineare che i modelli di governo dei dati applicati agli ecosistemi digitali urbani, pur offrendo degli strumenti concreti per amministrare una *smart city*, non possono definirne il profilo se non negli aspetti "tecnici" e solo latamente costituzionali. Invero però, sono numerosi i diritti fondamentali e i profili costituzionali coinvolti nelle dinamiche legate all'utilizzo delle nuove tecnologie nei contesti urbani. Detto altrimenti, l'amministrazione dei centri urbani non potrà ridursi a una logica di mera ottimizzazione dei servizi, ma dovrà piuttosto perseguire il benessere della totalità dei cittadini, comprese le minoranze. Ciò richiede il governo in chiave democratica non solo della città, ma anche del progresso digitale che la attraversa. In questi termini, l'amministrazione locale non solo deve tendere all'efficienza dei servizi che eroga, anche grazie alle *partnership* con imprese private, ma deve vigilare sul godimento delle prestazioni da parte di tutti i cittadini, secondo criteri di uguaglianza e solidarietà[106].

Nelle prossime pagine si farà cenno ad alcuni di questi profili, che consentiranno, sulla base del percorso di ricerca svolto, di svolgere riflessioni più ampie sulle rilevanti questioni giuridiche connesse alla *governance* dei dati nel settore pubblico.

[106] D. TESTA, *Governo e autogoverno della città digitale, luogo di conflitti tra valori pubblici e interessi privati,* in Diritto pubblico comparato ed europeo, Fascicolo 1/2023, gennaio-marzo, pp. 185-186.

CAPITOLO 5 – CONCLUSIONI

5.1 Considerazioni conclusive

L'itinerario di ricerca sin qui svolto ha consentito di esplorare le potenzialità di utilizzo di un modello di governo dei dati ai fini della amministrazione di quelle che vengono definite Città intelligenti. L'utilizzo dei dati nei contesti urbani però, proprio per il coacervo di diritti, doveri, interessi, dinamiche che in essi prendono forma, richiama lo studioso e l'amministratore a riflessioni di carattere costituzionale. Nei prossimi paragrafi verranno dunque proposte alcune considerazioni, partendo dalla normativa, passando per le questioni di *governance*, per poi giungere ad alcuni spunti sulle prospettive future.

5.2 Sull'apparato normativo

Per quanto riguarda i più rilevanti aspetti emersi dalla analisi del contesto normativo, pare di dover dare conto, innanzitutto della posizione sovraordinata del regolamento n. 2016/679 rispetto alle altre normative europee in materia di dati. Vi è da dire infatti che la *data governance* di un ente pubblico si basa innanzitutto sulla *compliance* al GDPR e trova nelle sue regole le coordinate fondamentali per costruire un sistema di gestione dei dati che comprenda tutte le categorie e le tipologie di flussi. Questa affermazione è supportata da almeno tre elementi.

Il primo attiene alla rilevanza che la tutela dei dati personali ha rispetto alle altre regole di gestione dei dati non personali[1]. La normativa in materia di dati personali, introdotta in sede europea nel 1995 per far sì che il libero scambio di merci, servizi, persone e capitali non fosse rallentato da leggi non uniformi in materia di dati personali, è stata fin dall'inizio connotata da una forte componente personalista, per cui il trattamento dei dati personali viene sottoposto a molte regole e garanzie in quanto espressione digitale della persona umana. Tale impostazione è stata poi confermata con l'inserimento della protezione dei dati personali tra i diritti elencati nella Carta dei diritti fondamentali dell'UE e con l'articolo 16 del TFUE[2] nel quale la protezione dei dati personali è considerata un diritto fondamentale. L'art. 16 ha poi costituito la base giuridica sulla quale è stato emanato il regolamento n. 2016/679. La normativa in materia di protezione dei dati personali è dunque ontologicamente diversa rispetto alle altre norme che regolano i flussi di dati non personali[3]. Questa diversità si esprime anche nella gerarchia tra le

[1] Contra, G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., in particolare p. 975, il quale ritiene che la primazia della normativa in materia di protezione dei dati personali sia destinata a cedere il passo ad un nuovo modello di regolazione in cui libero accesso, riuso e *data protection* avranno pari dignità.

[2] Ved. P. PIRODDI, *art. 16 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, cit..

[3] Confermano in modo netto la primazia del GDPR nel sistema giuridico europeo il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati, nel parere congiunto sulla proposta di Data Governance Act: «*EDPB e EDPS rilevano inoltre che il modello dell'Unione europea si basa sull'integrazione dei suoi valori e diritti fondamentali nello sviluppo delle sue politiche e che il GDPR deve essere considerato un fondamento sul quale costruire un modello di governance europea dei dati*», cfr. Comitato europeo per la protezione dei dati, Garante europeo della protezione dei dati, *Parere congiunto EDPB – EDPS 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance dei dati (Atto sulla governance dei dati)*, p. 8.

leggi in materia di dati. Questo è il secondo punto. Il regolamento n. 2016/679 viene richiamato da tutte le normative seguenti in materia di dati, ed in nessun caso vi è una deroga al GDPR. Al contrario sono le altre norme a cedere rispetto alle regole poste dal regolamento medesimo. Si può far riferimento, in questo senso, al regolamento FFD[4], alla proposta di AIA[5], al DGA[6], alla proposta di Data Act[7]. Si tratta di una serie di interventi che «*realizzano una sorta di "GDPR by default", posto che la normativa sulla protezione dei dati personali viene sempre dichiarata intangibile e prevalente*[8]». La terza ragione per cui, sicuramente, nella costruzione di un modello di *governance* dei dati negli enti locali occorre partire dal GDPR è la considerazione della rilevanza quantitativa e qualitativa dei dati personali rispetto alla totalità di dati raccolti e trattati quotidianamente in ambito urbano. Sul versante del trattamento dei *non-personal data*, il regolamento n. 2018/1807[9], c.d. FFD (*Free Flow Data Regulation*) pone regole volte a garantirne la libera circolazione. L'indicazione di maggior rilievo in merito alla *data governance* dell'ecosistema digitale urbano è nell'art. 2 par. 2 ove vengono delineate le regole di gestione degli insiemi di dati misti. La norma in questione stabilisce che ove all'interno di uno stesso insieme non sia possibile scindere i dati personali da quelli non personali, in quanto indissolubilmente legati, all'intero *dataset* verrà applicata la disciplina più tutelante per le persone fisiche, quella contenuta nel GDPR. Gli insiemi di dati misti peraltro rappresentano la stragrande maggioranza dei set di dati[10], e con ogni probabilità rappresentano anche la maggioranza di flussi di dati che alimentano le s*mart cities.* Ad esempio, in un sistema integrato di mobilità, dati aggregati relativi al trasporto pubblico urbano (i dati sull'accesso dei viaggiatori alla rete tramviaria) potrebbero essere analizzati congiuntamente a dati relativi all'utilizzo del

[4] Ved. art. 2 par. 2.

[5] Ved. Considerando n. 24, artt. 29 par. 6, 10 par. 5, 54.

[6] Ved. Considerando nn. 4, 35, art. 1 par. 3.

[7] Ved. Considerando n. 7, art. 1 par. 3.

[8] D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law and Technologies*, 1/2022, p. 54.

[9] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. Si veda S. TORREGIANI, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in *federalismi.it*, 10 giugno 2020.

[10] Cfr. COMMISSIONE EUROPEA, Comunicazione della Commissione al Parlamento europeo e al Consiglio Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final, p. 8 ss.

bike-sharing. In questa seconda ipotesi il processo di identificazione dell'interessato-fruitore del servizio risulterebbe molto meno complesso rispetto al primo[11].

Il secondo aspetto su cui vale la pena di soffermarsi in merito al panorama normativo esplorato nel corso della ricerca, è rappresentato dalla emersione di una inversione di tendenza nella disciplina dei flussi di dati, caratterizzata da una inedita maggiore attenzione alle possibilità, per il settore pubblico, di avere a disposizione un volume maggiore di dati da utilizzare per svolgere i propri compiti.

La strategia europea, nel suo complesso, essendo molto orientata allo sviluppo del mercato unico, sembra lasciare in secondo piano lo sviluppo della *data society* nel settore pubblico. Per meglio dire, lo sviluppo di politiche e servizi per la collettività è sembrato sin qui essere in posizione servente rispetto ai principali obiettivi di espansione del *Digital Single Market*. A fronte di un intero sistema di norme volte alla massima apertura e condivisione dei dati del settore pubblico in direzione G2B (*Government to Business*), risultano significativamente minori gli interventi volti ad accrescere la possibilità per le Amministrazioni pubbliche di fruire del patrimonio informativo privato[12].

Tale impostazione appare come una espressione della visione globale dell'Unione, che traspare da un'attenta lettura del documento *Shaping Europe's Digital Future.* Dal documento appena citato emerge infatti una evidente opzione per le tematiche dell'economia[13]. La sezione dedicata alla società[14] è piuttosto incentrata sulla difesa della democrazia e la tutela della legalità e dei valori europei anche nella dimensione digitale, mentre nulla si dice sullo sviluppo e l'ammodernamento delle Pubbliche Amministrazioni, di fronte alle sfide che le stesse debbono fronteggiare per governare il mercato e l'intera società digitale. Così quello che appare dalla lettura del documento di lancio della strategia digitale europea è la conferma di un divario tra il

[11] Sul tema della reidentificazione ved. Gruppo di lavoro Articolo 29 per la protezione dei dati, Parere 5/2014 sulle tecniche di anonimizzazione, 10 aprile 2014.

[12] Relativamente alla condivisione dei dati dal settore privato a quello pubblico si veda European Commission*, Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the high-level expert group on business-to-government data sharing*, 2020, 31 ss.

[13] «*For the development of many products and services, data needs to be widely and easily accessible, and simple to use and process. Data has become a key factor of production, and the value it creates has to be shares back with the entire society participating in providing the data*», cfr. European Commission, *Communication: Shaping Europe's Digital Future*, 19 febbraio 2020.

[14] Denominata "*An open, democratic and sustainable society*".

settore pubblico ed il settore privato, ove si guarda allo sviluppo del mercato e non dei servizi e della efficienza della PA. Forse in questi dettagli si nasconde l'opzione per il mercato.

Gli ultimi interventi normativi in tema di flussi di dati sembrano segnare, come anticipato, una, seppure ancora limitata, inversione di rotta, e una maggiore attenzione ai flussi di dati dal settore privato a quello pubblico. E' bene chiarire che l'Unione europea ha deciso di imprimere una spinta allo sviluppo del Mercato Unico Digitale attraverso interventi volti innanzitutto ad aumentare la quantità di dati a disposizione delle imprese[15], anche ai fini dell'addestramento dei sistemi di Intelligenza artificiale[16], attraverso l'approvazione di norme, l'individuazione di strumenti idonei, la realizzazione di infrastrutture, la creazione di competenze per la gestione dei dati per favorire l'aumento di dati conservati ed elaborati nell'UE[17] per realizzare uno spazio unico europeo dei dati affidabile ed attraente per investitori ed imprese.

Ma al contempo è la stessa Commissione a constatare che mentre l'utilizzo dei dati del settore pubblico da parte delle imprese è ormai da lungo tempo ampiamente garantito da politiche consolidate dell'Unione, al contrario i dati del settore privato messi a disposizione del settore pubblico non sono ancora sufficienti affinché possano essere utilizzati e valorizzati in termini di miglioramento delle politiche e dei servizi pubblici[18]. Di conseguenza, seppure all'interno di una serie di interventi finalizzati innanzitutto a favorire la libera circolazione dei dati nello spazio giuridico europeo e ad aumentarne il volume a disposizione delle imprese, alcune iniziative legislative della Commissione appaiono mirate a garantire anche agli attori del settore pubblico la disponibilità di dati sufficienti per la predisposizione di politiche *data-driven* a beneficio della collettività.

Il *Data Governance Act* (regolamento europeo 2022/868), di recente approvazione, nel quale vengono disciplinate le modalità di condivisione dei dati e viene introdotto il nuovo istituto del c.d. altruismo dei dati, e la proposta di *Data Act*, che prevede una ipotesi molto rilevante (se confluirà nel testo definitivo della legge) di acquisizione d'imperio dei dati in possesso di soggetti

[15] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020, p. 5.

[16] *Ivi*, p. 3.

[17] *Ivi*, p. 5.

[18] *Ivi*, p. 7.

privati da parte delle autorità pubbliche, per specifici motivi di necessità[19] sono il segno di una inedita attenzione del legislatore europeo verso l'efficienza della pubblica amministrazione.

Del resto, sulla stessa linea si collocano gli interventi volti a sviluppare i sistemi di interoperabilità. Il cambiamento di rotta è confermato dalla Comunicazione della Commissione europea, relativa al rafforzamento della politica del settore pubblico in materia di interoperabilità del 18 novembre 2022[20]. In questo documento viene infatti evidenziata la cruciale importanza per lo sviluppo dell'economia europea, di una amministrazione pubblica efficiente [21]. La medesima tendenza verso l'impiego della digitalizzazione quale strumento di semplificazione e la razionalizzazione delle procedure amministrative si evince anche dalle misure contenute nel PNRR riguardanti il potenziamento dell'Amministrazione digitale. Il PNRR prevede, infatti, la "*reingegnerizzazione, in chiave digitale, della disciplina dei procedimenti medesimi, da effettuare, tra gli altri, secondo i principi della soppressione degli adempimenti non più necessari, della riduzione dei tempi e dei costi, della trasparenza e dell'affidamento, della integrale digitalizzazione e della interoperabilità digitale*"[22].

Concludendo sui profili normativi, occorre dare conto della una sempre crescente tendenza espansiva della funzione regolatoria della *soft law* rispetto alla *hard law.* Il passaggio dalla "*preistoria dell'Internet*" alle sfide poste dalla digitalizzazione (*Big Data analytics,*

[19] Ved. *supra*, par. 3.3.2.

[20] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa al rafforzamento della politica del settore pubblico in materia di interoperabilità "Collegare i servizi pubblici, sostenere le politiche pubbliche e garantire benefici pubblici Verso un'"Europa interoperabile"”*, 18 novembre 2022.

[21] «*Il miglioramento delle prestazioni del settore pubblico grazie alla piena attuazione dell'interoperabilità a tutti i livelli dell'amministrazione potrebbe portare, secondo le stime, a un aumento dello 0,4 % del PIL dell'UE. I cittadini potrebbero risparmiare fino a 24 milioni di ore l'anno, ossia 543 milioni di EUR e le imprese 30 miliardi di ore l'anno, ossia 568 miliardi di EUR l'anno. Il risparmio annuo stimato sui costi grazie all'interoperabilità transfrontaliera è compreso tra 5,5 e 6,3 milioni di EUR per i cittadini e tra 5,7 e 19,2 miliardi di EUR per le imprese. Gli studi di casi dimostrano inoltre che l'interoperabilità ha un effetto positivo su altri valori pubblici, al di là degli incrementi di efficienza. Ad esempio i servizi pubblici proattivi o il sostegno semantico multilingue migliorano l'accesso ai servizi pubblici e la loro inclusività, aumentando la fiducia dei cittadini*», cfr. Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa al rafforzamento della politica del settore pubblico in materia di interoperabilità "Collegare i servizi pubblici, sostenere le politiche pubbliche e garantire benefici pubblici Verso un'"Europa interoperabile"”*, 18 novembre 2022, p. 4.

[22] F.F. PAGANO, Pubblica Amministrazione e innovazione tecnologica, in P. COSTANZO, *Lo "Stato digitale"*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 308.

Intelligenza artificiale, Internet of Things ecc.) ha reso necessario, secondo un paradigma efficientistico, un maggiore impiego di strumenti flessibili, altamente specializzati e soggetti a rapida e costante rivisitazione[23]. Tutto questo perché la regolazione della tecnologia richiede un'anticipazione rispetto a eventi che siamo abituati a regolare classicamente *ex post*, dato che in moltissimi casi, quando una certa soluzione tecnologica è già stata adottata o realizzata, diviene estremamente difficile condizionarne – o impedirne – l'uso attraverso norme e sanzioni di natura pubblica[24].

La velocità di comparsa di nuovi fenomeni tecnologici, con le loro conseguenze economiche, politiche, sociali, ha accentuato il ritardo che la legge sconta rispetto alla regolazione della realtà, rendendo spesso le norme obsolete prima ancora di essere entrate in vigore, perché nel frattempo le innovazioni hanno superato quanto poteva essere conosciuto e regolato.

Un esempio di questa rapida obsolescenza normativa ci viene fornito dall'applicazione del regolamento europeo n. 2016/679 ai *Big Data*. In dottrina molti illustri autori hanno evidenziato i limiti dell'impostazione del GDPR, quale normativa sui dati più di altre organica e dettagliata, nel disciplinare fattispecie di trattamento che, con l'avvento dei *Big Data*, sfuggono alle regole previste per trattamenti di insiemi di dati di minori dimensioni e privi delle caratteristiche riassunte nelle "V". Tra questi basti citare Franco Pizzetti, secondo la cui autorevolissima opinione *«[…] nell'evoluzione in atto della società digitale, basata sui Big Data, sulla Data analysis, sul machine-learning e sull'Intelligenza artificiale in tutte le sue applicazioni, ogni persona fisica è interessata alla tutela dei propri dati in qualunque momento, indipendentemente dal fatto che i dati a lei riferibili siano o no oggetto di un trattamento in atto*»[25], quindi ben oltre i "trattamenti " che ricadono formalmente nello schema disciplinato dal GDPR.

[23] D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra Codici di condotta e meccanismi di certificazione*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 375.

[24] A. SIMONCINI, *La dimensione costituzionale dell'Intelligenza artificiale*, in *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), Il Mulino, Bologna, 2022, p. 149.

[25] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 41. L'A. sottolinea anche come la corretta applicazione del principio di esattezza ed aggiornamento dei dati contenuto nell'articolo 5 del GDPR vieti di utilizzare i Big Data come "pesca a strascico" di dati, senza avere

A causa della velocità dei cambiamenti tecnologici, economici e sociali nel mondo contemporaneo, i parlamenti sono sempre meno in grado di elaborare testi legislativi completi e di operare tempestivamente gli aggiornamenti necessari, così in molti casi la legge si limita a porre i principi fondamentali della disciplina di una determinata materia e delega agli apparati amministrativi il compito di stabilire in via sublegislativa, con atti normativi e con altri tipi di atti (linee guida, circolari, norme tecniche ecc.), le regole di dettaglio volte a disciplinare anche i comportamenti dei privati[26].

È evidente, dunque, come il fenomeno tecnologico, più di altri, metta in crisi i sistemi costituzionali a forma di governo parlamentare, spostando il compito della normazione dalla legge primaria a strumenti regolativi di nuova generazione, come la *soft law*[27]. Le difficoltà incontrate dal Parlamento nell'intervenire rapidamente su settori caratterizzati da profili altamente specialistici – ed in particolare sulla innovazione tecnologica - hanno favorito l'emersione delle autorità amministrative indipendenti, dotate di incisivi poteri normativi, i cui atti, finiscono inevitabilmente per concorrere con le regole dettate da soggetti dotati di legittimazione democratica diretta o almeno indiretta[28]. Come si è appena ricordato, la *soft law* è considerata da sempre lo strumento ideale per governare fenomeni in continua evoluzione.

Questo ha fatto sì che, di pari passo con l'innovazione tecnologica, sia cresciuta l'importanza del ruolo delle Autorità indipendenti e di tutti gli organismi, altamente specializzati, in grado di regolare la realtà più velocemente ed in modo più specifico, attraverso i citati strumenti di *soft law.* Questi regolamenti, opinioni, linee guida costituiscono oggi l'ossatura del sistema, l'insieme di regole che disciplinano effettivamente la *Digital society* e la cui violazione può avere conseguenze molto gravi.

---

individuato a monte la finalità del trattamento posto in essere, cfr, ivi, p. 61. Sulla compatibilità dell'impianto del GDPR con il fenomeno dei Big Data si veda anche G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati e Big Data*, cit., pp. 464 ss.; G. FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., p. 237 ss.

[26] M. CLARICH, *Manuale di diritto amministrativo*, cit.7, p. 63.

[27] A. SIMONCINI, *La dimensione costituzionale dell'Intelligenza artificiale*, in *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), cit., p. 149.

[28] T.E FROSINI, *Declinazioni del governare*, Giappichelli, Torino, 2018, p. 67.

L’analisi del modello di *governance* dei dati e delle regole ad esso applicabili ci restituisce, in questa prospettiva, l’assetto sostanziale dei poteri dello Stato, riconducendo ancora una volta la questione al cuore del diritto costituzionale.

5.3 Sulla governance

Rispetto ai profili di *governance*, va innanzitutto rilevato che dall'osservazione dei modelli di governo dei contesti urbani descritti emergono spazi per sinergie che potrebbero rappresentare, se adeguatamente sostenute, applicazioni concrete del principio costituzionale di sussidiarietà orizzontale. Facciamo un passo indietro: grazie all'analisi delle dinamiche di sviluppo di un ecosistema digitale è stato possibile cogliere la dirimente importanza, nelle s*mart cities*, dell'accesso ai *Big Data* pubblici. La possibilità del loro riutilizzo rappresenta un fattore abilitante per le imprese e singoli che possono, valorizzando il patrimonio informativo urbano, agire direttamente nella gestione della *res publica*[29], in ossequio all'articolo 118 IV comma della Costituzione[30] .

L'art. 118 ultimo comma dispone, appunto, che «*Stato, Regioni, Città metropolitane, Province e Comuni favoriscono l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale*[31] *sulla base del principio di sussidiarietà*[32]». Le attività di interesse generale non rappresentano infatti oggetto di monopolio dei pubblici poteri, ma possono essere svolte anche da privati[33]. Peraltro le politiche di rigenerazione urbana, intese come strategie per migliorare la vita dei cittadini sia da un punto di vista ambientale che sociale, veicolano modelli di coinvolgimento dei cittadini in forme di amministrazione collaborativa, in cui non solo l'istruttoria ma anche la decisione ultima sono partecipate, in tal modo dando piena

[29] G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, cit., p. 474.

[30] C. CLARICH, *Manuale di diritto amministrativo*, cit., pp. 156-157; B. DI GIACOMO RUSSO, *Il principio di sussidiarietà orizzontale nell'ordinamento italiano: analisi e prospettive*, Youcanprint, Lecce, 2022.

[31] Commissione CE, Comunicazione 2001/C17/04, I servizi di interesse generale in Europa: *«[…] spetta in primo luogo alle autorità pubbliche di pertinente livello – locale, regionale o nazionale – e nella piena trasparenza definire le missioni dei servizi di interesse generale e le modalità per il loro adempimento*».

[32] «*Con la novella dell'art. 118, ultimo comma, Cost., la sussidiarietà orizzontale ha trovato espresso riconoscimento nella Costituzione, anche se parte della dottrina aveva da tempo ritenuto di poterla collocare nell'ambito di applicazione dell'art. 2 Cost., ove si afferma la centralità, nell'ambito dell'ordinamento giuridico, dell'individuo e delle formazioni sociali in cui si svolge la sua personalità*», cfr. B. DI GIACOMO RUSSO, *Il principio di sussidiarietà orizzontale nell'ordinamento italiano. Analisi e prospettive,* Youcanprint, Tricase, 2022, p. 172.

[33] B. DI GIACOMO RUSSO, *Il principio di sussidiarietà orizzontale nell'ordinamento italiano. Analisi e prospettive*, cit., p. 177.

valorizzazione al principio di sussidiarietà orizzontale[34]. Tale forma di sussidiarietà riguarda anche le circostanze in cui i soggetti privati vengono preferiti ai soggetti pubblici nel compito di erogare servizi, nel momento in cui riescano ad ottenere risultati soddisfacenti rispetto a quanto avrebbe fatto l'amministrazione pubblica[35].

Questa ultima caratteristica del principio di sussidiarietà orizzontale ci conduce al prossimo tema, che riguarda la fornitura, da parte di imprese private, di infrastrutture e servizi, necessari per l'esecuzione di compiti di interesse pubblico. Questo aspetto ha assunto dei tratti che, dato il potere immenso che le grandi aziende tecnologiche hanno acquisito negli ultimi anni, costringono a riflettere sulla tenuta dei principi del diritto costituzionale e sulla efficacia dello strumentario giuridico tradizionale nel limitare gli eccessi di questi nuovi poteri.

Il nodo giuridico appena richiamato trova applicazione concreta nei quotidiani dilemmi legati all'utilizzo dei servizi digitali offerti dai *Big Companies* internazionali. Buona parte dei servizi che caratterizzano la s*mart city* dipendono invero da infrastrutture, *know-how* e prodotti di operatori privati. Spesso si tratta di *Big Players,* attori di primo piano nella Società dei dati, dotati di potere tecnologico ed economico e di una visione strategica tale da consentire loro di porsi come interlocutori influenti, capaci di orientare le scelte pubbliche in base ad interessi non necessariamente corrispondenti alle priorità individuate dalle istituzioni rappresentative[36].

D'altronde è stato notato come nelle città intelligenti i servizi privati sempre più spesso sostituiscano o integrino i servizi pubblici esistenti[37], di fatto monopolizzando la fornitura delle tecnologie alla base delle *smart cities*[38]. Inoltre va ricordato che molto spesso le aziende fornitrici

---

[34] Cfr. B. MANNI, *Sviluppo sostenibile e rigenerazione urbana tra tutela dell'ambiente e inclusione socio-economica*, in *Diritto pubblico*, Fascicolo 1, gennaio-aprile 2022, p. 308.

[35] B. DI GIACOMO RUSSO, Il principio di sussidiarietà orizzontale nell'ordinamento italiano. Analisi e prospettive, cit., p. 181.

[36] «*La sovranità negli Stati costituzionali è intimamente legata al concetto di sovranità popolare e alla tutela dei diritti. Ma vuoto concetto sarebbe la sovranità popolare, se venisse spogliata della potestà di determinare, per mezzo dei propri rappresentanti democraticamente eletti, l'indirizzo politico generale*», cfr. *M. BETZU, Poteri pubblici e poteri privati nel mondo digitale,* in *Gruppo di Pisa, La Rivista, 2/2021, p. 170.*

[37] F.F. PAGANO, Pubblica Amministrazione e innovazione tecnologica, in P. COSTANZO, *Lo "Stato digitale"*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit. p. 312-313.

[38] D. TESTA, *Governo e autogoverno della città digitale, luogo di conflitti tra valori pubblici e interessi privati*, cit., pp. 184-185.

sono extraeuropee e pertanto sono soggette a normative meno stringenti dal punto di vista della protezione dei dati (circostanza che ha costretto l'Unione europea a programmare la costituzione di un *cloud* europeo per i dati[39]).

Abbiamo già evidenziato come il modello di *data governance* adottato per regolare i flussi di dati in un determinato contesto rappresenti la fotografia degli assetti di potere. Il caso appena descritto, relativo alla fornitura di infrastrutture e servizi digitali da parte delle grandi imprese tecnologiche in favore delle amministrazioni locali, ancora una volta porta l'attenzione alle principali questioni del costituzionalismo. Ci si chiede infatti come limitare i c.d. poteri privati[40] che hanno prepotentemente preso la scena, arrivando ad avere un peso significativo nella garanzia (o nella limitazione) dei diritti e delle libertà fondamentali[41].

L'avvento della digitalizzazione e delle nuove tecnologie ha provocato una alterazione degli assetti tradizionali del potere, con l'erompere di questi poteri privati nei tavoli una volta destinati esclusivamente a poteri pubblici. Ma questi poteri tecnologici che hanno assunto un ruolo sempre più centrale nella Società dei dati debbono essere ricondotti entro le regole (e i limiti) dell'ordinamento costituzionale, attraverso l'individuazione degli strumenti giuridici più adeguati. Dunque la domanda che ci si pone è quale sia il tipo di regolazione che può più efficacemente delimitare l'esercizio del potere tecnologico, specie quanto sono coinvolti le libertà e i diritti delle persone fisiche[42].

---

[39] D. TESTA, *Governo e autogoverno della città digitale, luogo di conflitti tra valori pubblici e interessi privati*, cit., pp. 184-185.

[40] Sui c.d. Poteri privati, *ex plurimis*, M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 39 ss; R. PARDOLESI, *Piattaforme digitali, poteri privati e concorrenza*, in *Diritto Pubblico*, 3/2021, p. 941 ss; F. MEZZANOTTE, *I poteri privati nell'odierno diritto dello sviluppo economico*, in *Politica del diritto*, 3/2018, p. 507 ss.; E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Edizioni Scientifiche Italiane, Napoli 2023.

[41] «*Un potere tecnologico come quello che si esprime attraverso l'intelligenza artificiale chiama direttamente in causa il diritto pubblico e costituzionale. Il costituzionalismo, infatti, quantomeno nella sua versione moderna, nasce proprio con lo scopo di porre un limite giuridico ai poteri (dapprima quelli privati e poi anche quelli pubblici) al fine di proteggere in maniera effettiva i diritti e le libertà fondamentali della persona*», cfr. A. SIMONCINI, *La dimensione costituzionale dell'Intelligenza artificiale*, in G.C. FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, cit., pp. 146-147.

[42] Ved. Ivi, p. 147.

In questi termini dunque l'analisi di uno *use-case* come la *smart city*, in cui convergono tutti gli attori della *Digital society*, dove si svolgono tutte le dinamiche (esercizio di diritti e libertà, attività economiche private, fornitura di servizi essenziali, governo del territorio, partenariato pubblico-privato, servizi digitalizzati e vita analogica, cultura digitale e *digital divide*), dove emergono tutti i rischi, consente di applicare l'intero strumentario giuridico per dare nomi, ruoli, regole, in definitiva per leggere la realtà.

Queste potenze economiche e digitali sempre più capaci di determinare e di orientare politiche, stili di vita e di lavoro, condizioni culturali e sociali[43], detentori dei dati, svolgono una funzione ormai ineliminabile nella fornitura di servizi e nel raggiungimento di obiettivi di interesse pubblico; non sono più solo fornitori di servizi nei confronti dello Stato, ma sono interlocutori che, come più volte ricordato, posseggono i dati e detengono il potere che deriva dalla loro analisi e da loro utilizzo, oltre che potere economico e strategico, e possono dunque interloquire con lo Stato da una posizione sicuramente non subalterna. Preso atto di questo assetto, il costituzionalista dovrà certamente interrogarsi sulle modalità di ricondurre tali rapporti di potere entro il contesto costituzionale, ma nel farlo dovrà anche chiedersi come sottoporre i nuovi attori ai doveri costituzionali[44].

Inoltre, affiancandosi ai rappresentanti democraticamente eletti dai cittadini, questi attori privati potrebbero orientare la scelta di determinate soluzioni tecnologiche piuttosto che altre per il raggiungimento di un obiettivo di pubblico interesse, di fatto però favorendo specifici interessi economici piuttosto che il bene comune. Come si potrebbero, allora, scongiurare sia il rischio di derive verso la sorveglianza universale [45] sia il pericolo che squilibri di potere economico e tecnologico provochino slittamenti verso modelli di *smart city* considerevolmente plasmati dagli interessi privati[46]?

---

[43] M. GIANNELLI*, Smart cities e dimensioni della solidarietà*, in M. GIANNELLI, V. PAGNANELLI (a cura di), *Smart cities. Diritti, libertà e governance*, Giappichelli, Torino, 2023 (in corso di pubblicazione).

[44] *Ibidem*.

[45] Si veda il provvedimento del Garante per la protezione dei dati personali relativo al sistema di riconoscimento facciale in tempo reale *SARI Real Time*, docweb n. 9575877 del 25/03/2021; ved. in proposito V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, cit., p. 793 ss

[46] «*The risk of corporate capture of public powers arises in this context since there is the significant risk that private companies will shape the way in which public bodies emply technology to pursue the public good*», S. RANCHORDAS, A. KLOP, *Data-Driven Regulation and Governance in Smart Cities*, cit., p. 33.

Il costituzionalismo nasce proprio con lo scopo di porre un limite giuridico ai poteri (dapprima quelli privati e poi anche quelli pubblici) al fine di proteggere in maniera effettiva i diritti e le libertà fondamentali della persona[47]. Servirà allora quella che Rodotà definiva una «*strumentazione istituzionale adeguata*[48]» per evitare che l'evidenza della forza dell'economia nel dettare con sempre maggior intensità e frequenza le proprie regole al diritto, anziché essere la destinataria di norme giuridiche, non distragga dalla necessità di rinnovare sulla base delle esigenze contemporanee l'originaria vocazione del costituzionalismo, tesa ad una reale e concreta limitazione dei poteri in funzione di una efficace garanzia dei diritti[49]. Questa azione potrà svolgersi entro un quadro saldamente ancorato al rispetto del principio democratico e dei diritti costituzionali. Infatti, come è stato osservato in dottrina, anche nel mondo digitale l'interpretazione evolutiva delle disposizioni costituzionali consente alle stesse di garantire le libertà della persona, fissando i criteri per realizzare il corretto equilibrio tra autorità e libertà, sia sul versante pubblicistico che su quello privatistico[50].

Le tecnologie utilizzate nelle città intelligenti hanno la capacità di aumentare il controllo e il grado di sorveglianza su ogni aspetto della vita dei cittadini, da parte dei singoli come anche dei privati, e aprono la strada a nuovi rischi sia per i diritti dei singoli che per la sovranità e la democrazia. Ai nuovi rischi, su cui dovrà concentrarsi in futuro l'attenzione di legislatori, amministratori e studiosi, è dedicato l'ultimo paragrafo.

[47] A. SIMONCINI, *La dimensione costituzionale dell'Intelligenza artificiale*, in *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), cit., p. 147.

[48] S. RODOTA', *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, p. 87.

[49] C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, Fascicolo speciale, Maggio 2019, p. 110.

[50] M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Gruppo di Pisa, La Rivista*, 2/2021, p. 172.

5.4 Sulle prospettive future

La difesa dei diritti e della democrazia è costantemente sottoposta, nell'era digitale, a vigorosi *stress-test*. La digitalizzazione, lo sviluppo delle ICTs, il progredire dell'Intelligenza artificiale hanno delle potenzialità eccezionali per il miglioramento della qualità dei servizi nel settore pubblico, oltre che in termini di semplificazione, riduzione dei costi, conoscibilità dell'azione amministrativa, esercizio dei diritti di cittadinanza, corretto svolgimento della vita democratica. I recenti accadimenti globali ne hanno dimostrato l'utilità anche per la gestione di situazioni complesse quali il contenimento di una epidemia, o la riduzione dei consumi energetici.

Ma l'accentramento di una quantità incalcolabile di informazioni in una banca dati, unito alla possibilità di incrociare tali informazioni con quelle provenienti da altri *database* utilizzando algoritmi raffinatissimi, porta con sé altrettanti gravi rischi per i diritti e le libertà dei singoli, soprattutto rispetto a possibili discriminazioni, e per la tenuta dei sistemi democratici, ove le informazioni venissero utilizzate per interferire con la libera formazione dell'opinione pubblica[51] o con lo svolgimento dell'attività politica-economica-amministrativa di uno Stato sovrano[52]. Ciò impone al settore pubblico di approcciarsi alle potenzialità dell'innovazione tecnologica nel massimo rispetto della normativa e con le cautele necessarie a salvaguardare valori fondamentali.

Le ampissime possibilità di sorveglianza e profilazione delle persone fisiche, unite all'utilizzo di algoritmi predittivi, possono come noto compromettere la libertà personale, i diritti di partecipazione alla vita democratica, la garanzia della tutela dei diritti alla salute,

[51] A titolo di esempio, sull'utilizzo delle tecniche di Deep fake si veda BERTONI F., *Deepfake, ovvero Manipula et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in Ciberspazio e diritto, vol. 20 n. 62 (1-2-2019), pp. 11-28. Più in generale, sul tema dei rischi per la democrazia ved. E. LONGO, *The Risks of Social Media Platforms for Democracy: A Call for a New Regulation*, in B. CUSTERS AND E. FOSCH-VILLARONGA (eds.), Law and Artificial Intelligence, Springer-The Asser Press, Berlino , 2022, p. 169 ss.

[52] Sulle potenzialità ed i rischi dell'utilizzo dei Big Data nel settore pubblico si veda G.M. RUOTOLO, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in Studi sull'integrazione europea, XIII (2018) pp.105 ss.; più in generale, su opportunità e rischi della democrazia al "tempo del digitale", P. COSTANZO, *La democrazia digitale (precauzioni per l'uso)*, in Diritto pubblico, I, gennaio-aprile 2019.

all'istruzione, al lavoro[53]. Scenari di questo genere sono già realtà in Paesi come la Cina[54], ove attraverso il *Social Credit System*[55] il governo tiene traccia della condotta di ciascun cittadino, ed in base allo *scoring* ottenuto concede a ciascuno l'accesso a determinati servizi, o al contrario l'esclusione dall'esercizio di alcuni diritti. Il modello cinese di sorveglianza totale degli spazi e delle persone[56], basato in larga parte sull'utilizzo di tecnologie di riconoscimento facciale si pone in totale contrapposizione, per esempio, rispetto alla moratoria sull'utilizzo di sistemi di videosorveglianza biometrica sul territorio italiano, stabilita dal decreto-legge convertito con modificazioni dalla legge 3 dicembre 2021, n. 205 (in G.U. 7/12/2021, n. 291). La moratoria, prorogata dal decreto-legge n. 51 del 2023 fino al 31 dicembre 2025 prevede infatti che l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, siano sospese fino all'entrata in vigore di una disciplina legislativa della materia.

La scelta di procedere con una moratoria, in via precauzionale, appare in linea con un approccio costituzionalmente orientato all'uso delle nuove tecnologie. La piena applicazione della Carta costituzionale italiana, incentrata sul principio personalista, pare infatti non consentire l'ingresso, nel nostro ordinamento, di modelli di applicazione dei sistemi di Intelligenza artificiale che abilitino un controllo pervasivo delle vite e dei corpi di ciascuno.

Vi possono essere però altre forme più subdole ma non meno pervasive di controllo. La combinazione dei dati raccolti grazie all'attività svolta attraverso i *devices* personali, all'utilizzo delle carte di credito, ai rapporti con la pubblica amministrazione, o ai sensori disseminati nelle

[53] Sul tema ved. la interessante analisi sui pregiudizi alle libertà che possono derivare dall'uso delle nuove tecnologie contenuta in M.S. ESPOSITO, *L'impatto del trattamento sui diritti e le libertà delle persone fisiche: una valutazione alla luce della giurisprudenza delle autorità garanti italiana e spagnola*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 219 ss.

[54] H. ROBERTS et al., *The Chinese Approach to AI: An Analysis of Policy, Ethics, and Regulation*, in *AI and Society*, 36, 2021, 59-77.

[55] Ved. R. BERTI, *Il Social Credit System cinese: un esempio di big data al servizio del potere*, in Agendadigitale.eu, 30 aprile 2019.

[56] Quella che è stata definita «*una distopia totalitaria condizionata dalla tecnologia*», cfr. Garante per la protezione dei dati personali e International Association of Privacy Professionals, Privacy 2030. Una nuova visione per l'Europa, reperibile al linkhttps://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9457003 , p. 10; ved. anche M. BETZU, Poteri pubblici e poteri privati nel mondo digitale, in Gruppo di Pisa. La Rivista, 2/2021, p. 171.

città intelligenti crea una quantità ed una qualità di informazioni riconducibili ad ogni singola persona tali da poterne tracciare un profilo dettagliato, comprensivo, ad esempio, delle preferenze politiche, dello stato di salute, dello stato di gravidanza, del livello culturale ed economico, ma anche dei gusti alimentari, dell'orientamento sessuale e delle varie preferenze, fino all'affidabilità finanziaria o alla propensione a delinquere[57].

Ancora più grave e apparentemente incontrastabile è nocività potenziale di quella che viene definita profilazione passiva [58]. Sempre più si verifica infatti una tipologia di discriminazione algoritmica in cui ciò che viene profilato è un contesto, più che un singolo individuo. Dalla osservazione di quante più persone che si muovono all'interno dello stesso contesto, e dei loro comportamenti, sarà possibile desumere – prevedere – il comportamento di singoli individui non profilati personalmente ma ricondotti per mezzo di altre correlazioni a quel determinato *cluster*.

Le nuove tipologie di profilazione basate sui *Big Data* sono incentrate su due presupposti: il volume dei dati e la loro varietà. Il volume interessa sino ad una certa misura, poiché le informazioni sulle abitudini passate di un soggetto servono a confermare uno stereotipo ma non aiutano a prevedere il comportamento futuro. A questo punto entra in gioco la varietà dei dati. Il modo migliore per prevedere una condotta infatti è osservare quante più persone possibili e integrare il profilo parziale dell'una con il profilo parziale dell'altra, piuttosto che continuare ad accumulare dati su un solo soggetto[59]. In questi termini, la *clusterizzazione* esce completamente dalla sfera di controllo (e dalle possibilità di difesa) dell'interessato[60]. Essere o non essere profilato all'interno di un gruppo, essere o non essere una minoranza

[57] C. CASONATO, Intelligenza artificiale e diritto costituzionale: prime considerazioni, in Diritto pubblico comparato ed europeo, Fascicolo speciale, Maggio 2019, p. 106.

[58] G. D'ACQUISTO, *Nuovi tipi di profilazione, ecco i rischi privacy: servono tutele più ampie*, in *AgendaDigitale*, 19 aprile 2019.

[59] *Ibidem*.

[60] «*Nella maggior parte dei casi, inoltre, l'obiettivo principale dell'analisi non è più il singolo e la profilazione dello stesso sulla base dei suoi comportamenti, quanto, piuttosto, la società nel suo insieme o determinate comunità sociali e gruppi di individui. I software per l'analisi dei Big Data vengono, infatti, per lo più impiegati per individuare caratteristiche comuni, preferenze o abitudini di una determinata collettività, al fine di predirne i futuri comportamenti ovvero di adottare decisioni che interessano tutta la comunità considerata*», M.S. ESPOSITO, *L'impatto del trattamento sui diritti e le libertà delle persone fisiche: una valutazione alla luce della giurisprudenza delle autorità garanti italiana e spagnola*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, cit.,, p. 220.

discriminata, non dipende da fattori e scelte personali ma da calcoli, previsioni, in definitiva da algoritmi.

Profilazione e decisioni automatizzate possono segregare le persone in specifiche categorie riducendo la loro possibilità di scelta, possono consolidare gli stereotipi, scoraggiare azioni rivelatrici di condotte "divergenti" (es. partecipare a gruppi di discussione su droghe, alcolismo, malattie mentali, sesso, e altri argomenti), produrre discriminazioni inattese (talvolta fondate su caratteristiche non modificabili). Ciò che rende ancora più pericoloso l'utilizzo di sistemi di *machine-learning* per profilare gli individui è la altissima possibilità che, a causa della scarsa qualità dei dati utilizzati per l'addestramento dei sistemi di Intelligenza artificiale, gli output siano gravemente discriminatori[61].

Ma vi è di più: l'algoritmo può non solo ereditare il pregiudizio preesistente attraverso l'etichettatura errata degli esempi, ma può anche riflettere un pregiudizio attuale, sino a dar vita a forme di discriminazione intenzionale, in quanto i decisori potrebbero essere in grado di mascherare attraverso la tecnica le loro intenzioni[62]. Qualsiasi forma di discriminazione che accada involontariamente può infatti anche essere orchestrata intenzionalmente[63]. Emerge quindi un tema di giustizia dei dati, intesa come equità e correttezza nel modo in cui le persone producono i dati, vengono rappresentate, classificate e trattate sulla base dei dati digitali, che deve essere usata e rispettata in tutte le fasi politiche e tecniche del "governo" dei dati medesimi[64].

---

[61] E. PELLECCHIA, *Privacy, decisioni automatizzate e algoritmi*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 422 ss.. Si parla di *data accountability* (intesa come attività di verifica e accertamento della qualità dei dati e delle tecnologie) con riferimento alla responsabilità dei soggetti pubblici per decisioni prese in base all'analisi di dati, cfr. V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 25 giugno 2018, p. 36.

[62] «*L'algoritmo, infatti, è un modello matematico che ammanta di scientificità (e, conseguentemente, di apparente oggettività) un meccanismo che riproduce le valutazioni di chi lo ha creato: insomma, "i modelli sono opinioni radicate nella matematica"*», cfr. S. SCAGLIARINI, *Identità digitale e tutela della privacy*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 352..

[63] E. PELLECCHIA, *Privacy, decisioni automatizzate e algoritmi*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 422 ss.

[64] E. LONGO, A. PIN *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *Diritto pubblico comparato ed europeo*, Fascicolo 1/2023, gennaio-marzo, p. 113.

Anche nel settore pubblico italiano, l'utilizzo degli algoritmi è evoluto nel tempo verso una sempre più stringente tendenza alla profilazione del cittadino, contribuente, lavoratore, o utente del Servizio Sanitario Nazionale, per le più svariate finalità. A questa tendenza ad un controllo più pervasivo, da realizzarsi grazie alle potenzialità dei trattamenti automatizzati, ha corrisposto un incremento dell'attività del Garante per la protezione dei dati personali.

Un caso appare particolarmente emblematico, per la rischiosità dei trattamenti proposti e per le conseguenti valutazioni dell'Autorità. Il 5 marzo 2020 il Garante ha reso un importante parere al Consiglio di Stato[65]. A sua volta il Ministero della Salute si era rivolto ai Giudici di Palazzo Spada per chiedere una valutazione relativa all'utilizzo di nuove modalità di ripartizione del fondo sanitario tra le Regioni e il Consiglio di Stato ha ritenuto di coinvolgere per competenza l'Autorità garante. Il Ministero della Salute proponeva un sistema di ripartizione del Fondo Sanitario Nazionale basato su una interconnessione tra i flussi amministrativi attivi presso il Ministero e, successivamente, un incrocio di tali flussi con le informazioni reddituali provenienti dall'Anagrafe tributaria, dai registri di mortalità, dall'ISTAT, oltre che i codici di esenzione per patologia. I profili risultanti da queste elaborazioni avrebbero consentito di procedere ad una *stratificazione* degli utenti del Servizio Sanitario Nazionale in base allo stato di salute individuale e alla situazione economica. Questa stratificazione avrebbe portato alla creazione di raggruppamenti per malattie croniche e per status sociale legato al reddito individuale.

Nel suo pronunciamento il Garante ha sottolineato la necessità di effettuare un attento bilanciamento tra interesse pubblico rilevante e tutela dei dati personali. Riconducendo esplicitamente il trattamento delineato dal Ministero della Salute alla definizione di profilazione contenuta nel GDPR[66], il Garante ha richiamato la sentenza del Consiglio di Stato n. 8472 del 2019 in cui i Giudici di Palazzo Spada avevano ricordato che dal diritto sovranazionale emergono tre principi che debbono essere applicati in presenza di decisioni automatizzate. Si tratta del principio di conoscibilità, ovvero la possibilità di conoscere l'esistenza di processi automatizzati riferiti alla propria persona e di ricevere informazioni significative sulla logica utilizzata dagli algoritmi, il principio di non esclusività della decisione algoritmica e infine il principio di non

[65] Garante per la protezione dei dati personali, Parere al Consiglio di Stato sulle nuove modalità di ripartizione del fondo sanitario tra le regioni proposte dal Ministero della salute e basate sulla stratificazione della popolazione - 5 marzo 2020, docweb n. 9304455.

[66] GDPR, art. 4 par. 1 n. 4, art. 22, ved. *ex plurimis* G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, cit., p. 219 ss.

discriminazione algoritmica "*secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo 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 che 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 che comportano misure aventi tali effetti*".

Il Garante ha poi concluso rilevando come nell'ordinamento italiano non esista una base giuridica per interconnettere i flussi informativi sanitari del Ministero della Salute e per acquisire categorie particolari di dati da altre Amministrazioni pubbliche, né sia possibile rinvenire una base giuridica idonea a fondare la prospettata attività di stratificazione di tutti gli utenti del Servizio Sanitario Nazionale.

L'esempio appena richiamato ci consente di soffermarci brevemente sulla funzione di garanzia e tutela dei diritti fondamentali dell'Autorità di controllo. È infatti nel ruolo del Garante che si uniscono una comprensione elevata delle questioni tecniche e tecnologiche sottese all'utilizzo degli algoritmi e attribuzioni poste a salvaguardia dei principi fondamentali e dei diritti delle persone fisiche i cui dati personali siano oggetto di una qualsiasi forma di trattamento: in definitiva il Garante svolge un controllo di costituzionalità tecnico e giuridico finalizzato ad individuare e correggere gli algoritmi incostituzionali[67].

Accanto ai poteri di *soft law*, il ruolo di vigilanza e regolazione del Garante può sostanziarsi invero anche attraverso specifici poteri che il GDPR attribuisce alle Autorità di controllo, tra cui quello di ottenere dal titolare o dal responsabile del trattamento l'accesso a tutte le informazioni necessarie per l'esecuzione dei suoi compiti[68]. Una interpretazione estensiva di questa disposizione potrebbe legittimare indagini molto penetranti su ogni aspetto

[67] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto, n. 1/2019*, p. 63 ss.

[68] Art. 58 par. 1 lett. e del GDPR.

della tutela dei dati personali. I compiti del Garante, infatti, comprendono la sorveglianza sull'applicazione del regolamento 2016/679 e la possibilità di svolgere indagini al fine di individuare eventuali violazioni. Non a caso nell'articolato la trattazione dei reclami e le attività di indagine sono elencati sotto punti separati.

Dunque il Garante potrebbe richiedere ai titolari di fornire informazioni sul trattamento dei dati personali, anche finalizzate a conoscere la logica sottesa agli algoritmi, e a comprendere come determinate pratiche di Intelligenza artificiale possano incidere significativamente nella sfera giuridica delle persone fisiche, anche e soprattutto quando queste non possono essere qualificate come interessati, in ragione del fatto che, come descritto in precedenza, vi potrebbe essere una scissione tra il soggetto i cui dati vengono analizzati e il soggetto destinatario di una decisione algoritmica.

La *toolbox* del Garante, delineata nel GDPR e nel Codice novellato, è ulteriormente arricchita dallo strategico potere consultivo sulla normativa primaria previsto dall'art. 58 par. 3 lett. b del GDPR[69]. Il Garante ora può di sua iniziativa, o a richiesta, rilasciare pareri al Parlamento, al Governo o ad altri organismi ed istituzioni su questioni riguardanti la protezione dei dati personali. Attraverso i pareri sulla normativa primaria l'Autorità può segnalare in anticipo eventuali criticità delle disposizioni, consentendo al legislatore di apportare i correttivi necessari al fine di garantire il pieno rispetto delle regole della protezione dati e quindi dei diritti e delle libertà degli interessati, anticipando il vaglio al momento della predisposizione degli atti normativi e regolamentari[70].

[69] La Direttiva 95/46 prevedeva che le Autorità di controllo fossero consultate solamente in merito alle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali (art. 28 par. 2).

[70] F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, cit., p. 372. Il Garante per la protezione dei dati personali ha accolto molto favorevolmente le nuove attribuzioni relative ai poteri sulla normativa primaria. Già nel Discorso per la Relazione annuale 2018 il presidente si era espresso in questi termini: «*Il parere obbligatorio del Garante sulla normativa primaria si è dimostrato, in questo primo anno di applicazione, un passaggio essenziale per delineare il miglior equilibrio possibile tra la protezione dati e gli altri diritti e interessi di rilevanza costituzionale, nel rispetto del canone di proporzionalità, valorizzato di recente dalla stessa Consulta in relazione alla trasparenza. Il dialogo tra Garante e legislatore ha spesso consentito apprezzabili miglioramenti dei testi, come nel caso del reddito di cittadinanza. Maggiori resistenze si sono invece riscontrate, ad esempio, rispetto all'introduzione generalizzata dei controlli biometrici per i dipendenti pubblici. È auspicabile che la sottovalutazione dei principi di proporzionalità e minimizzazione dei dati, riscontrata rispetto a tali provvedimenti, lasci spazio in futuro a un supplemento di riflessione,*

Vi sono questioni di assoluta delicatezza e complessità, che difficilmente potrebbero essere affrontate a livello politico o di legislazione primaria[71]. In questo senso il ruolo che al Garante viene assegnato dal regolamento e dal Codice della *privacy* sulla elaborazione di pareri obbligatori sulla normativa primaria è decisamente strategico. La stretta collaborazione con il legislatore e con l'esecutivo appare la via più efficace per garantire che le norme prodotte rispondano ai requisiti di tutela dei dati personali, e quindi, ai principi fondamentali di cui si è detto, dal momento della progettazione.

A ben vedere dunque la collaborazione tra Garante e legislatore altro non è che la forma più alta e ben riuscita di tutela dei dati personali *by design*. Inoltre i meccanismi di raccordo del Garante con le altre autorità di controllo, oltre che con il Comitato europeo per la tutela dei dati personali[72] assicurano un costate *double-check* e una verifica dell'aderenza della legislazione italiana all'*acquis* europeo in materia di protezione dati personali, scongiurando così la possibilità che lo Stato sia destinatario di procedure d'infrazione o pronunce pregiudiziali della Corte di Giustizia dell'Unione europea.

Da ultimo, occorre fare un seppur brevissimo cenno ad una tematica che meriterebbe, per complessità ed importanza, ben altro approfondimento. Infatti, nel futuro il tema della sicurezza cibernetica è destinato ad avere una sempre maggiore rilevanza. In occasione della presentazione della Relazione 2019 sull'attività del Garante, il discorso del Presidente Soro affrontava il tema della *cybersecurity* in questi termini: *«[…] la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale con i suoi vari snodi*». In effetti la datificazione della società ha esteso

sottraendo temi così rilevanti all'enfasi della politica di parte e al conseguente rischio di norme meramente simboliche». Anche il documento di *Obiettivi programmatici e linee di priorità dell'Autorità per l'anno 2021* contiene un riferimento alla crescente attività di redazione di pareri obbligatori sulla normativa primaria, cfr. Garante per la protezione dei dati personali, *Obiettivi programmatici e Linee di priorita' dell'Autorita' per l'anno 2021*, docweb n. 9539607.

[71] Cfr. *supra*, par. 5.2.

[72] Mi riferisco ai meccanismi di coesione e coerenza di cui al Capo VII del GDPR ed in particolare alla funzione di raccordo tra le Autorità di controllo che viene attribuita al Comitato europeo per la protezione dei dati, che tra l'altro: promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le Autorità di controllo, promuove programmi comuni di formazione e scambio di personale tra le stesse, promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo (cfr. art. 70, par. 1 lett. u,v,w del GDPR.

immensamente la superficie di attacco[73], esponendo a rischi per la libertà e la sicurezza gli individui, la collettività, finanche la sovranità dello Stato. Il Presidente del Garante continua il suo intervento affermando che «*le implicazioni, in termini di sicurezza nazionale, di alcuni data breach dimostrano anche come la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" induca a ripensare il concetto di sovranità digitale. […] In un contesto in cui le tecnologie ICT sono divenute – sempre più chiaramente con la pandemia – la principale infrastruttura di ciascun Paese, assicurarne una regolazione sostenibile e adeguata, tale da garantire la sicurezza, indipendenza dai poteri privati, soggezione alla giurisdizione interna, diviene un obiettivo non più eludibile*».

L'Unione europea è ben consapevole della centralità di questi aspetti per proteggere la sovranità statale ed europea, e dunque per garantire la democrazia e i diritti, e ha adottato diversi documenti rivolti a questo obiettivo, tra cui il c.d. *Cybersecurity Act*[74], che assegna all'ENISA[75] il compito di curare, vigilare, coordinare e migliorare la sicurezza cibernetica tra gli Stati membri e introduce un quadro europeo per la certificazione della cybersicurezza[76], e la Direttiva n. 2022/2555 (c.d. NIS 2[77]), che reca misure per un livello comune elevato di cybersicurezza nell'Unione.

Nell'ordinamento interno, con il decreto-legge 21 settembre 2019, n. 105 convertito in L. 18 novembre 2019, n. 133 l'Italia ha costituito il proprio Perimetro Nazionale di sicurezza cibernetica, per «*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei*

[73] «*Data protection in general is a significant issue for smart cities, due especially to the diversity of data sources, their dispersion across large areas of cities and the relative ease of accessibility to these devices. This extends the potential attack surface and entry points for malicious attacks such as denial-ofservice, brute force attack, session hijacking etc..*», cfr. T. OSU, D. NAVARRA, *Development of a data governance framework for smart cities*, cit., p. 133.

[74] *Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)*

[75] *European Union Agency for Cybersecurity*.

[76] Cfr. M BERRUTI, F. GAGGERO*, I pilastri normativi della sicurezza cibernetica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, cit., p. 381

[77] *Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (Testo rilevante ai fini del SEE).*

servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale è istituito il perimetro di sicurezza nazionale cibernetica». Il decreto-legge n. 82 del 14 giugno 2021[78] ha poi istituito l'Agenzia per la cybersicurezza nazionale.

Sembra emergere dunque con una urgenza senza precedenti la necessità di garantire la sicurezza dei sistemi, specialmente quelli relativi alle infrastrutture critiche, in quanto un loro guasto potrebbe mettere a rischio la vita o la salute di un numero molto elevato di persone o perturbare il normale svolgimento delle attività sociali ed economiche[79]. Di conseguenza, la sicurezza cibernetica non potrà che essere garantita al pari della massima tutela dei diritti (anche digitali) dei cittadini.

Nei prossimi mesi, con l'approvazione dell'*Artificial Intelligence Act*, sarà costituito ed entrerà in funzione anche un Comitato europeo per l'Intelligenza artificiale. Abbiamo sottolineato, poc'anzi, il ruolo "costituzionale" del Garante per la protezione dei dati personali nella difesa della democrazia e dei diritti fondamentali. Le funzioni dell'Autorità garante sono destinate, nel futuro, ad incrociarsi, e forse a sovrapporsi, con quelle delle altre istituzioni appena menzionate. Sebbene le sfere di competenza del Comitato per l'Intelligenza artificiale, dell'Agenzia per la sicurezza cibernetica e del Garante *privacy* siano ben differenti, in quanto il Comitato nasce come supporto alla Commissione europea nello sviluppo dell'industria basata sull'Intelligenza artificiale[80], l'Autorità per la cybersicurezza si occupa di sicurezza nazionale[81] e il Garante per la protezione dei dati personali veglia sui diritti fondamentali, a ben vedere, l'osservazione dei nuovi equilibri che si creeranno tra questi diversi attori della società algoritmica potrebbe offrire uno scorcio sugli obiettivi strategici, sul bilanciamento dei valori in gioco, in definitiva sul futuro dell'intera *Digital society* europea.

[78] *decreto-legge 14 giugno 2021, n. 82 Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito con modificazioni dalla L. 4 agosto 2021, n. 109.

[79] Cfr. Proposta di Regolamento sull'Intelligenza artificiale, Considerando 34.

[80] Cfr. *Proposta di Regolamento sull'Intelligenza artificiale*, art. 56.

[81] Cfr. *decreto-legge 14 giugno 2021, n. 82*, art. 5.

APPENDICE

Regolamento sulla protezione dei dati personali della Città metropolitana di Firenze

PREMESSA

Art. 1 – OGGETTO

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento europeo n. 2016/679 (d'ora in avanti GDPR) e del d. lgs. n. 196/2003 (d'ora in avanti Codice della Privacy) relative al trattamento di dati personali per finalità istituzionali della Città Metropolitana di Firenze., come previsto dall'art. 2 comma 3 dello Statuto.

2. Ai fini del presente Regolamento, per finalità istituzionali si intendono quelle:

a) previste dalla legge, dallo statuto e dai regolamenti;

b) esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;

c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente;

d) in esecuzione di un contratto con i soggetti interessati.

Il presente regolamento si applica anche a tutti i trattamenti di dati personali per i quali l'interessato abbia espresso il proprio consenso.

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si rimanda a quanto previsto dalla normativa vigente in materia di protezione dei dati personali e alle disposizioni contenute nei provvedimenti della Autorità Garante per la Protezione dei dati personali e del Comitato europeo per la protezione dei dati personali.

Art. 2 – PRINCIPI

Nella applicazione del presente Regolamento e in ogni caso di trattamento di dati personali, la Città Metropolitana di Firenze garantisce che tale trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, come previsto dal GDPR.

La Città Metropolitana di Firenze tratta i dati personali applicando i principi di:

- Liceità, correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza
- Responsabilizzazione.

La Città Metropolitana di Firenze adotta le misure tecniche e organizzative adeguate per impedire il verificarsi di violazioni dei dati personali, intese quali violazioni della sicurezza che possano comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'ente.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando art. 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;

- perdita di controllo dei dati personali;

- limitazione dei diritti, discriminazione;

- furto o usurpazione d'identità;

- perdite finanziarie, danno economico o sociale;

- decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione;

- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

La Città Metropolitana di Firenze promuove, al suo interno, ogni strumento di sensibilizzazione, ivi comprese le attività di formazione ed aggiornamento del personale, che possa consolidare la conoscenza e il rispetto delle regole volte alla protezione dei dati personali e migliorare la qualità dei servizi offerti ai cittadini.

Art. 3 – TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI PER MOTIVI DI INTERESSE PUBBLICO RILEVANTE

A norma degli Artt. 9 par. 2 lett. g del GDPR e 2 sexies del Codice della Privacy, la Città metropolitana di Firenze effettua trattamenti di categorie particolari di dati personali per motivi di interesse pubblico rilevante nelle seguenti materie:

- le attività attinenti alla tenuta delle liste elettorali;
- le attività finalizzate all'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nonché dirette all'esercizio del mandato degli organi rappresentativi;
- le attività finalizzate all'applicazione della disciplina relativa alla documentazione dell'attività istituzionale;
- le attività finalizzate all'instaurazione ed alla gestione dei rapporti di lavoro sia in ordine all'espletamento degli adempimenti previsti in relazione al trattamento economico e giuridico, sia in materia sindacale, di igiene e sicurezza del lavoro;
- le attività dirette all'applicazione, anche tramite i concessionari del servizio, delle disposizioni in materia di tributi in relazione ai contribuenti, ai sostituti e ai Responsabili d'imposta, nonché in materia di deduzioni e detrazioni;

- le attività finalizzate all'applicazione della disciplina in materia di rapporti con le organizzazioni di volontariato;
- le attività svolte in conformità di leggi o di regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.

Sono considerati trattamenti effettuati per motivi di interesse pubblico rilevante tutti quelli posti in essere dalla Città metropolitana di Firenze nelle materie indicate dall'art. 2 sexies comma 2 del Codice della Privacy.

Art. 4 – DEFINIZIONI

Il presente Regolamento utilizza e fa espresso rinvio alle definizioni contenute nell'art. 4 del GDPR.

PARTE PRIMA – SOGGETTI E NOMINE

Art. 5 – TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali ai sensi della normativa in materia di protezione dei dati personali è la Città Metropolitana di Firenze, in persona del Sindaco metropolitano pro-tempore. Questi è responsabile per tutte le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati e può agire tramite un suo delegato per le competenze attribuite dal presente regolamento.

Art. 6 CONTITOLARI

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata alla Città Metropolitana di Firenze da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del GDPR.

Un accordo tra le parti definisce le responsabilità di ciascuno dei Titolari in merito all'osservanza degli obblighi per la protezione dei dati personali, con particolare riferimento all'esercizio dei diritti degli interessati e alla comunicazione agli stessi delle informazioni di cui agli articoli 13 e 14 del GDPR.

Il contenuto essenziale di tale accordo è pubblicato nel sito istituzionale della Città Metropolitana di Firenze.

Art. 7 – RESPONSABILI INTERNI DEL TRATTAMENTO

Sono Responsabili interni del trattamento dei dati personali tutti i dirigenti della Città Metropolitana di Firenze, ciascuno per le funzioni di propria competenza. I Responsabili interni sono designati dal Sindaco metropolitano con il decreto di attribuzione delle funzioni dirigenziali e sono responsabili del trattamento dei dati personali riferibili a dette funzioni.

Il Responsabile interno anche a seguito di idonea formazione, possiede adeguata conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche ed organizzative volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

I nominativi dei Responsabili interni sono pubblicati nel sito istituzionale della Città Metropolitana di Firenze nella sezione Amministrazione trasparente.

Art. 8 RESPONSABILI ESTERNI DEL TRATTAMENTO

Sono definiti Responsabili esterni i soggetti pubblici o privati non facenti parte dell'organizzazione della Città Metropolitana di Firenze che trattano i dati per conto e su istruzione documentata dell'ente. Il Titolare del trattamento stipula con tali soggetti un contratto o altro atto giuridico che definisce la materia disciplinata, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o altri strumenti giuridici consentiti dalla legge con cui è affidata a tali soggetti esterni la gestione di attività e servizi per conto della Città Metropolitana, è prevista espressamente la nomina degli stessi soggetti affidatari quali Responsabili esterni del trattamento dei dati personali connessi alle attività istituzionali affidate.

Art. 9 – INCARICATI

I dipendenti che nello svolgimento delle proprie mansioni trattano dati personali sono nominati quali incaricati al trattamento dal Responsabile interno della propria unità organizzativa. La nomina avviene in sede di predisposizione degli atti di micro-organizzazione, facendo esplicito riferimento alle corrispondenti attività di trattamento individuate nel Registro di cui al successivo art. 19.

Il Responsabile interno garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e sia impegnato alla riservatezza.

Il Responsabile dei Servizi informativi predispone una modalità operativa che assicuri l'accesso informatico dell'incaricato ai soli dati personali necessari a svolgere le mansioni riportate nell'atto di nomina. In particolare, provvede ad una mappatura di tutte le autorizzazioni all'accesso informatico ai dati dell'ente, che viene aggiornata a seguito di ogni modifica degli atti di incarico. A tal fine, i Responsabili interni competenti comunicano al Responsabile dei Sistemi informativi ogni modifica relativa alle mansioni dei dipendenti che comporti una variazione nelle attività di trattamento dei dati personali a cui gli stessi sono autorizzati.

Art. 10 – INTERESSATI

Assume la qualifica di interessato ogni persona fisica individuata o individuabile cui i dati personali trattati dalla Città Metropolitana di Firenze si riferiscono. A titolo esemplificativo e non esaustivo, ove i loro dati siano trattati dal Titolare, sono interessati i cittadini, i dipendenti dell'ente, i non residenti, i turisti, i fruitori di servizi online.

Art. 11 – RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DATA PROTECTION OFFICER, DPO)

Il Titolare del trattamento dei dati nomina con proprio decreto motivato il Responsabile della protezione dei dati (DPO). Il DPO può essere una figura dirigenziale interna all'ente oppure un soggetto esterno. Esso garantisce conoscenza e competenza sulla disciplina della protezione dei dati ed è in posizione di autonomia nei confronti del Titolare del trattamento. Il Responsabile della protezione dei dati, ove individuato internamente all'ente, può ricoprire altri ruoli purché non generino conflitti di interesse con la sua funzione.

Il DPO è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti; egli riferisce direttamente al Sindaco metropolitano e al vertice gerarchico dell'ente.

La nomina del DPO è comunicata all'Autorità Garante per la protezione dei dati personali ed a tutto il personale in modo che la sua presenza e le sue funzioni siano note a tutti i dipendenti.

Il nominativo del DPO e un recapito email della funzione sono pubblicati nel sito istituzionale della Città Metropolitana di Firenze nella sezione Amministrazione trasparente.

Art. 12 - AMMINISTRATORE DI SISTEMA

La Città Metropolitana di Firenze si avvale di un c.d. Amministratore di sistema, al fine di assicurare che il sistema informatico dell'Ente sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso il sistema medesimo. La Città Metropolitana applica quanto previsto Garante per la protezione dei dati personali con provvedimenti del 27.11.2008 e del 25.6.2009 e ss.mm.ii..

L'Amministratore di sistema viene nominato dal Dirigente responsabile dei Servizi Informativi.

L'Amministratore di sistema collabora con il DPO fornendo allo stesso supporto ed assistenza.

PARTE SECONDA – COMPITI E FUNZIONI

Art. 13 – COMPITI DEL TITOLARE DEL TRATTAMENTO

Il Titolare mette in atto adeguate misure tecniche ed organizzative al fine di garantire ed essere in grado di dimostrare che i trattamenti di dati personali effettuati dalla Città Metropolitana di Firenze sono conformi al GDPR e al Codice della Privacy.

Tali misure sono definite fin dalla fase di progettazione dei trattamenti al fine di garantire la protezione dei dati personale e di agevolare l'esercizio dei diritti dell'interessato.

Il Titolare dirama le direttive necessarie per l'applicazione delle disposizioni della normativa vigente in materia di protezione dei dati personali e del presente Regolamento, sentito il Responsabile della Protezione dei dati.

Tramite verifiche periodiche esso vigila sulla osservanza delle istruzioni scritte impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni in materia di trattamento dati.

Art. 14 – COMPITI DEL RESPONSABILE INTERNO DEL TRATTAMENTO

Il Responsabile interno del trattamento svolge, per il proprio ambito di competenza, tutte le attività previste dalla legge e i compiti specificati nel provvedimento di nomina. In particolare:

- nomina per iscritto i dipendenti appartenenti al suo ufficio quali incaricati al trattamento, autorizzando i medesimi ad accedere ai dati personali al fine di svolgerne il trattamento afferente i rispettivi compiti istituzionali;
- garantisce che gli incaricati siano impegnati alla riservatezza e che siano in possesso di idonea formazione e supervisiona il rispetto della normativa sulla protezione dei dati personali nel compimento delle attività di trattamento di loro competenza;
- predispone le informative di cui agli articoli 13 e 14 del GDPR da fornire agli interessati, redigendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti i trattamenti di competenza della propria struttura organizzativa;
- nomina i Responsabili esterni del trattamento, a norma degli articoli 8 e 15 del presente regolamento;
- stipula accordi con altri soggetti pubblici e privati per l'esercizio del diritto di accesso alle banche dati nei limiti previsti dalle disposizioni legislative e regolamentari;
- individua ed attua, insieme al Titolare del trattamento, misure adeguate per garantire la sicurezza dei trattamenti;
- collabora con il Titolare del trattamento per dare seguito alle richieste per l'esercizio dei diritti degli interessati, relative a trattamenti di dati personali posti in essere nel proprio ufficio;

- compila la sezione di competenza del proprio ufficio del Registro dei trattamenti di cui all'art. 30 del GDPR della Città metropolitana di Firenze;

- cura la pubblicazione nel sito della Città metropolitana di Firenze del contenuto essenziale degli accordi di contitolarità di propria competenza;

- riferisce al Titolare del trattamento e al DPO ogni violazione di dati personali di cui viene a conoscenza senza ritardo e li assiste nel procedimento di notifica della violazione al Garante;

- fornisce assistenza al Titolare del trattamento per le comunicazioni all'interessato di violazione dei dati personali nei casi previsti dall'art. 34 GDPR;

- nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, sentito il DPO, effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (Data Protection Impact Assesment, DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del trattamento medesimo.

Art. 15 – COMPITI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Ai Responsabili esterni si applicano le disposizioni dell'articolo 28 del GDPR.

In particolare, a maggiore specificazione di quanto indicato nell'art. 28 del GDPR, la nomina a Responsabile esterno prevede che:

- il Responsabile esterno effettui tutte le comunicazioni al Titolare utilizzando il contatto del Responsabile interno che ha provveduto alla nomina;

- eventuali violazioni di dati personali siano comunicate al Responsabile interno di cui sopra e al DPO non oltre 48 ore dal momento in cui il Responsabile esterno ne sia venuto a conoscenza;

- il Responsabile restituisca / cancelli i dati entro il termine definito nel contratto.

Per verificare il pieno rispetto delle prescrizioni di cui all'art. 28 GDPR il Titolare effettua ispezioni anche di terza parte nei confronti del Responsabile esterno, con cadenza definita nella nomina.

Art. 16 – COMPITI DELL'INCARICATO

Ogni incaricato deve attenersi alle istruzioni ricevute, che individuano con esattezza l'ambito, le modalità e i limiti al trattamento dei dati personali.

In particolare, l'incaricato:

- opera sotto la diretta autorità del Responsabile interno;
- collabora con il Responsabile interno alla compilazione del Registro dei trattamenti, nella sezione di competenza del proprio ufficio;
- collabora con il Responsabile interno per dare seguito alle richieste per l'esercizio dei diritti degli interessati, relative a trattamenti di dati personali posti in essere nel proprio ufficio;
- informa senza ritardo il Responsabile interno del suo ufficio se viene a conoscenza di una violazione dei dati personali; se la violazione riguarda un trattamento non afferente al proprio ufficio, informa senza ritardo il DPO;
- collabora con il Responsabile interno per garantire il rispetto di quanto previsto dalla normativa in materia di protezione dei dati personali.

Art. 17 – COMPITI DEL RESPONSABILE PROTEZIONE DATI (DPO)

Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare, ai Responsabili interni e agli incaricati in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;

b) sorvegliare l'osservanza della normativa in materia di protezione dei dati personali e In tal senso indicare al Titolare e ai Responsabili interni i settori o i trattamenti che comportino un rischio maggiore per i diritti e le libertà delle persone fisiche;

c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dati personali (DPIA) e sorvegliarne lo svolgimento. Collaborare con il Titolare e i Responsabili interni coinvolti, in tutte le fasi di svolgimento della DPIA e in particolare nella analisi delle conclusioni raggiunte, proponendo osservazioni, ove richiesto, in in itinere e al termine delle operazioni;

d) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per questioni connesse al trattamento dei dati personali, tra cui la consultazione preventiva nei casi previsti dalla legge in collaborazione con il responsabile interno del trattamento.

Il DPO compila e conserva digitalmente il Registro delle violazioni dei dati personali e lo mette a disposizione del Garante per la protezione dei dati personali per la verifica del rispetto della normativa in materia di protezione dei dati personali.

Art. 18 – POSIZIONE DEL DPO NELLE QUESTIONI RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI

Il Titolare e i Responsabili interni assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il DPO:

- è invitato a partecipare alle riunioni di coordinamento dei Responsabili interni che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
- deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, orale o scritta;

Il parere del DPO sulle questioni inerenti il trattamento dei dati personali non è vincolante; ciò nonostante, nel caso in cui la decisione adottata sia difforme da quella raccomandata dal DPO, tale decisione deve essere motivata.

Il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati personali.

Il Titolare del trattamento fornisce al DPO le risorse organizzative e finanziarie necessarie per assolvere i propri compiti, compresa la formazione dei dipendenti, anche considerando l'attuazione delle attività nell'ambito della programmazione operative del DUP, e del bilancio.

Il DPO opera in posizione di autonomia nello svolgimento dei propri compiti; non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

PARTE TERZA – PROCEDURE

Art. 19 – TENUTA E AGGIORNAMENTO DEL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

A norma dell'art. 30 del GDPR la Città Metropolitana di Firenze si dota di un Registro delle attività di trattamento.

Il Registro è conservato in formato digitale presso la Segreteria Generale dell'ente. Esso deve essere aggiornato con cadenza annuale e comunque ogni volta che ciascun Responsabile del trattamento lo ritenga necessario.

A tal fine ciascun Responsabile interno, per la sezione di propria competenza, trasmette alla Segreteria Generale la sezione di propria competenza in formato excel, debitamente compilata ed aggiornata.

Art. 20 – VIOLAZIONI DEI DATI PERSONALI E REGISTRO DELLE VIOLAZIONI

L'incaricato informa senza ritardo il Responsabile interno del suo ufficio se viene a conoscenza di una violazione dei dati personali; se la violazione riguarda un trattamento non afferente al proprio ufficio, informa senza ritardo il DPO.

Il Responsabile interno riferisce al Titolare e al DPO, senza ingiustificato ritardo, ogni violazione dei dati personali di cui viene a conoscenza.

Il Titolare, ove ritenga probabile che dalla violazione dei dati personali possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante per la protezione dei dati personali. La notifica dovrà avvenire senza ingiustificato ritardo e comunque entro 72 ore dalla avvenuta conoscenza della violazione.

Nei casi previsti dall'art. 34 del GDPR il Titolare comunica la violazione all'interessato senza ingiustificato ritardo, con un linguaggio semplice e chiaro.

Il Titolare documenta le violazioni di dati personali subite, anche se non comunicate alla autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

Il Registro delle violazioni è compilato e conservato digitalmente dal DPO e viene messo a disposizione del Garante per la protezione dei dati personali al fine di verificare il rispetto della normativa in materia di protezione dei dati personali.

Art. 20 – INFORMATIVE

Il Responsabile interno, per il proprio ambito di competenza, garantisce che gli interessati ricevano idonea informativa prima dell'inizio del trattamento.

L'informativa deve essere fornita per iscritto in formato cartaceo o elettronico, è redatta in modo chiaro e sintetico, in modo che sia comprensibile per l'interessato.

Essa contiene le informazioni previste dagli articoli 13 e 14 del GDPR. Il Responsabile interno redige l'informativa inserendo informazioni specifiche relative ai trattamenti effettivamente svolti nel suo ambito di competenza, assicurandone la corrispondenza con le attività di trattamento individuate nel Registro di cui all'art. 18.

Art. 21 – GESTIONE DEI DIRITTI DEGLI INTERESSATI - REGISTRO DELLE RICHIESTE DEGLI INTERESSATI

Il Dirigente responsabile dell'URP predispone e mette a disposizione degli interessati la modulistica reperibile nel sito istituzionale o in formato cartaceo presso i propri uffici per agevolare l'esercizio dei diritti relativi al trattamento dei dati personali, come elencati nel GDPR.

Le richieste di esercizio dei diritti da parte degli interessati sono annotate in un apposito registro compilato e conservato dall'Ufficio Relazioni con il Pubblico dell'ente.

Tale registro contiene l'indicazione della data di ricezione della richiesta, del contenuto della stessa, della risposta fornita e della data della risposta.

Art. 22 – SICUREZZA DEL TRATTAMENTO

Il Titolare mette in atto misure di protezione per ridurre i rischi per i diritti e le libertà delle persone fisiche legati alla sicurezza dei trattamenti.

Tali misure sono finalizzate a: assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In particolare, il Titolare assicura sistemi di back-up automatico, programmi antivirus, firewall e altri sistemi di protezione del patrimonio informativo dell'ente.

A tal fine il Titolare incarica il Dirigente responsabile dei Servizi informativi.

Il Titolare garantisce la presenza e la revisione di misure volte a garantire la sicurezza fisica dei luoghi, quali a titolo esemplificativo:

- Misure antincendio;
- Registrazione degli accessi fisici;
- Forniture e infissi ignifughi e dotati di serratura.

Ciascun Responsabile interno si accerta, relativamente al suo ufficio, che siano presenti e correttamente applicati:

- Sistemi di autenticazione per l'utilizzo dei dispositivi;
- Sistemi di autorizzazione con diversi livelli di visibilità;
- Idonei sistemi di protezione degli archivi cartacei.

I Responsabili interni impartiscono idonee istruzioni rispetto alle misure di sicurezza a tutti gli incaricati che agiscono sotto la loro autorità.

Art. 23 – CANCELLAZIONE DEI DATI

Per la conservazione e cancellazione dei dati si fa riferimento a quanto indicato nel Massimario di scarto dell'ente.

I fogli di lavoro necessari allo svolgimento delle mansioni di competenza dell'ufficio vengono distrutti a cura degli incaricati coinvolti al termine delle operazioni che ne hanno richiesto l'utilizzo.

Il Responsabile interno si assicura che tutte le procedure di conservazione e cancellazione siano rispettate.

Art. 24 - TRASPARENZA E DATI PERSONALI

La Città metropolitana di Firenze tratta i dati personali contenuti in atti e documenti amministrativi che devono essere pubblicati nel sito istituzionale dell'ente secondo quanto previsto dal Regolamento in materia di accesso documentale, civico e generalizzato e dalla normativa vigente in materia di trasparenza amministrativa.

Art. 25 – ATTIVITA' DI SENSIBILIZZAZIONE E AGGIORNAMENTO SULLA PROTEZIONE DEI DATI PERSONALI

La Città metropolitana di Firenze sostiene e promuove ogni strumento di sensibilizzazione volto al consolidamento del diritto alla protezione dei dati personali e al miglioramento della qualità dei servizi offerti ai cittadini dell'area metropolitana.

A tal fine si avvale anche della collaborazione del Dipartimento di Scienze Giuridiche dell'Università di Firenze per l'organizzazione di eventi di approfondimento e aggiornamento sulle tematiche della protezione dei dati personali.

BIBLIOGRAFIA

ACCIAI R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004.

ADAM R., *Da Colonia a Nizza: la Carta dei diritti fondamentali dell'Unione europea*, in *Il diritto dell'Unione europea*, n. 4/2000.

ADAM R., TIZZANO A., *Lineamenti di Diritto dell'Unione europea*, quarta edizione, Giappichelli, Torino, 2016.

AIELLO G.F., *La protezione dei dati personali dopo il Trattato di Lisbona*, in *Osservatorio del diritto civile e commerciale*, n. 2/2015.

AINIS M., *Il regno dell'Uroboro*, La nave di Teseo, Milano 2018.

ALDUCCI ROMANO F., *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, n. 6/2015.

ALLEGRI M.R., *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a Internet (o al ciberspazio?)*, in *Rivista AIC*, n. 1/2016.

ALLEGRI M.R., *«Ubi social, ibi ius». Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei «provider»*, Franco Angeli, Milano, 2018.

ALPA G., *La disciplina dei dati personali*, Seam, Roma, 1998.

ALPA G., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e Impresa*, 2017.

ALPA G.-BESSONE M. (a cura di), *Banche dati telematiche e diritti della persona*, CEDAM, Padova, 1984.

AL-RUITHE M., BENKHELIFA E., HAMEED K., *A systematic literature review of data governance and cloud data governance*, in *Personal and Ubiquitous Computing* (2019) 23:839–859.

AMIDEI A. *La governance dell'Intelligenza artificiale: profili e prospettive di diritto dell'Unione europea*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020.

ANGELINI R., *Intelligenza artificiale e governance. Alcune riflessioni di sistema*, IN F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

ANNECCA T., *Codici deontologici e GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

ANTONIAZZI S., *Le sanzioni amministrative*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

ARENA G., *La tutela della privacy informatica*, in *Giornale di diritto amministrativo*, 1997.

ARENA G., *Trasparenza amministrativa*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Vol. VI, Giuffrè, Milano, 2006.

ARNÒ G., LENSI ORLANDI A., *La tutela della privacy nella rete Internet*, Giappichelli, Torino, 2002.

ARPETTI J., *Economia della privacy: una rassegna della letteratura*, in *MediaLaws*, n. 2/2018.

ASSANTE E., *Cosa ci può insegnare il caso Cambridge Analytica*, in *federalismi.it*, 25 aprile 2018.

ASTONE M., *Right to be forgotten online e il discutibile ruolo dei gestori dei motori di ricerca*, in *Diritto di Internet, Digital Copyright e Data Protection*, n. 1/2020.

ATELLI M., *Voce "Riservatezza (diritto alla), Diritto costituzionale, Postilla di aggiornamento*, in *Enciclopedia giuridica*, XXVII, Treccani, Roma, 2001.

AVITABILE A., *Il responsabile della protezione dei dati*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, Zanichelli, Bologna, 2019.

AZZARITI G., *Internet e Costituzione*, in *Costituzionalismo.it*, n. 2/2011 "*Diritto e Internet*".

BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, Roma, 1974.

BALESTRIERI F., BALESTIERI L., *Guerra digitale. Il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico*, LUISS University Press, Roma, 2019.

BANKS, R. R. et al., *Discrimination and implicit bias in a racially unequal society*, in *California Law Review* 94, (2006), 4.

BARBERA A., *Costituzione della Repubblica italiana*, in Enciclopedia del diritto, Annali VIII, Giuffrè, Milano, 2015.

BARBERA A., *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di Giustizia*, in *Rivista AIC*, n. 4/2017.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, Il Mulino, Bologna, 1984.

BARILE P., *Democrazia e segreto*, in *Quaderni costituzionali*, n. 1/1987.

BARILE P.-CHELI E.-GRASSI S., *Istituzioni di diritto pubblico*, CEDAM, Padova, 2016.

BARLETTA A., *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, in *Europa e Diritto Privato*, n. 4/2017.

BARLOW J.P., *A Declaration of the Independence of Cyberspace*, in *Duke Law & Technology Review* 5-7 (2019).

BARNARD-WILLS D., PAUNER CHULVI C., DE HERT P., *Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. Elsevier B.V. Computer Law & Security Review*, 2016, Vol.32 (4).

BARTOLE S., *La cittadinanza e l'identità europea*, in *Quaderni costituzionali*, n. 1/2000.

BARTOLE S.-CONFORTI B.-RAIMONDI G., *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, Padova, 2001.

BARTOLE S.-DE SENA P.-ZAGREBELSKY V., *Commentario breve alla Convenzione europea dei diritti dell'Uomo*, CEDAM, Padova, 2012.

BASSINI M., *Le tecnologie avanzano, le norme passano ma le costituzioni rimangono*, in *Diritti comparati*, 3 novembre 2014.

BASSINI M., *Né costituzione né legge. La Dichiarazione dei diritti in Internet verso una missione culturale*, in *MediaLaws*, 28 luglio 2015.

BASSINI M., *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, n. 3/2016.

BASSOLI E., *La Ciber-Etica: luci e ombre della predittività algoritmizzata*, in *Liber Amicorum per Pasquale Costanzo*, 2020.

BASUNTI C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, n. 2/2020.

BATTELLI E., D'IPPOLITO G., *Il diritto alla portabilità dei dati personali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

BAUMAN Z., *Modernità liquida*, Laterza, Roma-Bari, 2010.

BAUMAN Z., LYON D., *Liquid Surveillance. A conversation*, Polity Press, Cambridge, 2013.

BAUMAN Z., LYON D. *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Bari-Roma, 2014.

BELLOCCI M., MAGNANESI S., PASSAGLIA P., RISPOLI E. (a cura di), *Tutela della vita privata e prospettive costituzionali, Quaderni del Servizio studi della Corte costituzionale*, 2006.

BENEDETTI D., *IA e (in)sicurezza informatica*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

BENNET C.J., *Regulating privacy. Data protection and public policy in Europe and the United States*, Cornell University Press, Ithaca, 1992.

BERRUTI M., GAGGERO F*., I pilastri normativi della sicurezza cibernetica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

BERTI G., *Manuale di interpretazione costituzionale*, CEDAM, Padova, 2001.

BERTI SUMAN A., *Il diritto alla cancellazione*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

BERTOLISSI M. (a cura di), *L'ordinamento degli enti locali. Commento al Testo Unico sull'ordinamento delle autonomie locali del 2000 alla luce delle riforme costituzionali del 2001*, Il Mulino, Bologna, 2002.

BESSONE M, *Politica dell'informazione e strategie di ''Datenschutz''*, in G. ALPA, M. BESSONE, *Banche dati telematica e diritti della persona*, Padova, 1984.

BETZU M., *Regolare internet. Le libertà di informazione e di comunicazione nell'era digitale*, Giappichelli, Torino, 2012.

BETZU M., *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista AIC*, n. 4/2012.

BETZU M., *Poteri pubblici e poteri privati nel mondo digitale*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

BEVERE A.-CERRI A., *Il diritto di informazione e i diritti della persona: il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale*, Giuffrè, Milano, 2006.

BIANCA C.M.-BUSNELLI F.D. (a cura di), *La protezione dei dati personali*, CEDAM, Padova, 2007.

BIANCHI L., *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

BIANCHI L., D'ACQUISTO G., *Il trattamento dei dati personali effettuato dai motori di ricerca, le esternalità prodotte sugli interessati e il diritto di rettifica. Quali prospettive e limiti dopo la sentenza della Corte di Giustizia*, in F. PIZZETTI (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

BIFULCO R., *La sentenza Schrems e la costruzione del diritto europeo alla privacy*, in *Giurisprudenza Costituzionale*, 2016.

BIFULCO R., CARTABIA M., CELOTTO A. (a cura di) *L'Europa dei diritti: commento alla Carta dei diritti fondamentali dell'Unione Europea*, Il Mulino, Bologna, 2001.

BILOTTA F., *La responsabilità civile nel trattamento dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

BIN R.-PITRUZZELLA G., *Diritto costituzionale*, Giappichelli, Torino, 2016.

BINNS R., *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law* 7/2017.

BOBBIO N., *L'età dei diritti*, Einaudi, Torino, 1997.

BODEN M.A., *L'intelligenza artificiale*, Il Mulino, Bologna, 2019.

BOLOGNINI L., PELINO E., BISTOLFI C., (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Francis Lefebvre, Milano, 2016.

BOLOGNINI L., BISTOLFI C., *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation* Elsevier Ltd The computer law and security report, 2017-04, Vol.33 (2).

BOLOGNINI L., PELINO E., (a cura di), Codice della disciplina privacy, Giuffrè Francis Lefebvre, Milano, 2019.

BOLOGNINI L. (a cura di), *Privacy e libero mercato digitale*, Giuffrè, Milano, 2021.

BONFANTI A., *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, n. 3/2018.

BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti ''violabili'' in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, *Rivista AIC*, n. 3/2016.

BONZAGNI G., *Le comunicazioni elettroniche*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

BORGIA F., *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

BAROCAS S., SELBST A.D., *Big data's disparate impact*, in *California Law Review* 104 (2016), 3.

BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, New York – Oxford, 2020.

BRANCASI A., CARETTI P., *Il sistema dell'autonomia locale tra esigenze di riforma e spinte conservatrici: il caso della Città metropolitana*, in *Le Regioni*, Fascicolo 4/2010, luglio-agosto.

BRAVO F., *Le condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

BRESSAN-ISEPPI, *Le applicazioni mobili per la sicurezza urbana. Sicurezza dei cittadini, protezione della privacy e dei dati personali nella smart city*, in *eCrime Working papers*, n. 4/2015;

BRIGHI R., *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità ed esigenze di trasparenza*, Aracne, Roma, 2016.

BRUGIOTTI E., *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali, fino alla tutela del corpo elettronico*, in *dirittifondamentali,it* 2/2013.

BRUTTI N., *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

BULTRINI A., *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, Edizioni scientifiche italiane, Napoli, 2009.

BUQUICCHIO G., *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati*, Il Mulino, Bologna, 1981.

BURLA P., FRACCASTORO G., *Il diritto di accesso ai documenti della Pubblica amministrazione*, Laurus Robuffo, Roma, 2006.

BURREL J., How the machine 'thinks': Understanding opacity in machine learning algorithms, in *Big Data & Society* 3 (2016), 1.

BÜSCHEL I., MEHDI R., CAMMILLERI A., MARZOUKI, Y., ELGER B., SPIER R., MORDINI E., *Protecting Human Health and Security in Digital Europe: How to Deal with the "Privacy Paradox"?* Dordrecht: Springer Netherlands Science and engineering ethics, 2014-09, Vol.20 (3).

BUSIA G., *Riservatezza (diritto alla),* in Digesto delle discipline pubblicistiche, agg. I, Utet giuridica, Torino, 2000.

BUSIA G., *Le frontiere della privacy in Internet: La nuova corsa all'oro per i dati personali*, in O. POLLICINO, E. BERTOLINI, V. LUBELLO (a cura di), *Internet: Regole e tutela dei diritti fondamentali*, Aracne, Roma, 2013.

BUSIA G., FEROLA L., *Il Garante per la protezione dei dati personali*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016.

BUSIA G., LIGUORI L., POLLICINO O. (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Aracne, Roma, 2016.

BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria e internazionale*, Giuffrè, Milano, 1997.

BUTTARELLI G., *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law*, vol. 6, n. 2/2016.

BUTTARELLI G., *The geostrategic importace of data protection: an abstract of the EDPS 2018 Annual report*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

BUZZACCHI C., *Le smart cities tra sicurezza delle tecnologie e incertezza della dimensione democratica*, in C. BUZZACCHI, P. COSTA, F. PIZZOLATO (a cura di), *Technopolis. La città tra mediazione giuridica e profezia tecnologica*, Giuffrè Francis Lefebvre, Milano, 2019.

BUZZACCHI C., COSTA P., PIZZOLATO F. (a cura di), *Technopolis. La città tra mediazione giuridica e profezia tecnologica*, Giuffrè Francis Lefebvre, Milano, 2019.

CAGGIANO G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, n. 2/2018.

CALIFANO L., *Privacy e sicurezza*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, Santarcangelo di Romagna, 2013.

CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016.

CALIFANO L., *Trasparenza e privacy nell'evoluzione dell'ordinamento costituzionale*, in *Giornale di Storia costituzionale*, 31/2016.

CALIFANO L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

CALIFANO L., *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in *federalismi.it*, 3 maggio 2017.

CALIFANO L., *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in *MediaLaws*, 1/2018.

CALIFANO L., *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *federalismi.it*, 7 agosto 2019.

CALIFANO L., COLAPIETRO C. (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014.

CALIFANO L., FIORILLO V., Voce *Videosorveglianza*, in Digesto delle discipline pubblicistiche, Agg., Utet, Torino, 2015.

CALIFANO L., COLAPIETRO C., *Innovazione tecnologica e valore della persona - Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

CALO R., *Artificial Intelligence Policy: A Primer and Roadmap (August 8, 2017)*.

CALZA BINI P. (a cura di), *Nuove tecnologie e informatizzazione nei processi d'ufficio: studi di casi nella pubblica amministrazione*, Marsilio, Venezia, 1985.

CALZOLAIO S., *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, 31/2016.

CALZOLAIO S. Voce *Protezione dei dati personali*, in Digesto delle discipline pubblicistiche, Agg. Utet, Torino, 2107.

CALZOLAIO- S., PAGNANELLI V., *From data protection to privacy by research. Food for thoughts in the light of the new General data Protection Regulation*, in *Law and Administration XXI Century*, n. 4(41)/2016.

CAMARDI C. (a cura di), *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche - Ca' Foscari Venezia, 25-26 novembre 2021*, Wolters Kluwer, CEDAM, Milano, 2022.

CANDINI A., *Tutela amministrativa e giurisdizionale*, G. FINOCCHIARO (a cura di), in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

CANNADA-BARTOLI L., *Considerazioni su alcune norme in materia di giurisdizione contenute nel regolamento generale sulla protezione dati n. 2016/679*, in *Europa e Diritto Privato*, fascicolo n. 3/2018.

CANZIO G., *L'applicazione della Carta dei diritti fondamentali e il dialogo tra le Corti*, in V. PICCONE, O. POLLICINO (a cura di), *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività*, Editoriale scientifica, Napoli, 2018.

CAPILLI G., *La tutela dei dati personali dei minori*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Milano, 2019.

CARAVITA B., *La Costituzione dopo la Riforma del titolo V. Stato, Regioni e autonomie fra Repubblica e Unione europea*, Giappichelli, Torino, 2002.

CARAVITA B., *Social network, formazione del consenso, istituzioni politiche: quale regolamentazione possibile?*, in *federalismi.it*, 23 gennaio 2019.

CARAVITA B., *Principi costituzionali e intelligenza artificiale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefevbre, Milano, 2020.

CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004.

CARETTI P. (a cura di), *I poteri normativi delle autorità indipendenti*, in *Osservatorio sulle fonti 2003-2004*, Giappichelli, Torino, 2005.

CARETTI P., CARDONE A., *Diritto dell'informazione e della comunicazione nell'era della convergenza*, Il Mulino, Bologna, 2019.

CARETTI P., DE SIERVO U. (a cura di), *Diritto costituzionale e pubblico*, Giappichelli, Torino, 2020.

CARIDI V., *La tutela dei dati personali in internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2001.

CARNELUTTI F., *Diritto alla vita privata*, in *Rivista trimestrale di diritto pubblico*, 1955.

CARROZZA M.C., ODDO C., ORVIETO S., DI MININ A., MONTEMAGNI G., *AI: profili tecnologici. Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza artificiale*, in *BioLaw Journal-Rivista di BioDiritto 3/2019*.

CARTABIA M., *Cittadinanza europea*, in Enciclopedia giuridica, VII, Treccani, Roma, 1995.

CARTABIA M., *Principi inviolabili e integrazione europea*, Giuffrè, Milano, 1995.

CARTABIA M.-WEILER J.H.H., *L'Italia in Europa. Profili istituzionali e costituzionali*, Il Mulino, Bologna, 2000.

CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in M.G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001.

CARTABIA M., *I diritti fondamentali e la cittadinanza dell'Unione*, in F. BASSANINI, G. TIBERI (a cura di), *La Costituzione europea. Un primo commento*, Il Mulino, Bologna, 2004.

CARTABIA M., *L'ora dei diritti fondamentali nell'Unione Europea*, in M. CARTABIA (a cura di), *I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Il Mulino, Bologna, 2007.

CARULLO G., *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e mercato*, 23/2016.

CARULLO G., *Dati, banche dati, Blockchain e interoperabilità dei sistemi informatici nel settore pubblico*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020.

CARUSO C., *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in *forumcostituzionale.it*, ottobre 2013.

CASAROSA F., *La tutela aggregata dei dati personali nel regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

CASEY B., FARHANGI A., VOGL R., *Rethinking Explainable Machines: the "Right to Explanation" debate and the rise of algorithmic audits in enterprise*, in *Berkeley Technology Law Review 34 (2019), 1*.

CASINI L., *Lo Stato nell'era di Google*, in *Rivista trimestrale di diritto pubblico*, IV, dicembre 2019.

CASONATO C., *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, Fascicolo speciale, maggio 2019.

CASONATO C., *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal - Rivista di BioDiritto* n. 1/2019.

CASONATO C., MARCHETTI B., *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di Intelligenza artificiale*, in *Biolaw Journal - Rivista di BioDiritto* n. 3/2021.

CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P. (a cura di), *Il processo di adeguamento al GDPR aggiornato al d. lgs. 10 agosto 2018 n. 101*, Giuffrè Francis Lefebvre, Milano, 2018.

CASSESE S., *Tutela della privacy e banche dei dati della Pubblica Amministrazione*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati*, Il Mulino, Bologna, 1981.

CASSESE A., *I diritti umani nel mondo contemporaneo*, Laterza, Roma-Bari, 1998.

CASTELVECCHI D., *Can we open the black box of AI*, in *Nature 538 (2016) 7623*.

CATALETA A., *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

CATAUDELLA A., *La tutela civile della vita privata*, Giuffrè, Milano, 1972.

CAUSARANO M.C., *GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta*, in A. MANTELERO, D. POLETTI, (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

CAVALLARO M. C., SMORTO G., *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in federalismi.it n. 16/2019.

CAVALLO PERIN R., *Commentario breve al Testo Unico sulle autonomie locali*, CEDAM, Padova, 2006.

CAVALLO PERIN R., GALETTA D.U. (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020.

CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles, Information & Privacy Commissioner of Ontario, Canada*, 2011.

CERRI A., Voce *Riservatezza*, II, Diritto comparato e straniero, in Enciclopedia giuridica, v. XXVII, Treccani, Roma, 1991.

CERRI A., Voce *Riservatezza*, III, Diritto costituzionale, in Enciclopedia giuridica, XXVII, Treccani, Roma, 1991.

CERRINA FERONI G., FONTANA C., RAFFIOTTA E.C. (a cura di), *AI Anthology. Profili giuridi, economici e sociali dell'intelligenza artificiale,* Il Mulino, Bologna, 2022.

CHELI E., *Libertà di associazione e poteri di polizia: profili storici*, in P. BARILE (a cura di), *La pubblica sicurezza. Atti del congresso celebrativo del centenario delle leggi amministrative di unificazione*, Neri Pozza, Vicenza, 1967.

CHIARIELLO C*., Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale*, in *Giurcost.org*, fascicolo n. 2/2018, 7 marzo 2018.

CHIEFFI L., *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

CHIOLA C., Voce *Manifestazione del pensiero (libertà di)*, in Enciclopedia giuridica, XIX, Treccani, Roma, 1990.

CIANCIO A., *A margine dell'evoluzione della tutela dei diritti fondamentali in ambito europeo, tra luci ed ombre*, in *federalismi.it*, n. 21/2012.

CIFARELLI R., *La trasparenza amministrativa dalla legge n. 241/1990 all'accesso civico: spunti di riflessione*, in *AstridRassegna* n. 16/2014.

CLARICH M., *Manuale di diritto amministrativo*, Il Mulino, Bologna, 2017.

CLEMENTE A. (a cura di), *Privacy*, CEDAM, Padova, 1999.

COCUCCIO M.F., *Il diritto all'identità personale e l'identità "digitale"*, in *Diritto di Famiglia e delle Persone*, fascicolo n. 3/2016.

COHEN J.E., *What privacy is for*, in *Harvard Law Review*, 2013, 1924.

COLAPIETRO C., *Trasparenza e democrazia: conoscenza e/è potere*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014.

COLAPIETRO C., *La "terza generazione" della trasparenza amministrativa. Dall'accesso documentale, all'accesso generalizzato, passando per l'accesso civico*, Editoriale scientifica, Napoli, 2016.

COLAPIETRO C., *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Editoriale scientifica, Napoli, 2018.

COLAPIETRO C., *Il nuovo quadro giuridico europeo sulla protezione dei dati personali e l'adeguamento della normativa nazionale*, in *Studi parlamentari e di politica costituzionale*, 2018.

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 22, 2018.

COLAPIETRO C., IANNUZZI A., *Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014.

COLAPIETRO C., IANNUZZI A., *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

COLAPIETRO C., MORETTI A., *L'Intelligenza artificiale nel dettato costituzionale: opportunità, incertezze e tute-la dei dati personali*, in *BioLaw Journal - Rivista di BioDiritto*, n. 3/2020.

COLAPRISCO F., *Data Governance Act. Condivisione e "altruismo" dei dati*, in *I post di AISDUE, Focus "Servizi e piattaforme digitali*", n. 3, 5 maggio 2021

COMANDÈ G., MALGIERI G., *Manuale per il trattamento dei dati personali*, Il Sole 24 Ore, Milano, 2018.

CONTALDO A., PELUSO F., *Cybersecurity. La nuova disciplina italiana ed europea alla luce della Direttiva NIS*, Pacini, Pisa, 2018.

CONTI G.L., *La governance dell'internet: dalla costituzione della rete alla costituzione nella rete*, in M. NISTICÒ, P. PASSAGLIA (a cura di), *Internet e costituzione*, Giappichelli, Torino, 2014.

CORASANITI G., *Diritto e tecnologie dell'informazione. Linee introduttive*, Giuffrè, Milano, 1990.

CORASANITI G., *Il diritto nella società digitale*, Franco Angeli, Milano, 2018.

CORRALES M., FENWICK M., FORGÓ N. Eds, *New Technology, Big Data and the Law. Perspectives in Law*, in *Business and Innovation*, Springer, Singapore, 2017.

CORTESE B., *La protezione dei dati di carattere personale nell'Unione europea dopo il Trattato di Lisbona*, in *Il diritto dell'Unione europea*, n. 2/2013.

COSTANTINO F., *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Diritto pubblico*, Fascicolo 1, gennaio-aprile 2019.

COSTANTINO G., *La tutela giurisdizionale dei diritti al trattamento dei dati personali (Note a prima lettura dell'art. 152 d.lgs. 30 giugno 2003, n. 196)*, in *Studi di diritto processuale civile in onore di Giuseppe Tarzia*, tomo 3, Milano, 2005.

COSTANZO P., Voce *Internet* (diritto pubblico), in Digesto delle discipline pubblicistiche, agg. I, Utet, Torino, 2000.

COSTANZO P., DE MINICO G., ZACCARIA R. (a cura di), *I "tre codici" della società dell'informazione. Amministrazione digitale, comunicazioni elettroniche, contenuti audiovisivi*, Giappichelli, Torino, 2006.

COSTANZO P., *La dimensione costituzionale della privacy*, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, EGEA, Milano, 2008.

COSTANZO P., *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in *Associazione Italiana dei Costituzionalisti, Annuario 2012, Costituzionalismo e globalizzazione, Atti del XXVII Convegno Annuale, Salerno, 22-24 novembre 2012*, Jovene, Napoli, 2014.

COSTANZO P., *Il riconoscimento e la tutela dei diritti fondamentali*, in P. COSTANZO, L. MEZZETTI, A. RUGGERI (a cura di), *Lineamenti di Diritto costituzionale dell'Unione europea*, quinta edizione, Giappichelli, Torino, 2019.

COSTANZO P., MAGARO' P., TRUCCO L. (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

COSTANZO P., *Lo "Stato digitale"*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

CRADOCK E., STALLA-BOURDILLON S., MILLARD D., Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform, Computer law & security review, n. 33/2017.

CREA G., *Profili antitrust del consenso non libero al trattamento dei dati personali*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Giuffrè, Milano, 2021.

CREMONA E., *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Edizioni Scientifiche Italiane, Napoli 2023.

CREMONA E., LAVIOLA F., PAGNANELLI V. (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.

CRESPI S., *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comparato*, 2015.

CRESPI S., *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 2016.

CRISTOFARI G., *Il diritto alla limitazione del trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

CUDD A., NAVIN M., *Core Concepts and Contemporary Issues in Privacy*. Cham: Springer International Publishing AG; 2018.

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007.

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

CUKIER K., MAYER-SCHOENBERGER V., *The Rise of Big Data: How It's Changing the Way We Think About the World*, in *Foreign Aff.*, 2013, 28.

CUNIBERTI M., *Nuove tecnologie e libertà della comunicazione: profili costituzionali e pubblicistici*, Giuffrè, Milano, 2008.

CUPELLI C., FICO F., *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice privacy dal d.lgs. n. 101/2018*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

D'ACQUISTO G., *Il diritto alla memoria: prospettive tecnologiche*, in F. PIZZETTI (a cura di), *Internet e tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

D'ACQUISTO G., *Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

D'ACQUISTO G., *Nuovi tipi di profilazione, ecco i rischi privacy: servono tutele più ampie*, in *AgendaDigitale*, 19 aprile 2019.

D'ACQUISTO G., *Intelligenza artificiale. Elementi*, Giappichelli, Torino, 2021.

D'ACQUISTO G., NALDI M., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, Giappichelli, Torino, 2017.

D'AGATA C., *Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

D'AGOSTINO L., *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto Penale Contemporaneo* 2/2019.

D'ALOIA A., *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019.

D'AVACK L., *La rivoluzione tecnologica e la nuova era digitale: problemi etici*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020.

D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO, (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016.

D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G. (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

D'OTTAVIO A., *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

DE BERNART M., *La videosorveglianza e il controllo del lavoratore*, in R. PANETTA (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Giuffrè Francis Lefebvre, Milano, 2019.

DE COLLIBUS F. M., *L'era delle macchine che apprendono*, in *Limes, Rivista italiana di geopolitica*, 12/2022.

DE CUPIS A., *Il diritto alla riservatezza esiste* in *Il Foro Italiano*, Vol. LXXVII, n.4, 1954 (JSTOR) 159.

DE FRANCESCHI A., *Il «pagamento» mediante dati personali*, in *I dati personali nel diritto europeo*, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Giappichelli, Torino, 2019.

DE GIACOMO C., *Diritto, libertà e privacy nel mondo della comunicazione globale: il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Giuffrè, Milano, 1999.

DE GRAZIA D., *Il governo di Internet*, Franco Angeli, Milano, 2010.

DE GRAZIA D., *Informatizzazione e semplificazione dell'attività amministrativa nel "nuovo" codice dell'amministrazione digitale*, in *Diritto pubblico*, Fascicolo 2, maggio-agosto 2011.

DE GREGORIO G., TORINO R., *Privacy, protezione dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

G. DE GREGORIO., P. DUNN, *Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA*, in

https://assets.ctfassets.net/iapmw8ie3ije/5EuxLPaUIsgGt7R6PgeuFK/c9269e55e10bb2a7a0b392624c08f4d0/De_Gregorio_Dunn_My_Data_is_Mine__1_.pdf

DE HERT P., PAPAKONSTANTINOU V., *The new General Data Protection Regulation: Still a sound system for the protection of individuals?* Elsevier Ltd *The computer law and security report*, 2016-04, Vol.32 (2).

DE MEO R., *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2013.

DE MINICO G., *Diritti Regole Internet*, in *Costituzionalismo.it*, fasc. n. 2/2011 "*Diritto e Internet*".

DE MINICO G., *Gli open data: una politica costituzionalmente necessaria?*, in *Forumcostituzionale.it*, 2014.

DE MINICO G., *Big data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, I, gennaio-aprile 2019.

DE SALVIA M., *La Convenzione europea dei diritti dell'uomo: procedure e contenuti*, Editoriale scientifica, Napoli, 1999.

DE SALVIA M., *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida*, in M. FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, Editoriale scientifica, Napoli, 2015.

DE SIERVO U., *Dignità delle persone e diritto di informazione nel codice previsto dall'art. 25 della legge 675 del 1996*, in *Studi in onore di Leopoldo Elia*, Giuffrè, Milano, 1999.

DE SIERVO U., *Diritto all'informazione e tutela dei dati personali*, in Foro italiano, 1999.

DE SIERVO U., *Tutela dei dati personali e riservatezza*, in *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, CEDAM, Padova, 2003.

DE SIERVO U., *La privacy*, in S. PANUNZIO (a cura di), *I diritti fondamentali e le Corti in Europa*, Jovene, Napoli, 2005.

DE TULLIO M.F., *La privacy e i Big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 2016.

DI COSIMO G., *Sul ricorso alle linee guida da parte del Garante per la privacy*, in *Giornale di Storia costituzionale*, 31/2016.

DI GIACOMO RUSSO B., *Il principio di sussidiarietà orizzontale nell'ordinamento italiano. Analisi e prospettive*, Youcanprint, Lecce, 2022.

DI MARIA R., NAPOLI C., PERTICI A., *Diritto delle autonomie locali*, Giappichelli, Torino, 2022.

DI MARTINO A., *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, in S. PANUNZIO (a cura di), *I diritti fondamentali e le corti in Europa*, Jovene, Napoli, 2005.

DI MARTINO A., *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017.

DI PORTO F. (a cura di), *Big data e concorrenza*, *Concorrenza e mercato*, numero speciale, 23/2016.

DEL FEDERICO C., *Il trattamento dei dati nell'ambito dei rapporti di lavoro*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

DEL FEDERICO C., POPOLI A.R., *Le definizioni*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

DANIELIS R. (a cura di), *La città metropolitana: sfide, rischi e opportunità*, EUT, Trieste, 2016.

DELMATRO M., NICITA A., *Big data. Come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019.

DEMURO G., *Costituzionalismo europeo e tutela multilivello dei diritti. Lezioni*, Giappichelli, Torino, 2009.

DEMURO G., *La Carta dei diritti*, in A. LUCARELLI, A. PATRONI GRIFFI (a cura di), *Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea*, Edizioni Scientifiche italiane, Napoli, 2009.

DEMURO G., *La Carta dei diritti*, in A. LUCARELLI, A. PATRONI GRIFFI (a cura di*), Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea*, Napoli, Edizioni Scientifiche italiane, 2009.

DENNINGER E., *Tutela ed attuazione del diritto nell'età tecnologica*, in F. RICCOBONO (a cura di), *Nuovi diritti dell'età tecnologica*, Giuffrè, Milano, 1991.

DINELIN T., TREPTE S., *Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors*. Wiley Subscription Services, Inc European journal of social psychology, 2015-04, Vol.45 (3).

DOGLIANI M.-MASSA PINTO I., *Elementi di diritto costituzionale*, Giappichelli, Torino, 2014.

DONATI F., *art. 8, Protezione dei dati di carattere personale*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Il Mulino, Bologna, 2001.

DONATI F., *Article 8–Protection of Personal Data*, in W.B.T. Mock, G. Demuro (eds), *Human Rights in Europe. Commentary on the Charter of Fundamental Rights of the European Union*, Durham, North Carolina, 2010.

DONATI F., Voce *Internet* (diritto costituzionale), in Enciclopedia del diritto, Annali VII, Giuffrè, Milano, 2014.

DONATI D., *Il principio di trasparenza in Costituzione*, in F. MERLONI (a cura di), *La trasparenza amministrativa*, Giuffrè, Milano, 2008.

DONINI A., *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, in *Labour & Law issues*, vol. 3, no. 1, 2017.

DORIGO S., LOMBARDI E., LONGO E., PIETROPAOLI S., *The Phenomenon of the Algorithm and its Impact on the EU Legal Systerm: an Attempt at a Multidisciplinary Approach, Legal Issues in the Digital Age*, 2020 (3).

DROZDOWSKI P., RATHGEB C., DANTCHEVA A., DAMER N., BUSCH C., *Demographic Bias in Biometrics: A Survey on an Emerging Challenge in IEEE Transactions on Technology and Society*, 1 (2020) 2.

DURST L., *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

DURST L., *Il trattamento di categorie particolari di dati in ambito sanitario*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

EDWARDS L., VEALE M., *Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for*, in *Duke Law and Technology Review* 16 (2017) 1.

ERDOS D., *European Data Protection Regulation and the new media Internet: Mind the implementation gaps*, in *Journal of law and society,* 12/2016.

ESPOSITO M.S., *L'impatto del trattamento sui diritti e le libertà delle persone fisiche: una valutazione alla luce della giurisprudenza delle autorità garanti italiana e spagnola*, in A.

MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

ESPOSITO M.S., *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

ESPOSITO M.S., *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

ESPOSITO M.S., Il trattamento transfrontaliero e la cooperazione tra Autorità garanti. Il meccanismo di coerenza, in G. Finocchiaro (a cura di), La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, Torino, 2019.

ESPOSITO M.S., *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Diritto dell'Informazione e dell'Informatica*, fascicolo n. 4- 5/2019.

ETZIONI A., *The Limits of Privacy*, Basic Books, New York 1999.

FABBRIZZI F., SALERNO G.M. (a cura di), *La riforma delle autonomie territoriali nella legge Delrio*, Jovene, Napoli, 2014.

FAINI F., *Dati, algoritmi e regolamento europeo 2016/679, in A. Mantelero, D. Poletti, (a cura di), Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

FAINI F., *Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019.

FAINI F., *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefevbre, Milano, 2019.

FALCE V., GHIDINI G., OLIVIERI G. (a cura di), *Informazione e big data tra innovazione e concorrenza*, Giuffrè, Milano, 2017.

FALCON G., *Funzioni amministrative ed enti locali nei nuovi artt. 118 e 117 della Costituzione*, in *Le Regioni*, Fascicolo 2-3/2002, marzo-giugno.

FALLETTI E., *L'evoluzione del concetto di privacy e della sua tutela giuridica*, in G. CASSANO, G. SCORZA E G. VACIAGO (a cura di), *Diritto dell'Internet*, CEDAM, Padova, 2013.

FARACE D., *Privacy by design e privacy by default*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

FARES G., *I dati relativi alla salute e i trattamenti in ambito sanitario*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

FARO S., LETTIERI N., *Big Data: una lettura informatico-giuridica*, in *Scritti per Luigi Lombardi Vallauri*, vol. 1, CEDAM, Padova, 2016.

FASAN M., *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019.

FEROLA L., *Dal diritto all'oblio alla memoria sul "web". L'esperienza applicativa italiana*, in *Diritto dell'informazione e dell'informatica*, 2012.

FEROLA L., *La "nuova" figura del Responsabile della protezione dei dati personali e le sue caratteristiche*, in R. PANETTA (a cura di*), Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

FERRARI G.F. (a cura di), *I diritti fondamentali dopo la Carta di Nizza. Il Costituzionalismo dei diritti*, Giuffrè, Milano, 2001.

FERRARI G.F. (a cura di), *Nuove province e Città metropolitane*, Giappichelli, Torino, 2016.

FERRERO E., *Le smart city nell'ordinamento giuridico*, in *Il foro amministrativo*, 4/2015.

FILIPPETTA G., *La libertà personale e le libertà di domicilio, di circolazione e individuale*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, vol. 2, Giappichelli, Torino, 2006.

FINOCCHIARO G., *Il diritto all'anonimato*, CEDAM, Padova, 2008.

FINOCCHIARO G., Voce *Identità personale (diritto alla)*, in Digesto/civ., Agg., Utet, Torino, 2010.

FINOCCHIARO G., *Diritto e tecnica*, in *Il diritto dell'informazione e della tecnica*, n. 4-5/2012.

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012.

FINOCCHIARO G., *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Il Diritto dell'Informazione e dell'Informatica*, 4-5/2015.

FINOCCHIARO G. (a cura di), *Il nuovo Regolamento europeo sulla Privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, 1/2017.

FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

FINOCCHIARO G., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

FINOCCHIARO G., *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefevbre, Milano, 2020.

FINOCCHIARO G., *La proposta di Regolamento sull'Intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

FIORIGLIO G., *Il diritto alla privacy: nuove frontiere nell'era di internet*, Bononia University Press, Bologna, 2008.

FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *federalismi.it*, 15/2017.

FLICK C., *Il diritto all'oblio nella sentenza «Google Spain» e la sua applicazione pratica*, in F. PIZZETTI (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

FLORIDI L., *Philosophy and Computing: an introduction*, Routeledge, London, 1999.

FLORIDI L., *Infosfera. Etica e filosofia nell'età dell'informazione*, Giappichelli, Torino, 2009.

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017.

FLORIDI L., MITTELSTADT B., WACHTER S., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation in International Data Privacy Law* 7, (2017), 2.

FLORIDI L., *What the near future of artificial intelligence could be*, in *Philosophy & Technology* 32 (2019), 1.

FLORIDI L., *Pensare l'infosfera. La filosofia come design concettuale*. Raffaello Cortina Editore, Milano, 2020.

FOCARELLI C., *Privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna 2015.

FOGLIA C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione del GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

FOIS S., *Principi costituzionali e libertà di manifestazione del pensiero*, Giuffrè, Milano, 1957.

FONZI A., *Il principio di autodeterminazione dell'utente al cospetto delle nuove tecnologie*, in *dirittifondamentali.it*, 3/2021, 20 dicembre 2021.

FRAIOLI M., *Il diritto di opposizione e la revoca del consenso*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

FRANCA S., *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, in *Diritto pubblico*, Fascicolo 2, maggio-agosto 2021.

FRANCESCHELLI B., *Il diritto alla riservatezza*, Jovene, Napoli, 1960.

FRIED C., *Privacy*, in *Yale Law Review*, 1968.

FRIGERIO F., *La Corte di Giustizia, 5 anni dopo Google Spain, limita l'estensione del diritto all'oblio all'Unione europea*, in *Media Laws*, 4 ottobre 2019.

FRONTONI E., *La giurisprudenza costituzionale*, in A. CLEMENTE (a cura di), *Privacy*, CEDAM, Padova, 1999.

FROSINI T.E., *Google e il diritto all'oblio preso sul serio*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Romatre Press, Roma, 2015.

FROSINI A., *Gli atti normativi del Garante per la protezione dei dati personali*, in *Giurisprudenza Costituzionale*, 2014.

FROSINI T.E., Liberté, egalité, Internet, Editoriale scientifica, Napoli, 2015.

FROSINI T.E., POLLICINO O., APA E., BASSINI M. (a cura di), *Diritti e libertà in internet*, Mondadori, Milano, 2017.

FROSINI T.E., *Declinazioni del governare*, Giappichelli, Torino, 2018.

FROSINI T.E., *Il Costituzionalismo nella Società tecnologica*, in *Giurcost.org, Liber Amicorum per Pasquale Costanzo*, 25 maggio 2020.

FROSINI T.E., *L'orizzonte giuridico dell'Intelligenza artificiale*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

FROSINI V., *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI (a cura di), *Privacy e banche dati*, Il Mulino, Bologna, 1981.

FROSINI V., *Informatica diritto e società*, Giuffrè, Milano, 1992.

FROSINI V., *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA-M. BESSONE (a cura di), *Banche dati telematica e diritti della persona*, CEDAM, Padova, 1984.

FROSINI V., *Contributi ad un diritto dell'informazione*, Liguori, Napoli, 1991.

FULCO D., *Gli impatti della normativa in materia di protezione dei dati personali sulla libera iniziativa economica e sulle libertà di scelta individuali*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Giuffrè, Milano, 2021.

FUMAGALLI MERAVIGLIA M. (a cura di), *Diritto alla riservatezza e progresso tecnologico*, Editoriale scientifica, Napoli, 2015.

GAJA G., ADINOLFI A., *Introduzione al diritto dell'Unione europea*, Laterza, Roma-Bari, 2014.

GALETTA D.U., *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *federalismi.it*, marzo 2016.

GALETTA D.U., *La trasparenza, per un nuovo rapporto tra cittadino e Pubblica Amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2016.

GALETTA A., DE HERT P., *The proceduralisation of data protection remedies under EU data protection law: towards a more effective data subject-oriented remedial system?*, in Review of Administrative Law, vol. 8 n. 1/2015.

GALETTA D.U., CORVALAN J.G., *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, n. 3/2019, 6 febbraio 2019.

GALLINO L., *Mente comportamento e intelligenza artificiale*, Edizioni di Comunità, Torino, 1984.

GAMBETTA D. (a cura di), *Datacrazia. Politica, cultura algoritmica e conflitti ai tempi dei Big Data*, D editore, Roma, 2018.

GAMBINI M., *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *Costituzionalismo.it*, fascicolo n. 2/2011 "*Diritto e Internet*".

GAMBINI M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

GAMBINO S., *Diritti fondamentali e Unione europea*, Giuffrè, Milano, 2009.

GAMBINO S., *Alcune osservazioni sui diritti fondamentali europei e sul "multilevel constitutionalism"*, in *Giurcost.org, Liber Amicorum per Pasquale Costanzo*, 17 luglio 2019.

GAMBINO A.M., PETTI R., *Privacy e proprietà intellettuale*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

GARCIA M., *Racist in the machine: the disturbing implications of algorithmic bias*, in *World Policy Journal* 33 (2016) 4.

GARDINI G., *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Giappichelli, Torino, 2014.

GARDINI G., *Le regole dell'informazione. L'era della post-verità*, Giappichelli, Torino, 2017.

GIACOBBE G., *Riservatezza (diritto alla)*, in *Enciclopedia del diritto*, vol. XL, Giuffrè, Milano, 1989.

GIACOMINI G., *Potere digitale. Come Internet sta cambiando la sfera pubblica e la democrazia*, Meltemi, Milano, 2018.

GIAMPICCOLO G., *La tutela giuridica della persona umana e il diritto alla riservatezza*, in *Rivista di diritto processuale civile*, 1958.

GIANNANTONIO E., Voce *Dati personali (tutela dei)*, in *Enciclopedia del diritto*, Agg., Giuffrè, Milano, 1999.

GIANNANTONIO E., LOSANO M.G., ZENO ZENCOVICH V., *La tutela dei dati personali. Commentario alla L. 675/1996*, CEDAM, Padova, 1999.

GIANNETTI R., *La certificazione ai sensi del GDPR: standard per l'affidabilità del mercato data driven*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Giuffrè, Milano, 2021.

GIANNITI P. (a cura di), *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Il Mulino, Bologna, 2013.

GIANNONE CODIGLIONE G., *Risk-based approach e trattamento dei dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016.

GIANNONE CODIGLIONE G., *I dati personali come corrispettivo alla funzione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Diritto dell'informazione e dell'informatica*, 2017.

GIORDANO R., *La tutela amministrativa e giurisdizionale dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), in *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

GIORGIANNI M., *La tutela della riservatezza*, in S. RODOTÀ (a cura di), *Il diritto privato nella società moderna*, Il Mulino, Bologna, 1971.

GIORGIU A., LARSEN T.A., *Roles and powers of National Data protection Authorities, Moving from Directive 95/46/EC to the GDPR: stronger and more "European" DPA sas Guardians Consistency?*, in *European Data Protection Law Review*, 3/2016.

GIOVANELLA F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

GIOVANNANGELI S.F., *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

GIOVANNANGELI S.F., *La violazione di dati o data breach*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

GIUGGIOLI P.F., *Tutela della privacy e consumatore*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

GIUNTA C., *La libertà e la segretezza delle comunicazioni nella Costituzione italiana*, Aracne, Roma, 2011.

GONZÁLEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Bruxelles, 2014.

GOODMAN B. W., *A step toward accountable algorithms? Algorithmic discrimination and the European Union General Data Protection, in 29th Conference on Neural Information Processing Systems* (NIPS 2016), Barcelona, Spain.

GOODMAN B. W., FLAXMAN S., *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"*, in *AI Magazine* 38 (2017), 3.

GRANIERI M., *Il trattamento di categorie particolari di dati personali nel Regolamento UE 2016/679*, in *Nuove leggi civili commentate*, 2017.

GRECO L., *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Giappichelli, Torino, 2017.

GRECO L., *L'organigramma privacy: i soggetti del trattamento*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

GRIMALDI L., *Diritto alla deindicizzazione: dati sensibili, potere e responsabilità*, in *Diritto dell'Informazione e dell'Informatica*, fascicolo n. 2/2020.

GRISOLIA M.C., *Alcune considerazioni sul potere normativo del Garante per la protezione dei dati personali dalla l. n. 657/1996 al "Codice in materia di protezione dei dati personali"*, in P. CARETTI (a cura di), *Osservatorio sulle fonti 2003-2004. I poteri normativi delle autorità indipendenti,* Giappichelli, Torino, 2005.

GROPPI T., *Sub art. 7. Rispetto della vita privata e della vita familiare*, in R. BIFULCO, M. CARTABIA, A. CELOTTO, *L'Europa dei diritti*, Il Mulino, Bologna, 2001.

GROPPI T., *Alle frontiere dello stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in *Giurcost.org*, fascicolo n. 3/2020, 28 settembre 2020.

GROPPI T., OLIVETTI M. (a cura di), *La Repubblica delle autonomie. Regioni ed enti locali nel nuovo titolo V*, Giappichelli, Torino, 2003.

GROSSI P., *Mitologie giuridiche della modernità*, Giuffrè, Milano, 2001.

GROSSI P., *L'ultima Carta dei diritti, in Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, CEDAM, Padova, 2003.

GROSSO E., *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del Garante per la protezione dei dati personali*, in M.G. LOSANO (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001.

GUARDA P., *"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019.

GUARDIGLI E., *Le Autorità di controllo*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

GUARDIGLI E., *Le Autorità di controllo: dalla Direttiva 95/46/CE al Regolamento n. 679/2016*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, G. FINOCCHIARO (a cura di), Zanichelli, Bologna, 2019.

GUARINIELLO R., *Libertà di corrispondenza e garanzie giurisdizionali*, in *Giurisprudenza italiana*, 1968, IV.

GUERRA Y., *Il ruolo delle città metropolitane alla luce della sentenza n. 240 del 2021: governance metropolitana e funzioni*, in *Forum di Quaderni costituzionali*, 2/2022.

GUTWIRTH-LEENES-DE HERT (eds), *Reforming European Data Protection Law*, in *Law, Governance and Technology Series*, XX, Springer 2015.

HARBORTH D., PAPE S., *How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor*. New York: ACM The data base for advances in information systems, 2020-01-21, Vol.51 (1).

HIJMANS H., *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer, 2016.

HOFMANN H., *The Global Reach of EU Fundamental Rights. Data Protection and the Right to an Effective Remedy*, in *Italian Journal of Public Law*, n. 1/2015.

IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi parlamentari e di politica costituzionale*, 209, 1° semestre 2021.

ICHINO P., *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro. La disciplina giuridica della circolazione delle informazioni nell'impresa*, Giuffrè, Milano, 1979.

IELO D., *L'Agenda digitale: dalle parole ai fatti. Sanità, scuola, ricerca, start up, smart city, infrastrutture, appalti, anticorruzione, radiotelevisione*, Giappichelli editore, Torino, 2015.

IQBAL A., *Protecting Digital Privacy: Why the United States Should Follow Europe's Lead and Pass Federal Legislation*. Harvard University, Harvard Kennedy School Review, 2020, Vol. 20.

IPPOLITI MARTINI C., *Comitato Europeo per la protezione dei dati*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

JACOBELLI J. (a cura di), *Aspettando Robot. Il futuro prossimo dell'Intelligenza artificiale*, Laterza, Roma-Bari, 1987.

JANČIŪTĖ L., *European Data Protection Board: a nascent EU agency or an 'intergovernmental club'?* Oxford: Oxford University Press International data privacy law, 2020-02-01, Vol.10 (1).

KAISER B., *La dittatura dei dati*, Harper Collins, Milano, 2019.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, LUISS University Press, Roma, 2017.

KAYSEN C., *The computer, data banks, and privacy. The Diebold Research Program*. Professional Paper Series, 1968.

KELLY GARRET R., *Echo chambers online?: Politically motivated selective exposure among Internet news users*, in *Journal of computer-mediated communication*, vol. 14, n. 2/2009.

KIRSCHEN S., *Il trasferimento all'estero dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

KITCHIN R., *Big Data, new epistemologies and paradigm shifts*, in *Big data & Society*, 2014.

KITCHIN R., MCARDLE G., *What makes Big Data, Big Data?,* in *Big Data & Society*, 2016.

KLONICK K., *'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Ex-pression'*, in *Yale Law Journal*, vol. 129, 2020.

KRANENBORG H., *Protection of personal data*, in *The EU Charter of Fundamental Rights. A Commentary*, S. PEERS, T. HERVEY, J. KENNER, A. WARD (eds), OxfordPortland, Hart Publishing, 2014.

KRIMMER R., PRENTZA A., MAMROT S. (Eds), *The Once-Only Principle. The TOOP project*, Springer International Publishing, 2021.

KROLL J., HUEY J., BAROCAS S., FELTEN E. W., REIDENBERG J. R., ROBINSON D. G., YU H., *Accountable Algorithms*, in *University of Pennsylvania Law Review* 165 (2017).

KUNER C., BYGRAVE L., DOCKSEY C., *The EU General Data Protection Regulation: A Commentary*, Oxford, 2020.

KUNER C. SVANTESSON D.J.B., CATE F.H., LYNSKEY O., MILLARD C., *Machine learning with personal data: is data protection law smart enough to meet the challenge?* in *International Data Privacy Law*, 1/2017.

LABRIOLA S. (a cura di), *Le autorità indipendenti. Da fattori evolutivi ad elementi della transizione nel diritto pubblico italiano*, Giuffrè, Milano, 1999.

LAGIOIA F., SARTOR G., *Le decisioni algoritmiche tra etica e diritto*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefevbre, Milano, 2020.

LAGIOIA F., SARTOR G., SIMONCINI A., *Articolo 22*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA, (a cura di), *Codice della Privacy e Data protection*, Giuffrè, Milano, 2021.

LANDINI S., *Privacy, rischio informatico e assicurazioni*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

LAZZERINI N., *La carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Franco Angeli, Milano, 2018.

LEMME G., *Blockchain, Smart contracts, Privacy, o del nuovo manifestarsi della volontà contrattuale*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

LESSIG L., *Code, Version 2.0*, Basic Books, 2006.

LOBATO R., *Netlix Nations. Geografia della distribuzione digitale*, *Minimum fax*, Roma, 2020.

LOFGREN K., WEBSTER C.W.R., *The value of Big Data in government: The case of 'smart cities'*, in *Big Data & Society*, January–June 2020.

LONGO A., CICIRELLO L., *Città metropolitane e pianificazione di area vasta*, Franco Angeli, Milano, 2015.

LONGO E., The Risks of Social Media Platforms for Democracy: A Call for a New Regulation, in B. CUSTERS AND E. FOSCH-VILLARONGA (eds.), Law and Artificial Intelligence, Springer-The Asser Press, Berlino, 2022.

LONGO E., PIN A. *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *Diritto pubblico comparato ed europeo*, Fascicolo 1/2023, gennaio-marzo.

LONGOBARDI N., *Autorità amministrative indipendenti e sistema giuridico-istituzionale*, Giappichelli, Torino, 2009.

LOSANO M.G., *La privacy nelle legislazioni europee*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati*, Il Mulino, Bologna, 1981.

LOSANO M. G. (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*,Laterza, Roma-Bari, 2001.

LYNSKEY O., *Deconstructing data protection: the 'added-value' of a right to data protection in the eu legal order*. Cambridge, UK: Cambridge University Press The International and comparative law quarterly, 2014-07, Vol.63 (3).

LYNSKEY O., *The foundations of EU data protection law*, Oxford, 2015.

LYNSKEY O., *The Europeanisation of data protection law*, in *Cambridge Yearbook of European Legal Studies*, n. 19/2017.

LYON D., *La cultura della sorveglianza*, LUISS University Press, Roma, 2020.

LUBARSKY B., *Re-identification of "Anonymized" Data*, in *Georgetown Law Technology Review* 1 (2016), 1.

LUCARELLI A., *La città metropolitana. Ripensare la forma di stato ed il ruolo di regioni ed enti locali: il modello a piramide rovesciata*, in *federalismi.it*, 25 giugno 2014

LUCARELLI A., PATRONI GRIFFI A. (a cura di), *Dal Trattato costituzionale al Trattato di Lisbona. Nuovi studi sulla Costituzione europea*, Edizioni Scientifiche italiane, Napoli, 2009.

LUCCHINI GUASTALLA E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e Impresa*, 2018.

LUCCHINI GUASTALLA E., *Privacy e Data protection: principi generali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

LUCIANI M., *La libertà di informazione nella giurisprudenza costituzionale italiana*, in *Politica del diritto*, 1989.

LUCIANI M., *Diritti sociali e integrazione europea*, in *Associazione Italiana dei Costituzionalisti, Annuario 1999. La Costituzione europea (atti del XIV convegno annuale, Perugia, 7-8-9 ottobre 1999)*, CEDAM, Padova, 2000.

LUCIANI M., *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato, Studio del Servizio Ricerca del Parlamento europeo*, ottobre 2018, in

http://www.europeanrights.eu/public/atti/Studio_PE_su_rispetto_vita_privata_e_sfide_digitali_Italia.pdf.

MACCHIA M., FIGLIOLIA C., *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, in *Giornale di Diritto Amministrativo*, n. 4/2018.

MACRÌ I., *Digitalizzazione, innovazione e sicurezza nella P.A.*, Wolters Kluwer, Milano, 2022

MAGGIOLINO M., *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, fascicolo n. 1/2016.

MAGNANI C., *Libertà di espressione e fake news, il difficile rapporto tra verità e diritto. Una prospettiva teorica*, in *Costituzionalismo.it*, fascicolo n. 3/2018, "*Rotture e continuità nell'avvio della XVIII Legislatura*".

MAGRI M., *Diritto alla trasparenza e tutela giurisdizionale*, in *Istituzioni del Federalismo*, 2/2013.

MALAGNINO M.E., *Il ruolo del Garante all'alba del GDPR: verso un'autorità*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

MALFATTI E., *I "livelli" di tutela dei diritti fondamentali nella dimensione europea*, Giappichelli, Torino, 2015.

MALGIERI G., *Articolo 5*, in D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G. (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021

MALGIERI G., *Manipolazione commerciale e privacy mentale all'ombra del GDPR*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

MANHEIM K., KAPLAN L., *Artificial Intelligence: Risks to Privacy and Democracy*, in *Yale Journal of Law & Technology*, vol. 21, 25 ottobre 2018.

MANCOSU G., *Trasparenza amministrativa e Open Data: un binomio in fase di rodaggio*, in *federalismi.it*, 17/2012.

MANES V., MAZZACUVA F., *GDPR e nuove disposizioni penali del Codice privacy*, in *Diritto penale e processo*, n. 2/2019.

MANETTI M., *Le autorità indipendenti*, Laterza, Roma-Bari, 2007.

MANNI B., *Sviluppo sostenibile e rigenerazione urbana tra tutela dell'ambiente e inclusione socioeconomica*, in *Diritto pubblico*, Fascicolo 1, gennaio-aprile 2022.

MANNONI S.-STAZI G., *Is competition a click away. Sfida al monopolio nell'era digitale*, Editoriale scientifica, Napoli, 2018.

MANTELERO A., *Il diritto alla riservatezza nella l. n. 675 del 1996: il nuovo che viene dal passato*, in *Rivista trimestrale di diritto e procedura civile*, fascicolo 3/2000.

MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012.

MANTELERO A., *The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'*. Oxford: Elsevier Ltd The computer law and security report, 2013-06, Vol.29 (3).

MANTELERO, From Safe Harbour to Privacy Shield. The ''medieval'' sovereignty on personal data, CeI, n. 1/2016.

MANTELERO A., *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer law & Security review*, 2016.

MANTELERO A, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework* Elsevier Ltd The computer law and security report, 2017-10, Vol.33 (5).

MANTELERO A., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. FINOCCHIARO (a cura di), Zanichelli, Bologna, 2017.

MANTELERO A., *Il Consiglio d'Europa adotta le prime linee guida internazionali su Big Data e tutela dei dati personali*, in *Diritto Mercato Tecnologia*, 2017.

MANTELERO A., *Responsabilita` e rischio nel reg. UE 2016/679*, in *Nuove leggi civili commentate*, 1/2017.

MANTELERO A., *Il cloud computing*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

MANTELERO A., *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

MANTELERO A., *La privacy all'epoca dei Big Data*, in *I dati personali nel diritto europeo*, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Torino, Giappichelli, 2019.

MANTELERO A., *Sulle regole AI l'Europa sceglie approccio "industriale": luci e ombre*, in *AgendaDigitale*, 27 aprile 2021.

MANTELERO A., VACIAGO G., *The "Dark Side" of Big Data: private and public interaction in social surveillance. How data collections by private entities affect governamental social control and how the EU reform on data protection responds*, in *Computer Law Rev. Int*., 2013.

MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

MANTELERO A., VACIAGO G., *Internet of things (IoT)*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

MARESCA A., CIUCCIOVINO S., ALVINO I., *Regolamento UE 2016/679 e rapporto di lavoro*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

MARCELLI F., MARSOCCI P., PIETRANGELO M., (a cura di), *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, Editoriale scientifica, Napoli, 2015.

MARSOCCI P., *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista AIC*, n. 1/2015.

MARTINICO G., *Sub art. 7*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.

MASTROIANNI R., POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O, (a cura di), Carta dei diritti fondamentali dell'Unione europea, Giuffrè, Milano, 2017.

MASUCCI A., *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, in *Diritto pubblico*, Fascicolo 1, gennaio-aprile 2019.

MATHIEU V., *Privacy e dignità dell'uomo. Una teoria della persona*, Giappichelli, Torino, 2004.

MATTEUCCI N., (a cura di) *Privacy e banche dati*, Il Mulino, Bologna, 1981.

MAURO T., *I Big data tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

MAYER-SCHÖNBERGER V., CUKIER K., *Big Data. A revolution that will transform how we live, work and think*, Boston, 2013.

MARCHETTI B., *Amministrazione digitale*, in *Enc. dir. (i tematici), III Funzioni amministrative*, Milano, Giuffrè, 2022.

MARZO R., *Dati e Open Data: polifunzionalità e rilevanza costituzionale?,* in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

MAZZAMUTO S., *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, tomo 1, Giuffrè, Milano, 2006.

MAZZINI G., SCALZO S., *The proposal for the Artificial Intelligence Act: considerations around some key concepts*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

MENDOZA I., BYGRAVE L. A., *The Right not to be Subject to Automated Decisions based on rofiling*, in T. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU (a cura di), *EU Internet Law*, Springer International, 2017.

MENEGHETTI M.C., *I trasferimenti di dati personali all'estero*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

MERLONI F., *Sull'emergere della funzione di informazione nelle pubbliche amministrazioni*, in F. MERLONI (a cura di) *L'informazione delle pubbliche amministrazioni*, Maggioli, Santarcangelo di Romagna, 2002.

MERLONI F. (a cura di), *La trasparenza amministrativa*, Giuffrè, Milano, 2008.

MERUSI F., PASSARO M., *Le autorità indipendenti*, Il Mulino, Bologna, 2011.

MESSINA D., *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *federalismi.it*, 24 ottobre 2018.

MESSINA S*., L'adeguamento della normativa nazionale al Regolamento*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

MEZZANOTTE F., *I poteri privati nell'odierno diritto dello sviluppo economico*, in *Politica del diritto*, 3/2018.

MICHELI M., PONTI M., CRAGLIA M., BERTI SUMAN A., *Emerging models of data governance in the age of datification*, in Big Data & Society, July-December: 1-15, 2020.

MIDIRI M., *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *federalismi.it*, 13 maggio 2020.

MIGLIARESE CAPUTI F., *Diritto degli enti locali. Dalla autarchia alla sussidiarietà*, Giappichelli, Torino, 2016.

MILAZZO P., *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

MITTELSTADT B. D., ALLO P., TADDEO M., WACHTER S., FLORIDI L., *The ethics of algorithms: Mapping the debate*, in *Big Data & Society* 3 (2016) 2.

MOBILIO G., *Le Città metropolitane. Dimensione costituzionale e attuazione statutaria*, Giappichelli, Torino, 2017.

MOBILIO G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021.

MOCCIA L. (a cura di), *Diritti fondamentali e cittadinanza europea*, Franco Angeli, Milano, 2010.

MODAFFERI F., *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Giappichelli, Torino, 2021.

MONE D., *Città metropolitane. Area, procedure, organizzazione del potere, distribuzione delle funzioni*, in *federalismi.it*, 9 aprile 2014.

MONTAGNANI M.L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato Concorrenza Regole*, 2019 (2).

MONTANARO D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

MONTARULI V., *La protezione dei dati personali e il minore*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

MONTELEONE A.G., *Il diritto alla portabilità dei dati. Tra diritti della persona e diritti del mercato*, in LUISS Law Review, 2/2017.

MONTELEONE S., *Privacy, data protection e identità elettronica. Tra rapidi sviluppi della tecnologia e nuovo approccio europeo*, in M. VILLONE, A. CIANCIO, G. DE MINICO, G DEMURO, F. DONATI (a cura di), *Nuovi mezzi di comunicazione e identità*, Aracne, Roma, 2012.

MONTEROSSI M.W., *Estrazione e (ri)utilizzo di informazioni digitali all'interno della rete Internet. Il fenomeno del c.d. web-scraping*, in *Diritto dell'Informazione e dell'Informatica*, fascicolo. n. 2/2020.

MONTI A., *Tutela della vita privata, protezione dei dati personali e privacy. Ambiguità semantiche e problemi definitori*, in *Diritto di Internet, Digital Copyright e Data Protection*, n. 1/2019.

MONTUORI L., *Il superamento del Privacy Shield e la (libera?) circolazione commerciale dei dati fuori dalla UE*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, Giuffrè, Milano, 2021, 89 ss.

MORETTI A., *Il Valore dei dati nell'European Data Strategy: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.

MOROZOV E., *Silicon Valley: i signori del silicio*, Codice, Torino, 2016.

MOROZOV E., *L'ingenuità della rete. Il lato oscuro della libertà di internet*, Codice, Torino, 2019.

MORTATI C., *Istituzioni di diritto pubblico*, I, Padova, 1991.

MOSCO V., *The Smart City in a Digital World*, Emerald Publishing Limited, 2019.

MOSTACCI E., *Critica della ragione algoritmica: Internet, partecipazione politica e diritti fondamentali*, in *Costituzionalismo.it*, 2/2019.

MULAZZANI G., *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. FINOCCHIARO (a cura di*), La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

MULAZZANI G., *Il trattamento di categorie particolari di dati personali, necessario per motivi di pubblico interesse rilevante*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

MULAZZANI G., *Le sanzioni amministrative in materia di protezione dei dati personali nell'ordinamento europeo ed in quello nazionale*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Torino, 2019.

MULAZZANI G., *La collaborazione pubblico-privato e la sussidiarietà orizzontale da principio a modello efficace per lo sviluppo*, Cacucci Editore, Bari, 2020.

MUMFORD L., *Il mito della macchina*, Mondadori, Milano, 1969.

MURGANTE B., BORRUSO G., *Smart cities: un'analisi critica delle opportunità e dei rischi*, in GEOmedia, n. 3/2013.

MURGO M., *Diritti di libertà*, P. GIANNITI (a cura di), in *I diritti fondamentali nell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Zanichelli, Bologna, 2013.

MURRAY A., *Information Technology Law*, the Law and Society, Oxford University Press, 2019.

NAZZARO A.C., *Privacy, Smart cities e smart cars*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

NERVI A., *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

NICOTRA I.A., VARONE V., *L'algoritmo, intelligente ma non troppo*, in *Rivista AIC*, 4/2019.

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, CEDAM, Padova, 2006.

NITTI M., *Le disposizioni relative a specifiche situazioni di trattamento: la libertà di espressione e di informazione, l'accesso del pubblico ai documenti ufficiali e il trattamento del numero di identificazione nazionale*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

NOVARIO F., *Motori di ricerca, diritto all'oblio e social network: il caso Google+*, in F. PIZZETTI (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

O'NEIL C., *Weapons of math destruction. How big data increases inequality and threatens democracy*, Penguin Books 2017.

OOMS W., CANIËLS M.C.J., ROIJAKKERS N., COBBEN D., *Ecosystems for smart cities: tracing the evolution of governance structures in a dutch smart city initiative*, in *International Entrepreneurship and Management Journal* (2020) 16.

ONIDA V., *Le Costituzioni. I principi fondamentali della Costituzione italiana*, in G. AMATO, A. BARBERA (a cura di), *Manuale di diritto pubblico*, I, Il Mulino, Bologna, 1997.

OREFICE M., *I big data. Regole e concorrenza*, in *Politica del diritto*, 2016.

OREFICE M., *I Big data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne Editrice, Roma, 2018.

ORLANDO V.E., *Principii di diritto costituzionale*, Barbera, Firenze, 1905.

OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Giappichelli, Torino, 2014.

OROFINO M., PIZZETTI F.G. (a cura di), *Privacy, minori e cyberbullismo*, Giappichelli, Torino, 2018.

ORSONI G., D'ORLANDO E., *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del Federalismo*, n. 3/2019.

OSU T., NAVARRA D., *Development of a data governance framework for smart cities*, in *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume XLVIII-4/W5-2022.

OTTALIA A., *Big data e innovazione computazionale*, in *Quaderni di Aida*, 28 (2017), Torino.

PACE A., Voce *Libertà personale (diritto costituzionale)*, in *Enciclopedia del diritto*, XXV, Giuffrè, Milano, 1974.

PACE A., *Problematica delle libertà costituzionali*, II, CEDAM, Padova, 1992.

PACE A., *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza?)*, in *Giurisprudenza costituzionale*, 1993.

PACE A., MANETTI M., *Commento all'art. 21*, in G. BRANCA, A. PIZZORUSSO (a cura di), *Commentario alla Costituzione*, Zanichelli, Bologna, 2006.

PACE A., ZACCARIA R., DE MINICO G. (a cura di), *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008.

PADOVANI C., MUSIANI F., PAVAN E., *I diritti umani nell'età digitale: concetti in evoluzione e norme emergenti nel contesto transnazionale*, in *Politica del diritto*, III, settembre 2010.

PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008.

PAGALLO U., *Privacy e design*, in *Informatica e diritto*, vol. XVIII, n. 1/2009.

PAGALLO U., *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014.

PAGANO F.F., *Pubblica amministrazione e innovazione tecnologica*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

PAGNANELLI V., *Accesso, accessibilta`, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, in Giornale di storia costituzionale, n. 31/2016.

PAGNANELLI V., *Immuni: spunti per una riflessione privacy-oriented*, in *Questione giustizia*, 12 maggio 2020.

PAGNANELLI V. Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance alla luce delle nuove sfide globali, in Rivista italiana di Informatica e Diritto, Fascicolo 1/2021.

PAGNANELLI V., *Intelligenza artificiale e sviluppo urbano. Lo studio del Parlamento europeo, in Laboratorio sulla Transizione Digitale*, https://www.civiltadellemacchine.it/, 15 dicembre 2021.

PAGNANELLI V., *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *Osservatorio sulle fonti*, 2/2021.

PAGNANELLI V., *Il settore pubblico alla sfida dell'Intelligenza artificiale*, in C. CAMARDI (a cura di) *La via europea per l'intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

PAGNANELLI V., *Una "valutazione d'impatto" della privacy sulle Big Tech. Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati perso-nali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.

PAGNANELLI V., *La Smart city come ecosistema digitale. Profili di data governance*, in *Dirittifondamentali.it*, Fascicolo 2/2023, 12 giugno 2023.

PAJNO A., BASSINI M., DE GREGORIO G., MACCHIA M., PATTI F.P., POLLICINO O., QUATTROCCOLO S., SIRENA D., *AI: profili giuridici Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal-Rivista di BioDiritto* n. 3/2019.

PAJNO A., VIOLANTE L. (a cura di), *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, Il Mulino, Bologna, 2021.

PALADIN L., *Libertà di pensiero e libertà di informazione: le problematiche attuali*, in *Quaderni costituzionali*, 1987.

PALLARO P., *Libertà della persona e trattamento dei dati nell'Unione europea*, Giuffrè, Milano, 2002.

PALLONE E.C., *La profilazione degli individui connessi a Internet: privacy online e valore economico dei dati personali*, in *Ciberspazio e Diritto*, 2015.

PALMIRANI M., Big Data e conoscenza, in Riv. fil. dir., 2020, 1, pp. 73-92.

PALOMBELLI G., *Le informazioni pubbliche come risorsa. Profili comparati*, in F. MERLONI (a cura di), *L'informazione delle pubbliche amministrazioni*, Maggioli, Santarcangelo di Romagna, 2002.

PANETTA R., (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2007.

PANETTA R., (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, Giuffrè Francis Lefebvre, Milano, 2019.

PANETTA R., *Privacy is not dead: it's hiring!,* in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

PAPA A., *Trasferimento di dati all'estero*, in *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffrè, Milano, 2004.

PAPA A., *La problematica tutela del diritto all'autodeterminazione informativa nella big data society*, in *Giurcost.org, Liber Amicorum per Pasquale Costanzo*, 17 aprile 2020.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003.

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003.

PARDOLESI R., *Piattaforme digitali, poteri privati e concorrenza*, in *Diritto Pubblico*, 3/2021.

PASQUALE F., *The black box society. The Secret Algorithms that control money and information*, Harvard University Press, 2015.

PASQUINO T., *Identità digitale della persona, diritto all'immagine e reputazione*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

PASSAGLIA P., *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Giurcost.org,* 3/2016.

PASSAGLIA P., *Il sistema delle fonti normative in materia di tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

PATANE' A., *Democrazia rappresentativa durante la pandemia: il ruolo dei consigli regionali*, in A. PAJNO, L. VIOLANTE (a cura di), *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, Il Mulino, Bologna, 2021Vol. I.

PATRONI GRIFFI A., *L'indipendenza del Garante*, in *federalismi.it*, 14 febbraio 2018.

PATRONI GRIFFI F., *Intelligenza artificiale: amministrazione e giurisdizione*, in U. RUFFOLO, *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefevbre, Milano, 2020.

PATRONI GRIFFI F., *La trasparenza della Pubblica amministrazione tra accessibilità totale e riservatezza*, in *federalismi.it*, n. 8/2013, 16 aprile 2013.

PATRONI GRIFFI A., *Le città metropolitane nel guado costituzionale*, in *federalismi.it*, 6 luglio 2016.

PATRONO P., Voce *Privacy e vita privata (diritto penane)*, in *Enciclopedia del diritto*, XXXV, Giuffrè, Milano, 1986.

PATTI L., *Artt. 68-71*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

PEDUTO A., *art. 81*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

PELINO E., *Ambito di applicazione territoriale*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

PELINO E., *Approfondimento su alcune tipologie di dati personali*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

PELINO E., *Trattamento*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

PELINO E., *I soggetti del trattamento*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

PELLECCHIA E., *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civili e commentate* 41 (2018), 5.

PELLECCHIA E., *Privacy, decisioni automatizzate e algoritmi*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

PENNACCHI R., *Aspetti tecnici della sicurezza dei dati*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati*, Il Mulino, Bologna, 1981.

PERLINGIERI P., *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro napoletano*, 2018, 2.

PEZZA F., *Certification mechanism as a tool for the unification of data protection European law*, in *Medialaws* 1/2018.

PICCONE V., POLLICINO O. (a cura di), *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività*, Editoriale scientifica, Napoli, 2018.

PIERRI M. *Autorità indipendenti e dinamiche democratiche*, CEDAM, Padova, 2009.

PIERUCCI A., *Elaborazione dei dati e profilazione delle persone*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

PIRAINO F., *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili commentate*, n. 2/2017.

PIRAINO F., *GDPR tra novità e discontinuità. I "diritti dell'interessato" nel regolamento generale sulla protezione dei dati personali*, in *Giurisprudenza Italiana*, n. 12/2019.

PIRODDI P., *art. 16 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, seconda edizione, CEDAM, Padova, 2014.

PIRODDI P., *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *Diritto dell'informazione e dell'informatica*, 2015.

PISA R., *Il digital divide e le iniziative per superarlo*, in *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, F. MARCELLI, P. MARSOCCI, M. PIETRANGELO, (a cura di), Editoriale scientifica, Napoli, 2015.

PISAPIA A., *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *federalismi.it*, 31 gennaio 2018.

PITRUZZELLA G., *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, 1, gennaio 2016.

PITRUZZELLA G., *La libertà di informazione nell'era di Internet*, in G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI (a cura di), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, Milano, 2017.

PITRUZZELLA G., *L'Europa del mercato e l'Europa dei diritti*, in *federalismi.it*, Editoriale 20 marzo 2019.

PIZZETTI F., *Efficacia delle norme comunitarie nell'Ordinamento italiano*, Estratto dal Notiziario Giuridico Regionale della Federazione delle Associazioni Industriali del Piemonte n. 1 – 1982.

PIZZETTI F., *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013.

PIZZETTI F., *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya"*, in *Diritto dell'informazione e dell'informatica*, 2014.

PIZZETTI F. *La riforma degli enti territoriali. Città metropolitane, nuove province e unione di comuni*, Giuffrè, Milano, 2015.

PIZZETTI F. (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

PIZZETTI F., *Tutela della persona, diritto all'oblio, web reputation e identità digitale. Internet e la Luce delle Stelle*, in F. PIZZETTI (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016.

PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

PIZZETTI F., *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in MANTELERO A., POLETTI D. (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, Pisa, 2018.

PIZZETTI F., *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *MediaLaws*, n. 1/2018.

PIZZETTI F., *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Giappichelli, Torino, 2021.

PIZZETTI F., GRECO L., *art. 24*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

PIZZOLATO F., SCALONE A., CORVAJA F. (a cura di), *La città e la partecipazione tra diritto e politica*, Giappichelli, Torino, 2019.

POCAR F., BARUFFI M.C., *Commentario breve ai trattati dell'Unione europea*, CEDAM, Padova, 2014.

POGGI A., *Dati personali. Una soluzione "giurisdizionale" oppure "amministrativa" per l'effettiva tutela del cittadino?,* in M.G. LOSANO (a cura di), *La legge italiana sulla privacy: un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001.

POLETTI D., *Gli intermediari dei dati*, in *European Journal of Privacy Law and Technologies*, 1/2022.

POLETTI D., MANTELERO A., *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, Pisa, 2018.

POLETTI D., CASAROSA F., *Il diritto all'oblio (anzi, i diritti all'oblio) secondo le Sezioni Unite*, in *Diritto di Internet, Digital Copyright e Data Protection*, n. 4/2019.

POLETTI D., CAUSARANO M.C., *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* Giuffrè Francis Lefebvre, Milano, 2019.

POLITI F., *Libertà costituzionali e diritti fondamentali. Casi e materiali. Un itinerario giurisprudenziale*, Giappichelli, Torino, 2021.

POLLICINO O., *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *federalismi.it*, 24 novembre 2014.

POLLICINO O., BASSINI M., *art. 8*, in *Carta dei Diritti fondamentali dell'Unione europea*, R. MASTROIANNI, O. POLLICINO, A. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), Giuffrè, Milano, 2017.

POLLICINO O., *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in V. PICCONE, O. POLLICINO (a cura di), *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività*, Editoriale scientifica, Napoli, 2018.

POLLICINO O., *L'"autunno caldo" della corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *federalismi.it*, Editoriale – 16 ottobre 2019.

POLLICINO O., BASSINI M., DE GREGORIO G.*, Il Gdpr e la protezione dei dati nella società algoritmica: i nuovi sviluppi normativi e giuridici,* in Agenda *Digitale*, 10 settembre 2021.

PONTI B. (a cura di), *La trasparenza amministrativa dopo il d. lgs. 14 marzo 2013 n. 33. Analisi della normativa, impatti organizzativi ed indicazioni operative*, Maggioli, Santarcangelo di Romagna, 2013.

POPOLI A.R., *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

PREDIERI A., *L'erompere delle autorità amministrative indipendenti*, Passigli, Firenze, 1997.

PREDIERI A., *Gli elaboratori elettronici nell'amministrazione dello Stato*, Il Mulino, Bologna, 1971.

PRINCIPATO A.*, Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contratto e impresa*. Europa, n. 1/2015.

QUAGLIONE D., POZZI C., *Economia dei big data: Lineamenti del dibattito in corso e alcune riflessioni di policy*, in *L'industria*, XXXIX, n. 1, gennaio-marzo 2018.

QUINTARELLI S., *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, Torino, 2019.

QUNTARELLI S., COREA F., FOSSA F., LOREGGIA A., SAPIENZA S., *AI: profili etici. Una prospettiva etica sull'Intelligenza artificiale: princìpi, diritti e Raccomandazioni*, in *BioLaw Journal–Rivista di BioDiritto*, n. 3/2019.

RAAB C., SZEKELY I., *Data protection authorities and information technology*. Elsevier B.V. Computer Law & Security Review, 2017, Vol.33 (4).

RANCHORDAS S. – KLOP A., *Data-driven regulation and governance in smart cities,* University of Groningen Faculty of Law Legal Studies Research Paper Series No. 7/2018.

RATTI M., *La responsabilità da illecito trattamento dei dati personali*, G. FINOCCHIARO (a cura di), *in La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

RECCIA D., *art. 3. Ambito di applicazione territoriale*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

RESCIGNO P., *Diritto all'intimità della vita privata*, in *Studi in onore di F. Santoro Passarelli*, 1993.

RESCIGNO P., *Protezione dei dati e diritti della personalità*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1998.

RESTA G*., Identità personale e identità digitale*, estratto da *Il diritto dell'Informazione e dell'Informatica*, Anno XXIII, Fascicolo 3, Milano, 2007.

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Diritto dell'informazione e dell'informatica*, 2015.

RESTA G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, II, giugno 2019.

RESTA G., *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679 2019*, in *Annuario del contratto*, 2019.

RESTA G., *Cosa c'è di "europeo" nella proposta di Regolamento UE sull'Intelligenza artificiale?*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, Anno 2022, Fascicolo 4.

RESTA G., ZENO ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles al "Privacy Shield"*, collana *Consumatori e Mercato*, Roma, 2016.

RESTA G., ZENO-ZENCOVICH V., *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, Fascicolo n. 2/2018.

RICCI A., *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, vol. 33, n. 2/2017.

RICCI A., *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

RICCI M.R., *La città metropolitana nell'ordinamento giuridico italiano. Percorsi istituzionali e profili di criticità*, Il Mulino, Bologna, 2020.

RICCIO G.M., *art. 82*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

RICCIO G.M., *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e regolamento privacy*, in *La nuova giurisprudenza civile commentata*, n. 12/2018.

RICCIO G.M., PEZZA F., *Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

RICCIO G.M., PEZZA F., *Portabilità dei dati personali e interoperabilità*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

RICCIO G.M., SCORZA G., BELISARIO E. (a cura di), *GDPR e normativa privacy. Commentario*, Wolters Kluwer, Milano, 2018.

RICCIUTO V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

RICHARDS N. M., KING J. H., *Three Paradoxes of Big Data*, in *Stanford Law Review Online* 66 (2013).

RIGANO F., TERZI M., *Lineamenti dei diritti costituzionali*, Franco Angeli, Milano,2021.

RIGHETTINI M.S., *Regolare e rappresentare i nuovi diritti nell'era del web: il garante per la tutela della privacy*, in *Politica del diritto* Fascicolo 3, settembre 2010.

RIZZO V., *Artt. 55-56*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

RODOTA' S., *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974.

RODOTA' S., *Progresso tecnico e problemi istituzionali nella gestione delle informazioni*, in N. MATTEUCCI (a cura di), *Privacy e Banche dati*, Bologna, 1981.

RODOTÀ S., *Protezione dei dati e circolazione delle informazioni*, in *Rivista critica di diritto privato*, 1984.

RODOTÀ S., *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, 1991.

RODOTÀ S., *Intorno alle privacy. Ipotesi e prospettive*, in *Studi in memoria di Franco Piga*, vol. 2, Milano, 1992.

RODOTÀ S., *Tecnologie e diritti*, Il Mulino, Bologna, 1995.

RODOTA' S., *Tecnopolitica*, Laterza, Roma-Bari, 1997.

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1998.

RODOTÀ S., *Repertorio di fine secolo*, Laterza, Bari, 1999.

RODOTÀ S., Voce *Riservatezza*, in Enciclopedia Italiana, VI Appendice, Istituto della Enciclopedia Italiana, 2000.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma, 2004.

RODOTÀ S*., Intervista su privacy e libertà*, P. CONTI (a cura di), Laterza, Bari-Roma, 2005.

RODOTÀ S., *Prefazione*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, tomo 1, Milano, 2006.

RODOTÀ S., *Data Protection as a Fundamental Right*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (eds), *Reinventing Data Protection?,* Springer, 2009.

RODOTÀ S., *La vita e le regole: tra diritto e non diritto*, Feltrinelli, Milano, 2006.

RODOTÀ S., *Una Costituzione per Internet?*, in *Politica del diritto*, fascicolo n. 3/2010.

RODOTA' S., *Il diritto di avere diritti*, Laterza, Bari, 2012.

RODOTA' S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Roma-Bari, 2014.

RODOTÀ S., *Vivere la democrazia*, Laterza, Bari-Roma, 2018.

RODOTA' S., *Il cittadino e l'elaboratore elettronico, Quaderno dell'Istituto di ricerche sullo Stato e l'amministrazione*.

ROMANO C., *Open data e riutilizzo nel decreto trasparenza: propulsore per la democrazia e lo sviluppo o sfida ulteriore per i diritti fondamentali?,* L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014.

ROSSI E., *art. 2*, in R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, vol. 1, Utet, Torino, 2006.

ROSSI DAL POZZO F., *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, 2016.

ROTENBERG M., *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, in *European Law Journal*, 11 settembre 2020.

RUBECHI M., *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, 23, 2016.

RUBINO A., *Minori e privacy: una tutela rafforzata?*, in M. VILLONE, A. CIANCIO, G. DE MINICO, G. DEMURO, F. DONATI (a cura di), *Nuovi mezzi di comunicazione e identità. Omologazione o diversità?*, Aracne, Roma, 2012.

RUBINSTEIN I.S., *Big Data: The End of Privacy or a New Beginning?,* in *International Data Privacy Law*, vol. 3, n. 2/2013.

RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020.

RUGGERI A., *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in Giurcost.org, 3/2016.

RUGGERI, *La tutela "multilivello" dei diritti fondamentali, tra esperienze di normazione e teorie costituzionali*, in *Politica del diritto*, 3/2007.

RUGGERI A., SPADARO A., *Lineamenti di giustizia costituzionale*, Giappichelli, Torino, 2001.

RUOTOLO G.M., *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018.

SALERNO G.M., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, I, Giappichelli, Torino, 2001.

SALERNO G.M., *Le origini ed il contesto*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

SALVIA L., *Pianificazione strategica e indirizzo politico nelle Città metropolitane alla luce della riforma "Delrio" (legge 56 del 2014)*, in *Osservatorio costituzionale* – AIC, 2, 2016.

SAMMARCO P., *Giustizia e social media*, Il Mulino, Bologna, 2019.

SAMMARCO P., *Privacy digitale, motori di ricerca e Social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

SAMMARCO P., *L'attività di web scraping nelle banche dati ed il riuso delle informazioni*, in *Diritto dell'informazione e dell'informatica*, fascicolo n. 2/2020.

SANDULLI A.M., *Manuale di diritto amministrativo*, II, Jovene, Napoli, 1990.

SANINO M., *L'approdo dell'esperienza delle autorità indipendenti a oltre venti anni dalla loro istituzione*, CEDAM, Padova, 2015.

SANTANIELLO G. (a cura di), *La protezione dei dati personali*, in *Trattato di Diritto amministrativo*, diretto da G. Santaniello, CEDAM, Padova, 2005.

SANTANIELLO M., *Diritti umani nel ciberspazio. Patrimonio, persona e lex digitalis*, *Politica del diritto*, III, settembre 2010.

SANTOSUOSSO A., *Sistemi tecnologici, emozioni e regole*, in *Sociologia del diritto*, n. 1/2018.

SARTOR G., *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz",* in *Informatica e diritto*, 3/1986.

SARTOR G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996.

SARTOR G., *The Right to be Forgotten: Dynamics of Privacy and Publicity*, in L. FLORIDI (a cura di), *Protection of Information and the Right to Privacy – A New Equilibrium?,* Springer, 2014.

SARTOR G., LAGIOIA F., *Le decisioni algoritmiche tra etica e diritto*, in in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020.

SARTORE F., *Privacy by design, l'introduzione del principio nel corpus del GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019.

SARTORE F., *La valutazione d'impatto nel GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre Milano, 2019.

SARTORETTI C., *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *federalismi.it*, 3 luglio 2019.

SASSANO F., *Il diritto all'oblio tra Internet e mass media*, Vicalvi, 2015.

SASSO I., *Privacy post-mortem e "successione digitale"*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

SCAFFARDI L., *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, Santarcangelo di Romagna, 2013.

SCAGLIARINI S., *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013.

SCAGLIARINI S., *Identità digitale e tutela della privacy*, in P. COSTANZO, P. MAGARO', L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale scientifica, Napoli, 2022.

SCALISI A*., Il diritto alla riservatezza: il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, Giuffrè, Milano, 2002.

SCHREMER B.W., CUSTERS B., VAN DER HOF S., *The crisis of consent: how stronger legal protection may lead to weaker consent in data protection* Dordrecht: Springer Netherlands Ethics and information technology, 2014-06, Vol.16 (2).

SCIACCHITANO F., *Disciplina e utilizzo degli Open Data in Italia*, in Medialaws 1/2018.

SCORZA G., *Corte di Giustizia e diritto all'oblio: una sentenza che non convince*, in *Corriere giuridico*, n.2, 2015.

SCORZA G., *art. 2. Ambito di applicazione materiale*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Giuffrè, Milano, 2018.

SCOTTI G., *Dall'Habeas Corpus all'Habeas Data: il diritto all'oblio ed il diritto all'anonimato nella loro dimensione costituzionale*, in *diritto.it*, 7 settembre 2015.

SELBST A.D., POWLES J., *Meaningful information and the right to explanation*, in *International Data Privacy law*, 2017.

SENESE A., *Il diritto alla riservatezza nella prospettiva del diritto costituzionale europeo*, in M. SCUDIERO (a cura di), *Il diritto costituzionale comune europeo*, Jovene, Napoli, 2002.

SESSO SARTI O., *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

SIANO M., TEMPESTINI L., *Il diritto di rettifica e di cancellazione dei dati. Il regolamento europeo e gli interventi più significativi del Garante*, in F. PIZZETTI (a cura di), *Internet e la tutela della persona, Il caso del motore di ricerca*, Passigli, Bagno a Ripoli, 2015.

SICA S., *La libertà fragile. Pubblico e privato al tempo della rete*, Edizioni Scientifiche italiane, Napoli, 2014.

SICA S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO, (a cura di) *La nuova disciplina europea della privacy*, Giuffrè, Milano, 2016.

SICA S., STANZIONE P., (a cura di), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Il Mulino, Bologna, 2004.

SICA S., D'ANTONIO V., RICCIO G.M., (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016.

SIEGEL E., *Analisi predittiva. Sapere in anticipo chi clicca, compra, mente, muore*, LSWR, Milano, 2013.

SILVESTRI A., *Dal potere ai principi: Libertà ed eguaglianza nel costituzionalismo contemporaneo*, Laterza, Roma-Bari, 2009.

SIMONCINI A., *Autorita`indipendenti e costruzione dell'ordinamento giuridico: il caso del Garante per la protezione dei dati personali*, in *Diritto pubblico*, 3/1999.

SIMONCINI A., *Sovranità e potere nell'era digitale*, in *Diritti e libertà in Internet*, T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), Mondadori, Milano, 2017.

SIMONCINI A., *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, IV, dicembre 2019.

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto*, n. 1/2019.

SIMONCINI A., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in *Il diritto dell'amministrazione pubblica digitale*, R. CAVALLO PERIN, D.U. GALETTA (a cura di), Giappichelli, Torino, 2020.

SIMONCINI A., *Verso la regolamentazione della Intelligenza artificiale. Dimensioni e governo*, in *BioLaw Journal – Rivista di BioDiritto*, vol. 2, 2021.

SIMONCINI A., *Quale modello per la regolazione dell'Intelligenza artificiale? L'Europa al bivio*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

SIMONCINI A., *La dimensione costituzionale dell'Intelligenza artificiale*, in *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), Il Mulino, Bologna, 2022.

SIMONCINI A., MOBILIO G., *L'identità delle Città metropolitane attraverso i loro Statuti: sintomi di una sindrome "bipolare"?*, in *Le Regioni*, 2016.

SIMONCINI A.- SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, I, giugno 2019.

SOANA G., *Intelligenza artificiale e architettura del controllo. Una riflessione sull'utilizzo delle tecnologie di riconoscimento facciale basate su IA negli spazi pubblici*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

SOLA A., *Utilizzo dei big data nelle decisioni pubbliche tra innovazione e tutela della privacy*, in *MediaLaws*, 24 dicembre 2020.

SOLINAS C., *La nuova figura del responsabile della protezione dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

SOLUM L.B., *Artificially intelligent law*, in *BioLaw Journal - Rivista di BioDiritto*, 1/2019, 53 ss.

SORO A., *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Baldini e Castoldi, Milano, 2019.

SORRENTINO F., *Il controllo del garante per la protezione dei dati personali e l'autorità giudiziaria secondo le più recenti norme eurounitarie*, in *Questione giustizia*, 15 febbraio 2018.

SPANGARO A., *L'ambito di applicazione materiale della disciplina del Regolamento europeo 679/2016*, G. FINOCCHIARO (a cura di), in *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019.

SPILLER E., *Citizens in the loop? Partecipazione e Smart city, in La città e la partecipazione tra di-ritto e politica*, F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), Giappichelli, Torino, 2019.

SPINA A., *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al Regolamento (UE) 2016/679*, in *Rivista dei mercati*, 2016, 1.

STADERINI F., CAROZZA P., MILAZZO P. (a cura di), *Diritto degli enti locali*, Wolters Kluwer, Milano, 2022.

STANZIONE M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, 2016.

STANZIONE P., *La via europea all'Intelligenza artificiale*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale*, Wolters Kluwer, CEDAM, Milano, 2022.

STERPA A. (a cura di), *Il nuovo governo dell'area vasta: commento alla legge 7 aprile 2014, n. 56 Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni, c.d. legge Delrio aggiornato al d.l. 24 giugno 2014, n. 90 convertito con modificazioni dalla l. 11 agosto 2014, n. 114*, Jovene, Napoli, 2014.

STRADELLA E., *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, in *Rivista AIC*, n. 4/2016.

STROZZI G., MASTROIANNI R., *Diritto dell'Unione europea. Parte generale*, Giappichelli, Torino, 2016.

SUERZ M., *Internet tra diritti e giurisprudenza*, in *Rivista di scienze della comunicazione e di argomentazione giuridica*, n. 1/2013.

TADDICKEN M., *The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure.* Oxford, UK: Blackwell Publishing Ltd Journal of computer-mediated communication, 2014-01, Vol.19 (2).

TALIA D., *La società calcolabile e i Big Data. Algoritmi e persone nel mondo digitale*, Rubettino, Roma, 2018.

TAMÒ-LARRIEUX A., *Designing for Privacy and its Legal Framework Data Protection by Design and Default for the Internet of Things*, Springer Nature Switzerland AG 2018.

TARLI BARBIERI G., *Le Città metropolitane: il quadro generale e la forma di governo*, in G.F. FERRARI (a cura di), *Nuove province e Città metropolitane*, Giappichelli, Torino, 2016.

TESAURO F., *Il ruolo della Corte di giustizia nell'elaborazione dei principi generali dell'ordinamento europeo e dei diritti fondamentali*, in *Associazione Italiana dei Costituzionalisti*, *Annuario 1999. La Costituzione europea* (atti del XIV convegno annuale, Perugia, 7-8-9 ottobre 1999), Padova, 2000.

TESTA D., *Governo e autogoverno della città digitale, luogo di conflitti tra valori pubblici e interessi privati,* in Diritto pubblico comparato ed europeo, Fascicolo 1/2023, gennaio-marzo.

THOBANI S*., La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e diritto privato*, 2016.

THYVE U.F., *One-stop-shop – or not? The Regulation of competent supervisory authority in the new EU General Data Protection Regulation – does the one-stop-shop mechanism live up to its promise?*, University of Oslo, 2016.

TIBERI G., *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), *Diritti in azione*, Il Mulino, Bologna, 2007.

TIBERI G., *La direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quaderni costituzionali*, n. 3/2016.

TIMIANI M., *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, 2/2012.

TIKKINEN-PIRI C., ROHUNEN A., MARKKULA J., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies* Elsevier Ltd The computer law and security report, 2018-02, Vol.34 (1).

TOBANI S., *Il danno non patrimoniale dal trattamento illecito di dati personali*, in *Diritto dell'informazione e dell'informatica*, 2014.

TORINO R., *La valutazione d'impatto (Data Protection Impact Assessment*), in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

TORREGIANI S., *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in *federalismi.it*, 10 giugno 2020.

TOSCHEI S., *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017.

TOSI E., *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno e responsabilità*, n. 4/2020.

TOSI E., *La responsabilità civile per trattamento illecito dei dati personali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

TOSI E*., Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice Privacy*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffro Francis Lefebvre, Milano, 2019.

TRAPANI M., *GDPR e Intelligenza artificiale: i primi passi tra governance, privacy, trasparenza e accountability*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, Pisa, 2018.

TROJSI A., *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino, 2013.

TRUCCO L., *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Giappichelli, Torino, 2013.

TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017.

TURCO V., *Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

TURING, A. M., *Computing Machinery and Intelligence*, in *Mind* 59 (1950), 236.

URBANO G., *Le "Città intelligenti" alla luce del principio di sussidiarietà*, in *Istituzioni del federalismo*, 2019.

VALASTRO A., *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Giuffrè, Milano, 2001.

VALERINI F., *Le novità processuali in materia di privacy dopo il Reg. 679/2016 (GDPR) e il D.lgs. 101/2018*, in *Judicium. Il processo civile in Italia e in Europa*, 23 ottobre 2018.

VALLE L., *Il diritto all'identità personale*, in M. SESTA, V. CUFFARO (a cura di), *Persona, famiglia e successioni nella giurisprudenza costituzionale*, Edizioni Scientifiche italiane, Napoli, 2006.

VALLE L., RUSSO B., LOCATELLO D.M., BONZAGNI G., *Privacy e contratti di cloud computing*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lebebvre, Milano, 2019.

VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Diritto dell'Informazione e dell'Informatica*, fascicolo n. 2/2017.

VANDELLI L., *Città metropolitane*, in *Enciclopedia del diritto*, Annali IX, Giuffrè, Milano, 2016.

VANDELLI L., BARRERA P., TESSARO P., TUBERTINI C., *Città metropolitane, province, unioni e fusioni di comuni: la legge Delrio, 7 aprile 2014, n. 56 commentata comma per comma*, Maggioli, Santarcangelo di Romagna, 2014.

VIGGIANO M., *L'attività cd. paragiurisdizionale nella casistica dei ricorsi proposti dinanzi al Garante per la protezione dei dati personali*, in *Rassegna di diritto pubblico europeo. Autorità indipendenti e tutela giurisdizionale nella crisi dello Stato*, n. 1- 2/2015.

VIGGIANO M*., I limiti alla pubblicità dell'azione amministrativa per finalità di trasparenza derivanti dalla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), Le nuove frontiere della trasparenza nella dimensione costituzionale, Editoriale scientifica, Napoli, 2014.

VIOLA L., *Attività amministrativa e intelligenza artificiale*, in *Ciberspazio e diritto*, vol. 20, n. 62, 1-2/2019.

VISINTINI G., *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, Milano, n. 1/2019.

WARREN S.D., BRANDEIS L.D., *The right to privacy*, *Harvard law review*, 1890.

WARSO Z., *There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age.* Oxford: Elsevier Ltd *The computer law and security report*, 2013-10, Vol.29 (5).

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017.

WANG J., QUE NGUYEN D., BONKALO T., GREBENNIKOV O., *Smart governance of urban data*, *E3S Web of Conferences* 301, 05005 (2021).

WEBBER M., *The GDPR's impact on the cloud service provider as a processor*, in *Privacy & Data Protection*, vol. 16, Issue 4, 2016.

WESTIN A.F., *Privacy and freedom*, New York, 1967.

WILLIS K.S., AURIGI A., *Digital and Smart cities*, Routeledge, London-New York, 2018.

WOLTERS P.T.J., *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, in *Int. Data privacy Law*, 2017, Vol. 7 n. 3.

WONG J., HENDERSON T., *'The right to data portability in practice: exploring the implications of the technologically neutral GDPR'*, in *International Data Privacy Law*, 2019.

YOUM K.H., PARK A., *The "Right to Be Forgotten" in European Union Law: Data Protection Balanced With Free Speech?* Los Angeles, CA: SAGE Publications Journalism & mass communication quarterly, 2016-06, Vol.93 (2).

ZACCARIA R., *Diritto dell'informazione e della comunicazione*, CEDAM, Padova, 2010.

ZACCARIA R., VALASTRO A., ALBANESI E., *Diritto dell'informazione e della comunicazione*, CEDAM, Padova, 2021.

ZAGREBELSKY G., *Manuale di diritto costituzionale. I. Il sistema delle fonti del diritto*, Utet, Torino, 1990.

ZAGREBELSKY G., *I diritti fondamentali oggi*, in *Materiali per una storia della cultura giuridica*, 1992.

ZAGREBELSKY G. (a cura di), *Diritti e Costituzione nell'Unione europea*, Laterza, Roma-Bari, 2003.

ZAGREBELSKY V., CHENAL R., TOMASI L., *Manuale dei diritti fondamentali in Europa*, Il Mulino, Bologna, 2016.

ZALLONE R., ELLI G., *Il nuovo Codice della privacy (commento al d. lgs. 30 giugno 2003, n. 196) con la giurisprudenza del Garante*, Giappichelli, Torino, 2004.

ZAMBRANO V., *Il Comitato europeo per la protezione dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019.

ZENO-ZENCOVICH V., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Corriere giuridico*, 1997.

ZENO ZENCOVICH V., *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante*, in *Corriere giuridico*, 1997.

ZENO ZENCOVICH V., *Ten legal perspectives on the "big data revolution"*, Editoriale scientifica, Napoli, 2017.

ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, n. 2/2018.

ZUBOFF S., *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Roma, 2019.

ZUBOFF S., *Molte sfaccettature di un solo diamante, in Privacy 2030. Una nuova visione per l'Europa, Garante per la protezione dei dati personali*, International Association of Privacy Professionals, novembre 2019, reperibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9457003

ZUIDERVEEN BORGESIUSM FREDERIK J., *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation* Elsevier Ltd The computer law and security report, 2016-04, Vol.32 (2).

ZUIDERVEEN BORGESIUSM F., POORT J., *Online Price Discrimination and EU Data Privacy Law* New York: Springer US Journal of consumer policy, 2017-09, Vol.40 (3).

ZUIDERVEEN BORGESIUS F.J., TRILLING D., MÖLLER J., BODÓ B., DE VREESE C.H., HELBERGER N., *Should we worry about filter bubbles?,* in *Internet Policy Review*, vol. 5, n. 1/2016.

ZUPPETTA M., *Città metropolitane e strategie di sviluppo dei territori*, Maggioli, Rimini, 2019.