La borsa di dottorato è stata finanziata con le risorse del
Programma Operativo Complementare Ricerca e Innovazione 2014-2020,
Azione I.1 "Dottorati Innovativi con caratterizzazione industriale"

UNIONE EUROPEA
Fondo Sociale Europeo

Ministero dell'Università e della Ricerca

PON RICERCA E INNOVAZIONE 2014-2020

UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI SCIENZE GIURIDICHE (SCUOLA DI GIURISPRUDENZA)

Dottorato di Ricerca in Scienze giuridiche

CICLO XXXV

Tesi di dottorato:

"Big data e predictive policing per il contrasto alla corruzione e al conflitto d'interessi nel procurement sanitario, nel rispetto dei diritti fondamentali e tutela dei dati personali"

Coordinatore:

Chiar.mo Prof. Geminello Preterossi

Tutor:

Chiar.mo Prof. Francesco Fasolino

Dottorando:

Dott. Alberto Biancardo (matr. 8800600075)

ANNO ACCADEMICO 2021-2022

La borsa di dottorato è stata cofinanziata con risorse del
Programma Operativo Nazionale Ricerca e Innovazione 2014-2020 (CCI 2014IT16M2OP005),
Fondo Sociale Europeo, Azione I.1 “Dottorati Innovativi con caratterizzazione Industriale”

UNIONE EUROPEA
Fondo Sociale Europeo

Ministero dell' Istruzione, dell'Università e della Ricerca

La borsa di dottorato è stata finanziata con le risorse del
Programma Operativo Complementare Ricerca e Innovazione 2014-2020,
Azione I.1 "Dottorati Innovativi con caratterizzazione industriale"

UNIONE EUROPEA
Fondo Sociale Europeo

La borsa di dottorato è stata finanziata con le risorse del
Programma Operativo Complementare Ricerca e Innovazione 2014-2020,
Azione I.1 "Dottorati Innovativi con caratterizzazione industriale"

UNIONE EUROPEA
Fondo Sociale Europeo

Ministero dell'Università e della Ricerca

PON RICERCA E INNOVAZIONE 2014-2020

UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI SCIENZE GIURIDICHE (SCUOLA DI GIURISPRUDENZA)

Dottorato di Ricerca in Scienze giuridiche

CICLO XXXV

Tesi di dottorato:

"Big data e predictive policing per il contrasto alla corruzione e al conflitto d'interessi nel procurement sanitario, nel rispetto dei diritti fondamentali e tutela dei dati personali"

Coordinatore:

Chiar.mo Prof. Geminello Preterossi

Tutor:

Chiar.mo Prof. Francesco Fasolino

Dottorando:

Dott. Alberto Biancardo (matr. 8800600075)

ANNO ACCADEMICO 2021-2022

Indice

Abstract

La presente ricerca analizza preliminarmente le vigenti normative anticorruzione, per poi focalizzarsi sulle nuove tecnologie utilizzate per l'individuazione di aree a rischio di conflitti di interessi, con particolare riguardo ai big data analytics e alle moderne tecniche di predictive policing.

In un Paese come l'Italia, con un elevato rischio di corruzione e le carenze di una normativa sul conflitto d'interessi, l'utilizzo di tali tecnologie può, indubbiamente, raggiungere risultati ragguardevoli, non solo nell'individuazione di reati già in atto, ma specialmente nella prevenzione e deterrenza. In particolare nel procurement del settore della sanità, il conflitto d'interessi è spesso alla base dei fenomeni corruttivi, con conseguente lievitazione della spesa pubblica e diminuzione della qualità dei servizi sanitari, costituzionalmente tutelati dall'art. 32.

In tale quadro saranno analizzate le capacità dei big data ai fini del contenimento dei fenomeni corruttivi senza, tuttavia, dimenticare i rischi riguardanti i diritti fondamentali dell'uomo e la tutela dei dati personali. Verrà, infine, proposto un innovativo utilizzo delle tecnologie, col supporto di una normativa avente il merito di creare un punto di equilibrio fra la necessità di contrastare la corruzione ed il rispetto della privacy e della tutela dei dati personali.

Introduzione

La diffusione dei fenomeni corruttivi ha, negli ultimi decenni, raggiunto livelli di guardia in molti Paesi. Gli effetti sono stati così rilevanti sul piano socio-economico, da indurre le principali organizzazioni internazionali quali l'ONU e l'OCSE, a programmare tavoli permanenti ed approvare numerosi documenti, aventi come protagonista principale il contrasto al sistema corruttivo[1]. In particolare, nei Paesi industrializzati ad elevato tasso di corruzione, come l'Italia[2], si è tentato di porre rimedio alla crescita di tale fenomeno tramite nuovi impianti normativi ed apparati di controllo più capillari; tuttavia i risultati non sono stati pienamente soddisfacenti. La necessità di controllare il fenomeno è divenuta sempre più urgente, poiché esso incide sia sulla lievitazione vertiginosa della spesa pubblica[3], ma anche sulla diminuzione drastica della quantità e qualità dei servizi offerti ai cittadini. Nella maggioranza dei casi il problema della corruzione trae origine da situazioni di conflitto di interessi, sempre frequenti nel nostro Paese poiché non esiste tutt'oggi una normativa organica e completa che lo regoli. È, difatti, innegabile che la corruzione sia essenzialmente alimentata da una prorompente e costante presenza di conflitti di interessi, in ogni settore, ed in particolare in quello delle grandi opere edili, nonché in ambito sanitario e farmaceutico[4].

In Italia, come nella maggior parte dei Paesi europei, a soffrire più significativamente della presenza di fenomeni illeciti, mancanza di trasparenza e conflitti di interessi è, indubbiamente, l'ambito del procurement pubblico. Nelle gare ad evidenza pubblica, difatti, il principio della partecipazione in regime di concorrenza e *par condicio* fra i candidati, è soltanto un presupposto teorico, smentito dall'ampia casistica riguardante gli affidamenti ed i relativi ricorsi giudiziari. Il

[1] Fra i più importanti, la Convenzione delle Nazioni Unite contro la corruzione, adottata dall'Assemblea generale il 31 ottobre 2003 e aperta alla firma a Merida dal 9 all'11 dicembre dello stesso anno, e la Convenzione dell'OCSE del 17 dicembre 1997.

[2] Nonostante il miglioramento del nostro Paese negli ultimi anni, l'indice di percezione della corruzione degli Italiani nei confronti dei Paesi partner dell'UE resta alto, in particolare per quanto riguarda gli appalti pubblici, che rappresentano il 74 per cento dei casi complessivi dei fenomeni corruttivi.

[3] Secondo le stime del RAND (Research And Development) in Italia ogni anno vengono persi, a causa della corruzione, 236,8 miliardi di euro di ricchezza, pari a circa il 13 per cento del prodotto interno lordo, ed a 3.903 euro per abitante.

[4] Ampia è la bibliografia in materia di corruzione in Italia. A puro titolo esemplificativo si cita: Cantone R., *Il sistema della prevenzione dalla corruzione*, Giappichelli, febbraio 2020; Brioschi C.A., *La corruzione. Una storia culturale*, Guanda, 2018; Davigo P.C., *Il sistema della corruzione*, Laterza, 2007; Davigo P.C., Mannozzi G., *La corruzione in Italia. Percezione sociale e controllo penale*, Laterza, 2017; Vannucci A., Della Porta D., *La corruzione come sistema. Meccanismi, dinamiche, attori*, Il Mulino, 2021; Stampanoni Bassi G., *La Corruzione, le corruzioni*, Wolters Kluwer, maggio 2022; Cerioni M., De Angelis M., Toschei S. (a cura di), *Anticorruzione nella sanità. Reazioni e Azioni*, Aracne Editrice, 2017.

più importante organo della giustizia amministrativa ha più volte ribadito l'importanza della valorizzazione di quei profili che tendono a salvaguardare l'immagine dell'Amministrazione Pubblica e ad evitare la determinazione di un'oggettiva confusione tra valutatore e concorrente, di per sé idonea ad appannare l'immagine di imparzialità e di buona amministrazione[5], al fine di scongiurare il verificarsi nelle gare pubbliche di fenomeni distorsivi della par condicio e di una sana concorrenza tra gli operatori economici[6].

Nonostante l'inerzia che per molti anni ha caratterizzato il legislatore italiano nel fronteggiare tale problematica e le difficoltà innegabili che lo stesso si è trovato ad affrontare, sia politiche che sociali, nell'ultimo decennio sono state emanate nuove regole che hanno permesso di colmare il gap legislativo nei confronti delle altre democrazie occidentali. Tuttavia le nuove norme anticorruzione e sul conflitto d'interessi, non sono da sole sufficienti a scalzare un fenomeno ormai divenuto endemico nella nostra società civile. Per ottenere risultati apprezzabili è necessario accompagnare la produzione normativa a strumenti che in concreto consentano l'individuazione, localizzazione e qualificazione del fenomeno, permettendo così di approntare una strategia punitiva e premiale, ma soprattutto preventiva. A tal uopo ci si è avvalsi sempre di più delle moderne tecnologie, valido alleato nella lotta ai fenomeni corruttivi, nonché all'individuazione dei conflitti di interessi anche soltanto potenziali[7]. I Paesi che maggiormente si sono avvalsi di tali strumenti hanno conseguito risultati sorprendentemente positivi nell'impegno di arginare la corruzione, conseguendo un crollo finanche del settanta per cento dei fenomeni corruttivi in generale e dell'ottanta per cento degli illeciti e dei conflitti di interessi negli appalti pubblici. Anche l'Italia negli ultimi anni ha iniziato ad utilizzare tecnologie innovative per il contrasto alla corruzione, avvalendosi di sistemi muniti di intelligenza artificiale[8]: big data, open data e tecnologie di predictive policing, ossia polizia predittiva. Tuttavia giurisprudenza e dottrina sollevano notevoli perplessità con riguardo alla violazione del diritto alla privacy, che l'analisi di

[5] Così come previsto dall'art. 97 comma 2 della Costituzione, secondo il quale "I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione".
[6] Consiglio di Stato, Sez. V, sent. n. 3415/2017.
[7] Cfr. Graffuri F., *Il conflitto di interessi nell'esercizio del potere amministrativo*, G. Giappichelli Editore, 2018, p. 26 ss.; D'Angelo G., *Conflitto di interessi ed esercizio della funzione amministrativa*, G. Giappichelli Editore, 2020, p. 51 ss.
[8] Le più recenti tecnologie munite di intelligenza artificiale si identificano, oggi, nel machine learning, cfr. Biancardo A., *Problematiche etico giuridiche relative all'utilizzo dell'intelligenza artificiale in ambito sanitario*, in *Jus Online*, vol. VII n. 3, giugno 2021, per cui l'i.a. "non segue un percorso lineare stabilito dal software e prevedibile secondo gli algoritmi da cui è composto, bensì segue una logica di autoistruzione, nella quale emerge l'abilità di assimilare dall'esperienza acquisita dall'interazione con gli ambienti esterni e dall'uomo stesso, per il raggiungimento di un obiettivo".

grandi quantità di dati può mettere a rischio. La storia recente, difatti, ci insegna che tecnologie innovative ed automazione vanno utilizzate con moderazione ed oculatezza, poiché racchiudono rischi e problematiche più o meno occulti, e possono provocare effetti collaterali non indifferenti. Ci si riferisce, nello specifico, al rischio riguardante alcuni princìpi costituzionalmente tutelati, quali l'eguaglianza ed il diritto a non essere discriminati, ma soprattutto la tutela dei dati personali ed il diritto alla privacy di ogni individuo[9]. Nonostante l'analisi di grandi quantità di dati abbia le potenzialità per conseguire risultati estremamente positivi contro corruzione e conflitto di interessi, con evidente vantaggio di tutti i cittadini, è necessario non ricadere nell'errore di precludere la tutela di alcuni diritti della persona. Non si vuole, con tale affermazione, sostenere la sussistenza di un'incompatibilità fra l'utilizzo dei big data e il diritto alla privacy, ma solo la necessità di utilizzare i dati in maniera corretta e previ costanti controlli da parte di autorità indipendenti.

La predisposizione e l'analisi delle banche dati necessarie per l'emersione del conflitto di interessi deve, peraltro, necessariamente essere combinata con la trasparenza dell'operato della P.A., specialmente in tema di trattamento dei dati personali. A livello sovranazionale il GDPR[10] rappresenta indubbiamente una corretta e completa regolamentazione sul rispetto della privacy. Esso deve, tuttavia, essere applicato senza deroghe da tutti i Paesi membri dell'UE, ossia anche in caso di specifiche emergenze e particolari necessità delle singole nazioni. La tendenza di affidarsi alla politica emergenziale, spesso applicata dai governi anche nelle moderne democrazie occidentali e in ambito UE[11], per eludere gli accordi sovranazionali di tutela dei diritti della persona, è un punto essenziale da evitare, poiché rischia di minare la credibilità internazionale di ogni Paese membro e della stessa Unione Europea.

Di fondamentale importanza è l'istituzione, in materia di privacy, di un organo indipendente operante a livello nazionale, un'autorità garante in grado di rilevare e sanzionare le violazioni

[9] Fra le opere più recenti sul diritto alla privacy si legga: Alongi A., Pompei F., *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Tab, 2021; Tosi E. (a cura di), *Privacy digitale*, Giuffrè Editore, 2019.

[10] General Data Protection Regulation, 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, approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e applicabile a decorrere dal 25 maggio 2018.

[11] Cfr. Longo M., Preite G., Bevilacqua E., Lorubbio V. (a cura di), *Politica dell'emergenza*, Tangram Edizioni Scientifiche, 2020, p. 22 ss.; Yuri Kazepov (a cura di) *La dimensione territoriale delle politiche sociali in Italia*, Carocci Editore 2009, p. 121 ss.

riguardanti il diritto alla tutela dei dati personali. Le autorità garanti nazionali sono, peraltro, coordinate e supervisionate da un comitato europeo, l'European Data Protection Board (EDPB), al fine di preordinare un'uniformità di trattamento per tutti i cittadini dell'Unione. Tale uniformità andrebbe estesa anche ai Paesi extraeuropei e di conseguenza a tutti i continenti, stante l'extraterritorialità e il carattere transfrontaliero del dato personale. Alla luce delle recenti novelle in materia di dati personali introdotte a livello europeo dal GDPR verranno approfondite, nella presente ricerca, le articolate problematiche giuridiche sottese all'utilizzo e alla gestione dei big data analytics, in particolare nelle pubbliche amministrazioni.

L'elaborato analizza la recente normativa, ma soprattutto le nuove tecnologie utilizzate nella lotta alla corruzione e nell'individuazione di aree sensibili al conflitto d'interessi, soffermandosi approfonditamente sui big data e sulle tecniche di predictive policing. Ci si distacca definitivamente, in tal modo, dalla tradizionale antitesi fra diritto ed innovazione tecnologica, per creare una sinergia fra discipline apparentemente così lontane, in cui l'informatica si pone quale strumento principale per la prevenzione ed individuazione delle fattispecie di reato. Quale area strategica di estrema rilevanza socio economica, ci si concentra in particolare sul conflitto di interessi nel procurement sanitario pubblico e sui conseguenti eventi corruttivi che possono scaturire da eventuali aporie e contraddizioni ad esso connesse. Uno dei settori maggiormente colpiti dai fenomeni corruttivi è, difatti, indubbiamente quello sanitario. Ciò non solo perché la sanità pubblica necessita di un'immensa ricchezza, essendo ad essa, soltanto nel nostro Paese, destinati oltre cento miliardi di euro ogni anno[12], ma anche per le frequenti situazioni di conflitto di interessi che si vengono a creare nel rapporto fra dirigente medico ed azienda fornitrice nel procurement sanitario. Altro elemento da considerare riguardo il conflitto di interessi in sanità è, peraltro, il complesso rapporto fra sanità privata e pubblica ed il duplice ruolo di alcune figure legate alla sanità, sia in ambito pubblico che privato.

La presente ricerca è, necessariamente, multidisciplinare. Pur ponendo al centro dell'analisi le problematiche giuridiche, lambirà campi quali l'innovation system, le information technologies, il public management. Al termine dell'analisi delle attuali contromisure per il contrasto al conflitto d'interessi, saranno prese in considerazione le prospettive future dell'utilizzo della tecnologia in tale ambito, i possibili sviluppi delle scienze tecnologiche stesse, i rischi connessi alla tutela dei

[12] Dato ISTAT in Italia: nel 2021 il Fondo Sanitario è di 122 miliardi di euro, cresciuto nel 2022 a 124 miliardi di euro.

diritti umani e dei dati personali. Verrà, poi, compiuta un'analisi comparatistica con altre realtà, in particolare quella spagnola, utile per poter condividere le soluzioni ed apprendere anche da esperienze differenti, facendo tesoro di un costante confronto per un reciproco affinamento delle tecniche e delle normative. Allo scopo di mantenere uno stretto contatto con la realtà sociale e giuridica saranno, altresì, esaminati alcuni casi concreti, al fine di far emergere fattori evolutivi, nonché problematicità e vulnerabilità, con specifico riferimento all'utilizzo di tecnologie per il contrasto alla corruzione nel procurement pubblico in ambito sanitario.

Nello specifico, l'elaborato ha inizio con l'analisi delle recenti norme per il contrasto alla corruzione pubblica e privata. Si porrà, in primo luogo, l'accento sull'evoluzione normativa in materia di corruzione e sul connubio che unisce indissolubilmente la stessa corruzione al conflitto d'interessi. Negli ultimi anni sono state molteplici le norme aventi il preciso fine di frenare l'alto tasso di corruzione presente nel nostro Paese. L'attuale orientamento vede prevalere un'inclinazione alla prevenzione, nei confronti della repressione degli atti antigiuridici compiuti nei confronti dell'amministrazione, che si concretizza col tentativo di eliminare quelle situazioni potenziali che possano generare eventi criminosi. Le cause che originano i fenomeni corruttivi sono molteplici, ma è innegabile che la corruzione sia essenzialmente alimentata da una prorompente e costante presenza di conflitti di interessi, in ogni settore. Ciò è dovuto principalmente all'assenza una normativa organica che regoli il conflitto di interessi ed alla difficoltà di percezione dello stesso. Con riguardo al conflitto di interessi verranno attentamente esaminate le differenze fra le varie tipologie, in particolare fra conflitto di interessi attuale, potenziale e apparente. Rilevanti, nel tentativo di arginare la corruzione sono, indubbiamente, le novelle introdotte dalla legge n. 190 del 2012, dal d.lgs. n. 33 del 2013, dal d.lgs. n. 97 del 2016 ossia il c.d. Freedom of Information Act, e dalla legge n. 3 del 2019, la c.d. Spazzacorrotti. Le recenti norme hanno, indiscutibilmente, sortito effetti positivi ponendo un freno alla piaga della corruzione, soprattutto in ambito pubblico, tuttavia i risultati non sono quelli sperati, a dimostrazione che quanto si è fatto non sia assolutamente adeguato alla portata e alla capillare diffusione del fenomeno, nonché alla ritrosia dell'opinione pubblica nel percepirla quale elemento di disvalore sociale. Le norme da sole non sono, difatti, sufficienti al fine di scalzare un fenomeno ormai divenuto endemico, quasi accettato con indifferenza e rassegnazione, nella nostra società civile. Oltre a norme più incisive, precise e coraggiose soprattutto nell'ambito della prevenzione e del conflitto di interessi, per sortire effetti più rilevanti si rivela necessario l'ausilio di tecniche moderne e di personale estremamente preparato. Dopo aver analizzato il binomio

corruzione-conflitto di interessi, che ha creato grandi problemi nelle società moderne ed in particolare nel nostro Paese, il lavoro si focalizzerà, pertanto, sulle moderne tecnologie informatiche utilizzate per il contrasto di tali fenomeni.

Per ottenere risultati più incisivi, specialmente nella prevenzione della corruzione, ci si avvale sempre di più delle nuove tecnologie, indispensabili in particolare nell'individuazione di aree sensibili al conflitto d'interessi. Pertanto, la ricerca si concentra sulle moderne tecnologie informatiche utilizzate per l'identificazione di aree e soggetti ove l'analisi dei dati prospetta situazioni di conflitto di interessi, ed in particolare sui big data analytics e le tecniche di polizia predittiva. L'ausilio delle suindicate tecnologie può incidere in maniera ancor più profonda, non solo nell'individuazione di reati già commessi, ma nella prevenzione degli stessi, con controlli più severi, al fine di evitare *ab origine* quei conflitti di interessi che generalmente sono alla base di fenomeni corruttivi. I risultati ottenuti con l'utilizzo delle tecnologie a scopo preventivo, nei Paesi che le usano già da svariati anni, sono incoraggianti poiché esse hanno un notevole potere dissuasivo stanti i maggiori controlli mirati in alcune specifiche aree. L'utilizzo massivo dei dati al fine di ottenere tali risultati può, tuttavia, facilmente deviare nell'impiego distorto, ovvero indiscriminato degli stessi, con conseguente lesione di diritti costituzionalmente tutelati, con pericolo di discriminazioni e violazioni del diritto alla privacy. Pertanto, pur senza mai demonizzare l'uso delle tecnologie innovative quale valido strumento al fine di arginare piaghe che nel nostro Paese sono ormai radicate ed evitando visioni distopiche, si cercheranno di individuare possibili alternative per evitare che tale utilizzo possa confliggere con la tutela dei diritti dell'uomo. È, certamente, necessario aprire alle innovazioni della scienza che possano sconfiggere le devianze delle società, ma non dimenticando in alcun caso i diritti dell'uomo sanciti nelle carte dei diritti nazionali, quali la Costituzione repubblicana, e sovranazionali, come la Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali. L'obiettivo è quello di creare una situazione di equilibrio fra diritti confliggenti ed esigenze socio politiche, dando la precedenza alle tutele di rango superiore, costituzionale e comunitario, ma senza ricadere nell'errore di un immobilismo giuridico, dovuto all'eccesso di tutela.

Il lavoro si focalizzerà, poi, sulle aree a rischio nel procurement sanitario, ambito fra i più colpiti dal conflitto d'interessi e dai fenomeni corruttivi. Tale settore è di primario rilievo non solo per l'entità economica dei danni provocati da attività illecite, ma soprattutto per la preminenza del bene tutelato che ne riceve nocumento, ossia la salute delle persone. È proprio nel settore della

sanità che il bene giuridico costituito dal dato sensibile deve essere maggiormente tutelato, stante la tipologia intima e strettamente personale dell'informazione che viene raccolta, manipolata, analizzata. Il rischio che l'incrocio di informazioni raccolte possa dare risultati distorti è notevole, ma ancora più pericolosa può risultare una fuoriuscita di informazioni personali, nonché un utilizzo illecito o finalizzato all'osservazione e monitoraggio della vita privata degli individui. Le tematiche del procurement in sanità con particolare riguardo alle gare ad evidenza pubblica e della gestione dei big data sono state trattate approfonditamente, tramite uno studio sul sistema sanitario in Italia e negli altri contesti internazionali, con particolare attenzione agli aspetti legati al conflitto di interessi e tutela della privacy.

Sarà dato, poi, spazio ad un'analisi comparatistica di normative e tecnologie dei Paesi che hanno ottenuto i risultati più rilevanti. In particolare saranno raffrontate le normative italiana e spagnola riguardanti il conflitto d'interessi e le rispettive tutele in materia di dati personali. A tale riguardo, particolare rilevanza ai fini della ricerca ha avuto la collaborazione dello scrivente con l'Universitat de Barcelona[13], con specifico riferimento alla normativa spagnola ed europea sulla tutela della privacy. Si cercherà, così, di tracciare un parallelo fra il sistema spagnolo e quello italiano nell'utilizzo nelle tecnologie per l'individuazione del conflitto d'interessi, nel rispetto della tutela dei dati personali. Nell'ambito dell'area tematica "Agenda Digitale, Smart Communities, Sistemi di mobilità intelligente", tra quelle individuate dalla Strategia Nazionale di Specializzazione Intelligente nella Pubblica Amministrazione, l'attività di ricerca all'estero e in azienda ha permesso di individuare, da un punto di osservazione prevalentemente giuridico, soluzioni atte a rendere le nuove tecnologie conformi al rispetto delle norme nazionali e sovranazionali in un contesto in continua espansione ed in rapida evoluzione socio culturale. In particolare, il lavoro si è focalizzato sulla verifica di compatibilità di algoritmi automatizzati utilizzati per i controlli incrociati effettuati al fine di rilevare la sussistenza di conflitti d'interesse, con il sistema normativo europeo di tutela della privacy.

L'elaborato cercherà, così, di fornire credibili soluzioni giuridiche che costituiscano un compromesso fra l'utilizzo delle moderne tecnologie informatiche utili per porre un freno ai fenomeni corruttivi e la tutela della privacy ed in generale dei diritti costituzionalmente tutelati, che potrebbero subire nocumento dall'uso massivo di tali sistemi. L'attività di ricerca consentirà

[13] Università di Barcellona, Gruppo di ricerca in Diritto privato, del consumo e nuove tecnologie, coordinatrice Prof. M. Gramunt Fombuena.

di evidenziare le criticità dell'attuale quadro normativo in materia di dati personali, con l'individuazione di soluzioni giuridiche e applicative. Nello specifico si fornirà, nell'ambito del procurement sanitario, un modello di legislazione che, pur prevedendo l'utilizzo delle moderne tecnologie e l'analisi massiva dei dati, tuteli sufficientemente la privacy, rendendo ancor più preziose le banche dati per l'emersione del conflitto di interessi. Sono proprio le banche dati delle Pubbliche Amministrazioni un bene comune prezioso ed irrinunciabile, in sintonia con una società sempre più "data driven", ma solo a patto di riuscire a preservare la trasparenza ed una generalizzata consapevole condivisione[14].

Si giunge, al termine di tale percorso, alla consapevolezza che l'apporto delle recenti tecnologie ha in sé parte della soluzione, ossia la formazione di *smart communities*, persone e aziende che condividono le stesse necessità[15], piattaforme create su moderne infrastrutture tecnologiche, con algoritmi che tengano conto delle necessità dell'utenza, e basate sulla tecnologia blockchain, che se da un lato consente una partecipazione e controllo da parte di ogni individuo nell'area della pubblica amministrazione, dall'altro riesce in maniera convincente a tutelare la privacy di tutti i soggetti privati che vi prendono parte. Il blockchain ha, difatti, le potenzialità per gestire dati e informazioni in maniera trasparente, senza necessità di intermediari o organi di controllo e verifica. L'utilizzo di una piattaforma con le predette caratteristiche, che possa regolare e rendere pubblica ogni singola fase del procurement in sanità, può essere una valida soluzione. L'espansione di tale sistema sia nel pubblico che nel privato, connessa all'utilizzo di algoritmi che 'depurino' le basi di dati analizzate nei controlli incrociati, da tutte quelle informazioni sensibili che possano ledere il diritto alla privacy costituisce, ad avviso dello scrivente, la corretta modalità di utilizzo dei dati per conseguire l'emersione del conflitto di interessi, nel rispetto delle norme nazionali e sovranazionali che tutelano i dati personali.

[14] Cfr. Fabiano N., *GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity*, go Ware Editore, maggio 2019.
[15] Sull'argomento, Manfredi F., *Smart community. Comunità sostenibili e resilienti*, Cacucci Editore, 2015.

Capitolo 1. Il contrasto alla corruzione e il conflitto d'interessi

1.1. Conflitto di interessi e corruzione

1.1.1. Il problema della corruzione in Italia

Il problema della corruzione, per decenni sottovalutato nel nostro Paese è, da sempre, di massima rilevanza se si considerano le conseguenze in termini di costi in risorse economiche ed umane, crollo della qualità e quantità dei servizi pubblici, effetti distorsivi della vita sociale e democratica del territorio. La stretta correlazione fra i livelli di corruzione e lo sviluppo socio economico, con particolare riguardo alla crescita del prodotto interno lordo e l'interesse degli investitori, nonché le normative comunitarie sempre più stringenti, hanno richiesto un deciso intervento del legislatore nazionale nell'ultimo decennio. L'intervento non si è limitato, come nel passato, al mero inasprimento delle pene per gli illeciti corruttivi, ma si è concentrato prevalentemente sulla prevenzione della corruzione, sulla trasparenza e sull'integrità dei funzionari pubblici[16].

Per corruzione si intende, in linea generale, la violazione di un obbligo per ottenere un beneficio personale, mentre nel settore pubblico consiste nell'abuso "da parte di un soggetto del potere a lui affidato al fine di ottenerne vantaggi privati e illeciti"[17]. Sotto il profilo penalistico, nei reati contro la Pubblica Amministrazione occupano un posto di rilievo i delitti corruttivi, previsti e puniti agli articoli 318 c.p. e ss., ed in particolare la corruzione per l'esercizio della funzione, che si consuma allorché pubblico funzionario e privato si accordano attraverso un *pactum sceleris*, affinché il primo riceva da quest'ultimo un compenso indebito, per l'esercizio delle proprie funzioni (ex art. 318 c.p., c.d. corruzione impropria[18]). Si ha, invece, la fattispecie di corruzione per un atto contrario ai doveri di ufficio, nell'ipotesi in cui il privato corrisponda al funzionario un

[16] Cfr. Monteduro F., Brunelli S., Buratti A., *La corruzione. Definizione, misurazione e impatti economici*, Formez PA, Gangemi Editore, Roma, marzo 2013, p.8. Per gli autori "sono quattro gli assi portanti su cui intervenire: a) l'adozione all'interno delle amministrazioni di piani di prevenzione della corruzione, nei quali si dovranno individuare i settori a maggior rischio e le soluzioni organizzative volte ad abbattere o ridurre quel rischio; b) l'adozione di misure per l'integrità dei funzionari pubblici; c) l'innalzamento dei livelli di trasparenza delle amministrazioni; d) la tutela del whisteblowing".

[17] Pope J., *Confronting corruption: The elements of a national integrity system, Transparency International Source Book*, TI, 2000, p. 2 "corruption involves behaviour on the part of officials in the public sector, whether politicians or civil servants, in which they improperly and unlawfully enrich themselves, or those close to them, by the misuse of the power entrusted to them".

[18] Per l'art. 318 c.p. (Corruzione per l'esercizio della funzione) "il pubblico ufficiale, che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa, è punito con la reclusione da tre a otto anni".

compenso, non per il compimento di un atto che attiene al pubblico ufficio cui esso è preposto, bensì per l'omissione, il ritardo o un atto contrario ai doveri d'ufficio (art. 319 c.p., c.d. corruzione propria[19]). Il disvalore della condotta di corruzione impropria è minore nei confronti di quella propria, poiché anche per ciò che riguarda i beni giuridicamente e costituzionalmente tutelati di imparzialità e buon andamento della Pubblica Amministrazione non vi sono atti che ledano così gravemente gli interessi della stessa, come avviene invece nella corruzione propria, con ritardi o omissione di atti dovuti, ovvero con il compimento di atti contrari ai doveri d'ufficio. È bene, tuttavia, precisare che la scelta operata dalle più importanti convenzioni internazionali[20], è orientata verso l'allontanamento dal reato di corruzione in sé considerato, preferendo specifici reati espressione di atti corruttivi, quali peculato e malversazione, traffico di influenze, abuso di potere e d'ufficio, illecito arricchimento, riciclaggio. È punito in maniera ancora maggiore il pubblico ufficiale o incaricato di un pubblico servizio che si macchia del reato di concussione[21], che si verifica quando questi costringa o induca taluno a dargli o promettergli denaro o altra utilità, abusando dei suoi poteri. Il maggior disvalore, nel caso della concussione prevista ex art. 317 c.p., è rappresentato dall'abuso dei poteri, fatto valere dal funzionario pubblico nei confronti del privato, nella forma della coazione psichica, tale da incidere in maniera sostanziale sui processi decisionali di quest'ultimo[22].

La definizione di corruzione non si può, tuttavia, limitare rigidamente alla fattispecie penale, in quanto troppo ristretta nel suo contenuto[23]. La corruzione, difatti, non si concretizza sempre nella commissione di un atto antigiuridico. Una delle definizioni più precise ed appropriate è, indubbiamente, quella del Comitato di studio sulla prevenzione della corruzione[24], per il quale la

[19] Per l'art. 319 c.p. (Corruzione per un atto contrario ai doveri d'ufficio) "Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni".

[20] In primis la Convenzione ONU contro la corruzione del 31 ottobre 2003, la c.d. "Convenzione di Merida", ratificata in Italia con la legge n. 116 del 3 agosto 2009, e la Convenzione penale contro la corruzione del Consiglio d'Europa del 27 gennaio 1999, c.d. "Convenzione di Strasburgo", ratificata dall'Italia con la legge n. 110 del 28 giugno 2012.

[21] L'articolo 317 c.p. prevede per il reato di concussione una pena compresa fra i sei e i dodici anni. Esso dispone che "Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità, è punito con la reclusione da sei a dodici anni".

[22] Secondo la Suprema Corte, Cass. n. 38658 del 2019 "Ai fini della configurabilità del tentativo di concussione, è necessaria l'oggettiva efficacia intimidatoria della condotta, mentre è indifferente il conseguimento del risultato concreto di porre la vittima in stato di soggezione".

[23] Cfr. Borsari R., *La corruzione pubblica. Ragioni per un cambiamento della prospettiva penale*, G. Giappichelli Editore p. 18 ss.

[24] Il Comitato di studio sulla prevenzione della corruzione, ovvero Comitato dei tre saggi, istituito il 27 settembre 1996 con provvedimento del Presidente della Camera dei deputati, composto da Sabino Cassese, Luigi Arcidiacono

corruzione è "una forma di accordo fra una minoranza allo scopo di appropriarsi di beni che spettano alla maggioranza della popolazione, considerata questa, o come insieme di consumatori, o come insieme di cittadini elettori. Poiché i danni in termini di consumo, o in termini di domanda politica, si ripartiscono su di un'ampia popolazione (che, inoltre, è poco ascoltata), essi tendono a venir giudicati irrilevanti da coloro che perpetrano atti corrotti"[25]. Da tale definizione si intuiscono le più gravi conseguenze della corruzione, quali lievitazione dei costi di beni e servizi, minor qualità dei servizi pubblici, cedimento del PIL, sfiducia nei confronti dell'amministrazione, normalizzazione del disvalore della corruzione, senza contare sul piano internazionale la minor competitività dell'economia, l'aumento del debito pubblico e la perdita di prestigio e credibilità della nazione[26].

Parlare di corruzione esclusivamente come una fattispecie penale è, pertanto, altamente riduttivo, poiché essa è soprattutto un fenomeno culturale e sociale. Per fare un'ampia valutazione riguardo il rischio di esposizione a fenomeni corruttivi non basta, difatti, considerare quegli ambiti strettamente legati alla sfera di rilevanza penale, ma è necessario valutare anche altri fenomeni che fungano da fattori di dissuasione e disincentivo, quali il contrasto al conflitto di interessi, le tematiche sulle lobby, i codici etici e di comportamento, gli incentivi alla trasparenza, la promozione della cultura della legalità e la partecipazione della società civile alla vita politica del Paese. Di assoluto rilievo è la sensibilità dell'opinione pubblica nel discernere i comportamenti corruttivi, che possono essere considerati moralmente riprovevoli, ovvero possono essere accettati con complicità, indifferenza, tolleranza o rassegnazione. La reazione della collettività può condizionare la possibilità di contrastare il fenomeno, in maniera ancor più incisiva della reazione dello Stato e costituire un deterrente più efficace anche della criminalizzazione di livello giuridico. Il fenomeno va, difatti, compreso nella sua realtà sociologica prima ancora che giuridica, poiché solo la visione di ogni atto corruttivo come disvalore sociale potrà permettere l'identificazione di efficaci politiche di contrasto, sia sul piano della repressione

ed Alessandro Pizzorno, aveva il compito di "elaborazione, nell'ambito dei princìpi fondamentali dell'ordinamento amministrativo italiano, di ipotesi di intervento legislativo per prevenire fenomeni di corruzione, tenendo conto delle caratteristiche del sistema delle imprese e delle principali esperienze straniere".

[25] CSPC, Comitato di studio sulla prevenzione della corruzione, *Rapporto al Presidente della Camera dei deputati*, Roma, 1996, p. 3.

[26] Op. cit. Pope J., p. 3, "corruption raises the cost of goods and services; it increases the debt of a country (and carries with it recurring debt-servicing costs in the future); it leads to lowering of standards, as sub-standard goods are provided and inappropriate or unnecessary technology is acquired".

che della prevenzione e del controllo[27]. La radicalizzazione e persistenza del fenomeno nel tessuto sociale ha richiesto innumerevoli interventi di contrasto, a partire dall'approvazione della legge Severino del 2012 fino alla c.d. Spazzacorrotti, con inasprimento delle pene e la possibilità di estendere le operazioni sotto copertura anche per i delitti contro la pubblica amministrazione. Si ribadisce, tuttavia, che non ci si può limitare all'aspetto patologico del problema puntando sulla sola repressione, poiché svolge un ruolo fondamentale l'aspetto della prevenzione compresa in una logica di sistema. Anche a parere dell'ANAC è necessario combinare strumenti repressivi e preventivi, e nell'ambito di questi ultimi intensificare le azioni per arginare il conflitto di interessi, riducendo a monte i fattori di rischio, ad esempio mediante la rotazione periodica del personale, o con il c.d. revolving doors[28]. Negli ultimi anni si sono diffuse in ambito penale le regole premiali per coloro che restituiscono quanto sottratto, con la previsione di sconti di pena consistenti. Ciò potrebbe, tuttavia, costituire un'arma a doppio taglio, poiché se da un lato incentiva l'imputato per reati di corruzione alla riparazione, rischia di svilire la portata deterrente delle sanzioni, fornendo altresì una sorta di giustificazione morale agli autori degli illeciti.

I settori ove la corruzione si insinua maggiormente sono le aree di intersezione fra pubblico e privato, ossia gli enti pubblici più prossimi al territorio, con una diffusione capillare negli appalti e nelle nomine di cariche pubbliche e private. È proprio il procurement pubblico dei settori edile, medico e farmaceutico a soffrire maggiormente dell'infiltrazione dei fenomeni corruttivi, poiché altamente permeabili al conflitto di interessi e al controllo politico e di potere. La multiformità del fenomeno fa sì che anche le cause siano molteplici, e non sempre di immediata individuazione. La tipologia del fatto corruttivo può variare sensibilmente, creando ampie difficoltà, ove si voglia individuare origine e localizzazione del problema, nella sussunzione a situazioni tipo. Si parla di grande e piccola corruzione a seconda che vengano coinvolti i vertici degli apparati amministrativi, ovvero piccoli funzionari. Tuttavia la piccola corruzione, pur non minando alla base la credibilità delle istituzioni del Paese, è altrettanto allarmante poiché la sua capillarità e diffusività incide pesantemente sui servizi della Pubblica Amministrazione, sulla loro fruizione e qualità. La corruzione può, poi, essere politica o burocratica, a seconda che si annidi nel sistema politico del Paese, oppure nel sostrato della Pubblica Amministrazione. La distinzione non è, tuttavia, così netta come potrebbe apparire, poiché le scelte politiche, nella moderna organizzazione dello

[27] Cfr. Ufficio dell'Alto Commissario Anticorruzione, *Il fenomeno della corruzione in Italia*, 2007, studi sulla "mappa del fenomeno" in Italia, p. 7 ss.
[28] Di questo avviso è il Rapporto ANAC sulla corruzione 2016-2019.

Stato, vengono quasi a fondersi con l'apparato burocratico. Nel settore pubblico, requisito dell'evento corruttivo è, difatti, il potere discrezionale della Pubblica Amministrazione. Il pubblico amministratore può, pertanto, essere corrotto nelle scelte discrezionali da soggetti che possano ottenerne dei vantaggi, in contropartita di un interesse personale, che prevalga sull'interesse pubblico concreto.

Le più diffuse cause di amplificazione dei fenomeni corruttivi sono l'inefficienza amministrativa, che determina la creazione di corsie preferenziali, la confusione di ruoli fra politica e personale burocratico, che rende più appetibile la collusione e non il reciproco controllo, ma anche la scarsità di vigilanza e la sfiducia dei cittadini nella tutela dei loro diritti, con conseguente ricerca degli stessi di canali privilegiati. Un altro importante problema, cui si è tentato di porre rimedio solo negli ultimi anni, è la complessità normativa e l'eccessiva multiformità delle fonti, con conseguente sovrapposizione e contrasto fra norme, nonché incertezza ed eccessiva discrezionalità sulla disciplina da applicare. Secondo il Comitato di studio sulla prevenzione della corruzione "Il risultato è uno stato di confusione, in cui gli amministratori possono scegliere quali norme applicare, possono interpretarle in modo da favorire l'una o l'altra parte, possono aggirare i vincoli imposti dalla legge[29]".

Una strategia efficace di contrasto alla corruzione richiede la conoscenza approfondita del fenomeno, delle cause, dell'analisi dei comportamenti devianti, delle mappe delle aree maggiormente esposte e dell'evoluzione storica dei fattori di rischio individuati. La conoscenza del fenomeno è strumentale sia riguardo l'attività repressiva delle tecniche di indagine, che preventiva. Oltre alla repressione delle attività illecite e dei reati corruttivi si è, giustamente, gradatamente a partire dal terzo millennio, scelto di percorrere preferenzialmente la strada della prevenzione[30]. Già nel 1997 il Comitato di studio sulla prevenzione della corruzione[31] affermava che l'applicazione del solo strumento repressivo potesse avere conseguenze negative non intenzionali, quali l'accrescimento del prezzo della corruzione, in considerazione dei maggiori rischi corsi dagli attori. La preferenza orientata alla prevenzione è stata dettata, principalmente, dal fallimento del tradizionale approccio unicamente repressivo che aveva connotato fino ad allora il contrasto alla corruzione. La repressione aveva ampiamente mostrato i propri limiti con

[29] CSPC, Comitato di studio sulla prevenzione della corruzione, *Rapporto al Presidente della Camera dei deputati*, Roma, 1996, p. 42.
[30] Tortora A., *La prevenzione della corruzione. Un sistema in continua evoluzione,* Giappichelli Editore, 2018, p. 52 ss.
[31] Id., p. 3.

la deflagrazione di una delle vicende giudiziarie fra le più eclatanti del nostro Paese, che aveva come protagonista la corruzione nel settore pubblico e coinvolgeva politici ed imprenditori italiani di spicco, definita "Mani Pulite", iniziata nel 1992. Anni dopo "Tangentopoli"[32], si è difatti constatato l'effetto temporaneo e parziale della mera repressione e, ben più grave, un'attività di supplenza della magistratura nei confronti della politica, che mal si accompagna alle istituzioni ed ai sistemi democratici occidentali. Ma non è tutto: la classe politica che ha sostituito quella antecedente Mani Pulite ha, per osmosi occupato i posti dei politici uscenti, mantenendo gli stessi livelli di corruzione, di talché i protagonisti della prima ma anche quelli della seconda repubblica sono, nella visione comune, stati identificati col malaffare. In tale quadro politico e sociale le riforme anti corruzione degli anni immediatamente successivi alla caduta della prima repubblica sono state soltanto di facciata, senza alcun intento decisivo, innovatore o risolutore. La nuova classe politica si è presto adeguata continuando a perseguire i propri interessi, e nonostante l'ostentazione della propria ostilità alla corruzione al fine di ottenere consensi dai cittadini sensibili alla questione morale, non ha affatto inteso combatterla realmente. Ma, a ben vedere, anche gli avversari politici di soggetti coinvolti in vicende di corruzione hanno preferito evitare di contrastarla, potendola così utilizzare quale argomento per produrre consensi o arma di ricatto contro gli avversari, ovvero servirsene come mezzo per accedere a benefici non divisibili, e ad utilità personali di interi gruppi politici e sociali[33]. L'ampiezza della diffusione del fenomeno e la gravità delle sue conseguenze richiedono interventi di riforma efficaci e non solo di facciata, altrimenti la corruzione continuerà a diffondersi in ogni maglia del tessuto sociale, fino ad essere percepita da tutti i cittadini come parte del sistema, accettata, e di fatto legalizzata.

Un aspetto da conoscere approfonditamente per prevenire e contrastare la corruzione riguarda i fattori da cui ha origine il fenomeno. In primis è da citare l'elemento di natura sociologica, ossia i valori culturali, lo spirito civico, il senso di responsabilità, di unità nazionale ed il percepimento di disvalore sociale dell'illecito degli amministratori pubblici e privati, e più in generale di ogni cittadino[34]. La spiegazione del fenomeno corruttivo non può, tuttavia, basarsi soltanto sui valori

[32] Sciarrone R., *Politica e corruzione. Partiti e reti di affari da Tangentopoli a oggi*, Donzelli Editore, 2017.
[33] In tal senso CSPC, *Rapporto al Presidente della Camera dei deputati*, Roma, 1996, p.5, secondo cui "in presenza di corruzione, anche i politici non corrotti sono portati a non denunciare la corruzione di cui vengono a conoscenza, e ad usare, invece, le loro informazioni a riguardo per ottenere vantaggi 'politici' dai loro colleghi di altri partiti".
[34] Di questo avviso Pizzorno A., *La corruzione nel sistema politico*, secondo cui "Il costo morale sarà tanto più basso quanto più labili appaiono ormai, agli occhi di un determinato individuo, i contorni delle cerchie di riconoscimento morale che gli avevano fornito criteri di valutazione morale positiva dell'osservanza della legge", *Lo scambio occulto*, in D. della Porta, Bologna, il Mulino, 1992, p. 46.

culturali individuali in quanto l'analisi interpretativa si connoterebbe di staticità ed autoreferenzialità[35]. Acquisisce, pertanto, rilevanza l'elemento di natura economica, secondo una precisa analisi costi/benefici attesi dai protagonisti di un evento corruttivo, condizionato dai deterrenti percepiti dagli stessi, quali la severità della sanzione e la probabilità di non essere puniti. L'altro elemento è di natura collettiva e riguarda principalmente l'ambito in cui si agisce: quanto più la corruzione è diffusa in un ambiente, minore è il disvalore che le si attribuisce. Ciò fa sì che negli ambienti ad alto tasso di corruzione, sarà sempre più probabile un incremento della stessa, in una logica di autogiustificazione e normalizzazione delle condotte devianti. Si crea, così, una sorta di ecosistema, nel quale l'equilibrio è fondato sulla diversificazione e diffusione soggettiva dell'illiceità e del malaffare. L'azione contemporanea e costante sui predetti elementi può certamente indurre i soggetti a comportamenti differenti e nel medio termine ridurre il livello di corruzione. I rimedi dovrebbero concentrarsi, pertanto, sul rinvigorire il senso soggettivo di appartenenza ad un'istituzione o una comunità, sullo sforzo di modificare il rapporto costi benefici delle attività corruttive, con minori profitti, pene più severe e maggiori controlli. Riuscendo a porre un carattere di discontinuità alla prassi corruttiva per ciò che riguarda l'elemento sociologico e quello economico, anche la percezione di disvalore dell'illecito nella comunità dovrebbe aumentare, con conseguente diminuzione della corruzione.

Oltre alla imprescindibile, approfondita conoscenza della corruzione e delle sue cause per poter orientare l'impianto normativo attuale e valutarne l'adeguatezza, una corretta analisi del fenomeno richiede un continuo aggiornamento, al fine di poter individuare e contrastare il diffondersi delle emergenti forme corruttive[36], dovute all'evoluzione dei comportamenti e ai cambiamenti del tessuto sociale nel tempo. Riconosciuta la centralità della conoscenza della corruzione e dell'aggiornamento costante, primaria importanza per il suo contrasto riveste la predisposizione di una mappa del fenomeno che ne delinei i confini, la rilevanza economica, le aree di maggior rischio. Per un'efficace strategia del contrasto è necessario analizzarne l'estensione a seconda della natura del fenomeno, e rapportarla ai *vulnera* delle amministrazioni e alle aree delle istituzioni più permeabili ad infiltrazioni corruttive. La complessità del fenomeno corruttivo e delle problematiche connesse al suo contrasto, sia in termini repressivi che

[35] Secondo Heywood A., *Politics*, 1995, p. 36, le spiegazioni basate solo sui valori culturali "sono incapaci di interpretare i cambiamenti delle abitudini politiche o dei modelli di comportamento".
[36] Ufficio dell'Alto Commissario Anticorruzione, *Il fenomeno della corruzione in Italia*, 2007, studi sulla "mappa del fenomeno" in Italia, p. 3 e ss.

preventivi, è data dalla sua multiformità e dalla trasversalità dei soggetti coinvolti. Tale complessità è percepibile in particolare nel momento prodromico al tentativo di risoluzione del problema, ossia l'analisi dei dati statistici, che risulta, pertanto, un momento centrale nel contrasto alla corruzione. I dati da analizzare vanno raccolti nel breve e lungo periodo, in maniera non occasionale ma continua e sistematica, per poter apprezzare l'efficacia delle azioni di contrasto e l'andamento dei progressi rispetto al piano anti corruzione. Solo tramite piani strategici pluriennali è possibile una stima delle tendenze dei fenomeni ed una valutazione circa la validità delle azioni intraprese, ovvero la necessità di semplici correttivi o riallineamenti, o al contrario un cambio di rotta. Importante è l'individuazione degli indicatori, che non devono essere tendenziosi, propagandistici, ottimistici, falsati o autoreferenziali, ma realistici, adeguati e completi. Solo in tal modo può essere creata una solida base per indirizzare le strategie anti corruzione, e può essere stimata l'efficacia reale delle azioni di contrasto intraprese. La fase di raccolta dei dati del patrimonio informativo dell'amministrazione pubblica è, pertanto, un elemento cruciale, in quanto punto di riferimento iniziale per una concreta azione strategica. A tal fine le informazioni devono interessare: l'identificazione delle istituzioni e dei settori maggiormente vulnerabili alla corruzione; le specifiche tipologie di corruzione, cause e relative concause; la determinazione dei costi diretti ed indiretti del fenomeno. Riguardo il monitoraggio è necessario un adeguamento agli standard internazionali più autorevoli, forniti dall'OCSE[37]. Più difficile è, invece, l'individuazione dei metodi di acquisizione dei dati, poiché nessuno di essi riceve unanime riconoscimento dagli esperti.

Nonostante sia evidente la centralità dei dati statistici e della loro analisi, bisogna tuttavia considerare che essi costituiscono un indicatore limitato, se non deviante, riguardo l'effettiva situazione del Paese, in considerazione della difficile emersione del fenomeno, raramente denunciato o giudizialmente accertato. È, pertanto, doveroso tenere sempre in considerazione la difficoltà nel circoscrivere la reale portata del fenomeno, poiché gli alti livelli di corruzione sommersa non possono essere rilevati in quanto di complessa identificazione, alterando così l'obiettività ed il realismo dei dati. Soltanto partendo da dati obiettivi aderenti alla realtà dei fatti e confrontando gli stessi a livello internazionale si può costituire un valido indice di valutazione, che fornisca elementi di apprezzamento della normativa vigente di ogni singolo Paese. Il solo dato

[37] OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico): Report annuale sulla corruzione internazionale.

giudiziario non può certamente essere esaustivo, ma si limita a fornire indicazioni circa le fattispecie penali più comuni, l'adeguatezza della normativa nella sua parte repressiva e l'efficacia di strumenti investigativi. Tuttavia, stante il carattere ontologicamente sommerso della corruzione, il dato giudiziario isolato potrebbe addirittura mostrarsi fuorviante, in quanto condizionato dall'efficienza degli organi e degli strumenti di contrasto[38]. Difatti una flessione dei dati relativi ai reati di corruzione, è sensibilmente condizionata dalla minore capacità o volontà degli organi preposti alla loro individuazione e contrasto, ovvero dalla scarsa volontà di denunciare eventi corruttivi ove il fenomeno sia così diffuso da non essere più percepito quale disvalore sociale. Non ci si può, pertanto limitare all'emersione della fattispecie di reato ed identificarla col dato del fenomeno corruttivo, ma è necessario quanto meno incrociarlo con altre informazioni, quali analisi di settore, sondaggi focalizzati su specifiche fasce di popolazione, rilevamenti indiretti, come quelli sulla qualità della vita e sulla percezione della legalità.

Altri aspetti essenziali per la prevenzione ed il contenimento della corruzione sono la trasparenza delle procedure e il controllo nella contrattualistica, la semplificazione dei procedimenti amministrativi con conseguente limitazione del numero e delle funzioni degli uffici che intervengono nell'iter di ognuno di essi, il contenimento dei poteri lobbistici, la precisazione di limiti all'accesso alle cariche pubbliche e politiche, la fissazione di regole sulle incompatibilità e vincoli sugli avanzamenti di carriera, la promozione dei codici di comportamento dei dipendenti pubblici, il minore ricorso a tecnici e consulenti esterni all'amministrazione. Semplificazione e sburocratizzazione non devono essere considerate come un elemento di antitesi alle regole anti corruzione. Anzi, la corruzione vive e si dilata proprio nelle complicazioni burocratiche. Le pratiche di semplificazione sono, nondimeno, osteggiate da chi grazie alla *maladministration* trova spazio per i propri interessi personali. Rimane sempre, tuttavia, di primaria importanza nel contrasto ai fenomeni corruttivi, un'attenta disciplina del conflitto di interessi, che tenda a contenere la commistione in capo ad uno stesso soggetto di interessi privati e pubblici confliggenti. L'attività di controllo deve, a tal riguardo, essere svolta da un organismo indipendente istituito ad hoc, evitando, ovviamente, che membri dell'organo controllore possano subire l'influenza dei controllati. Settore che necessita di una maggiore vigilanza, poiché estremamente vulnerabile ai fenomeni corruttivi e di conflitti d'interessi è, senza dubbio alcuno, quello degli appalti pubblici,

[38] Cfr. Tartaglia Polcini G., *La corruzione tra realtà e rappresentazione*, Minerva Editore, Bologna, 2018.

e ancor più nello specifico, le procedure di aggiudicazione relative ad alcuni settori con grandi movimentazioni di denaro pubblico, quali l'edilizia di grandi opere e la sanità.

I costi della corruzione in Italia sono altissimi: a titolo di esempio si pensi che l'alta velocità ferroviaria nelle tratte Novara-Milano e Bologna-Firenze è costata rispettivamente 79,5 e 96,4 milioni di euro al chilometro, mentre all'estero 10,2 milioni al chilometro della Parigi-Lione, 9,8 milioni della Madrid-Siviglia e 9,3 milioni di euro della Tokyo-Osaka[39]. Al tempo dell'entrata in vigore delle nuove norme anticorruzione, a partire dalla legge 190 del 6 novembre 2012, seguita dal d.lgs. n. 235/2012, d.lgs. n. 33/2013 e d.lgs. n. 39/2013, i costi totali diretti della corruzione ammontavano a 60 miliardi di euro l'anno, pari al 4 percento del PIL italiano, ossia la metà del costo complessivo dell'intera corruzione europea, stimato in circa 120 miliardi di euro annuali. A quasi dieci anni dall'entrata in vigore della normativa il centro Research and development (RAND) ha stimato che la corruzione costa oggi all'economia italiana almeno 236,8 miliardi, pari a circa il 13 percento del PIL, mentre è diminuita l'incidenza italiana nei confronti della corruzione dei Paesi europei, pari ad un totale di oltre 900 miliardi di euro[40]. Anche la percezione della corruzione nella popolazione era, all'epoca, particolarmente elevata poiché fra le imprese italiane il 90% considerava raccomandazioni e corruzione il modo più semplice per accedere a determinati servizi pubblici (contro una media U.E. del 69%), ed il 92% riteneva che corruzione e favoritismi impedissero la concorrenza commerciale (media U.E. del 73%)[41]. A distanza di un decennio l'opinione pubblica percepisce, oggi, l'Italia come un Paese meno corrotto, con ben 29 posizioni recuperate nei confronti degli altri Stati[42]. La valutazione della Commissione europea sui suddetti interventi di riforma era ampiamente positiva. Essa, difatti, affermava nella Relazione sulla lotta alla corruzione che tali interventi hanno consentito all'Italia di "fare un importante passo avanti", dopo che per anni sono stati "più volte ostacolati i tentativi di definire un quadro giuridico" efficace, con riferimento alle varie leggi *ad personam* a favore di politici imputati in procedimenti

[39] Dati della Relazione della Commissione europea sulla lotta alla corruzione.

[40] Le stime sono, tuttavia, da analizzare con le dovute cautele, poiché dipendono dalla capacità dei singoli Stati di conseguire l'emersione del fenomeno. Dal raffronto tra i dati giudiziari e quelli relativi alla percezione del fenomeno corruttivo lato sensu forniti da Trasparency International e dalla Banca mondiale si evince, difatti, che sussiste un ampio divario tra corruzione effettiva e quella denunciata. Il dato lascia, comunque, inequivocabilmente intendere le dimensioni in termini economici della problematica.

[41] Cfr. Speciale Eurobarometro n. 397/2013 (sondaggio condotto ogni due anni in tutti gli Stati membri, al fine di accertare il livello generale di percezione del fenomeno corruttivo).

[42] Il parametro di riferimento è il Corruption Perception Index (CPI) elaborato da Transparency International: nel 2011 l'Ialia era al sessantanovesimo posto, nel 2012 al settantaduesimo, mentre nel 2021 al quarantaduesimo, guadagnando un'ulteriore posizione nel 2022.

penali per reati di corruzione[43]. Nonostante il giudizio positivo la Relazione evidenziava criticità nel sistema italiano, soprattutto in riferimento al conflitto di interessi e alla prevenzione dei fenomeni corruttivi. Oltre alla necessità di rafforzare ulteriormente la tutela dei pubblici dipendenti segnalanti illeciti, i c.d. whistleblower, veniva considerata prioritaria la trasparenza delle attività di lobby e degli appalti pubblici, l'estensione di poteri di un'autorità anti corruzione indipendente, l'eliminazione delle contraddizioni della normativa in materia di conflitto d'interessi. Il giudizio della Commissione sulla legge 190 del 2012, pur essendo complessivamente positivo, scopre alcune fragilità, ossia l'aver frammentato le fattispecie penali di concussione e corruzione, e soprattutto non aver modificato o trattato punti scoperti quali il falso in bilancio, l'autoriciclaggio e la prescrizione[44]. Fornisce, poi un dato criminologico interessante, riferendo che non è la criminalità organizzata a generare la corruzione, bensì è la corruzione ad attrarre i gruppi criminali organizzati. Se ne deduce che la corruzione preesiste ai gruppi criminali, riuscendo ad indirizzare le attività illecite di questi ultimi in determinati settori ed aree geografiche. Secondo la Commissione, insufficienti risultano anche gli interventi di riforma in materia di corruzione nel settore privato. In particolare mancano attribuzioni di responsabilità per carenza di sorveglianza ed i procedimenti penali prendono generalmente inizio su querela dell'offeso e non *ex officio* da parte delle procure.

Riguardo la dislocazione territoriale della corruzione nel nostro Paese, da rilevare che nella sola regione Sicilia, nell'ultimo triennio è stato registrato approssimativamente lo stesso numero di eventi corruttivi dell'intero Nord Italia; a seguire Lazio, Campania, Puglia e Calabria, ossia tutte regioni del Sud del Paese, ad esclusione del Lazio[45]. Il 74% dei casi ha riguardato l'assegnazione di appalti pubblici, a conferma del rilievo di tale ambito nel complesso degli eventi corruttivi. La contrattualistica pubblica è, pertanto, il settore più a rischio, ed in particolare quella legata ai lavori pubblici, i cui eventi corruttivi censiti sono pari al 40% del totale, seguiti dal comparto legato allo smaltimento rifiuti, poi il settore sanitario, i cui eventi sono pari al 13% del totale. Le forme di corruzione si registrano più diffusamente a livello locale[46]. Negli ultimi anni si è riscontrata una progressiva smaterializzazione della c.d. tangente, per cui l'aspettativa per il corrotto riguarda un

[43] La Commissione fa specifico riferimento al DDL 3137 sulla prescrizione breve, il c.d. "lodo Alfano" del 2008, la legge sul legittimo impedimento n. 51 del 2010 e la depenalizzazione di reati come il falso in bilancio, ad opera del d.lgs. n. 61 del 2002.

[44] In Italia i procedimenti penali estinti per decorso dei termini di prescrizione sono l'11,4% contro una media UE dello 0,1% (fonte Min. Giustizia).

[45] ANAC, *La corruzione in Italia - Numeri, luoghi e contropartite del malaffare*.

[46] Comuni 41%, società partecipate 16%, Aziende sanitarie locali 11%.

beneficio non più necessariamente monetario. Il c.d. *pay-off*, ossia il vantaggio derivato dall'accordo corruttivo, non è più meramente di natura economica, configurando un vero e proprio scambio di favori, e sempre più spesso riguarda non personalmente il corrotto, ma soggetti terzi, quali membri della famiglia, gruppi di interesse, amici e colleghi. Si riscontra, difatti, alla base dello scambio corruttivo, una minor ricorrenza alla contropartita economica, stante la difficoltà di occultamento delle somme illecitamente percepite, ed il conseguente avanzamento di forme non direttamente economiche di corrispettivo ed interessi di diversa natura, quali l'acquisizione di potere o prestigio, la promessa di una promozione, l'assunzione di un congiunto, l'assegnazione di prestazioni professionali e consulenze, assegnazione di borse di ricerca, ma anche prestazioni sessuali[47]. In ogni caso qualsiasi comportamento corruttivo presuppone da parte dei soggetti coinvolti, una stima costi-benefici, influenzata dall'entità del margine di rischio, che se troppo alta può risultare dissuasiva[48]. Pertanto la comprensione dei meccanismi, non solo economici, che portano alla corruzione è di particolare interesse per indirizzare le attività di contrasto sia repressive che preventive. Il calcolo dei costi diretti ed indiretti della corruzione è essenziale per comprendere l'incidenza del fenomeno sulla spesa pubblica e sulla qualità dei servizi e della vita dei cittadini, ridestando, così, una maggior attenzione nell'opinione pubblica ed un sentimento di ribellione e volontà comune di contrasto allo stesso.

La corruzione riesce non solo ad indirizzare l'allocazione di risorse economiche verso un settore determinato o verso un'area geografica piuttosto che un'altra, ma anche la tipologia di investimenti. Tutto ciò può condurre al rischio del c.d. *State capture*, ossia il sopravvento degli interessi economici di un gruppo di privati rispetto all'interesse pubblico. È, questa, un tipo di corruzione sistemica in cui le decisioni governative e la burocrazia vengono manipolate da privati e aziende per influenzare le politiche e i processi legislativi statali per promuovere interessi privati. Tale livello di corruzione non solo deteriora l'economia di un Paese, ma arriva a minare gravemente la credibilità delle istituzioni e a danneggiare il tessuto della società civile[49]. Sul piano economico, oltre all'alterazione del sistema dei prezzi nei mercati e l'ostacolo alla libera concorrenza, la corruzione inibisce lo sviluppo di nuove attività, sottrae risorse ad imprese e Stato,

[47] Cfr. ANAC, *La corruzione in Italia - Numeri, luoghi e contropartite del malaffare*, p. 5. Nello specifico le assunzioni di congiunti si sono riscontrate nel 13% dei casi, l'assegnazione di prestazioni professionali nell'11%, mentre il corrispettivo in denaro è diminuito al 48% dei casi totali.

[48] In tal senso Malem Segna J.F., *Globalizzazione, commercio internazionale e corruzione*, Edizioni Il Mulino 2004, p. 199 e ss.

[49] Si pensi agli altissimi tassi di corruzione presenti in alcuni Paesi sudamericani, che permettono la pervasiva entrata del fenomeno dai livelli più bassi della burocrazia fino ai più alti organi dello Stato.

altera l'offerta di risorse umane e riduce la qualità dei servizi pubblici, minandone addirittura la sussistenza. Il tutto corrisponde ad un rallentamento della crescita o ad un decremento del Prodotto Interno Lordo e sfiducia per investimenti provenienti dall'estero.

Si può pacificamente giungere alla conclusione che un ambiente corrotto generi nuovi eventi corruttivi, non solo perché viene progressivamente a perdersi una percezione di disvalore nelle condotte illecite, ma anche per la crescente tolleranza del sistema giuridico verso tali eventi[50]. Dopo la prima condotta corruttiva non sanzionata, si riduce drasticamente l'efficacia dissuasiva della norma giuridica e le ritrosie dovute all'eventuale biasimo morale, e ciò funge quale incentivo per la reiterazione della condotta. È necessario, pertanto, l'unanime riconoscimento della condotta corruttiva quale elemento di nocumento per tutti i cittadini, e ciò deve avvenire sia da parte delle istituzioni che da parte dell'opinione pubblica, ed in particolare dei mezzi di informazione di massa e di divulgazione culturale.

1.1.2. Il fulcro del contrasto alla corruzione: l'ANAC e il PNA

L'Autorità nazionale anticorruzione (ANAC) è un'autorità amministrativa indipendente col compito di prevenire la corruzione tramite attività di vigilanza e controllo nei confronti della Pubblica Amministrazione, delle società da essa partecipate e controllate e nel settore dei contratti pubblici. Nasce in Italia nel 2012 con la legge 6 novembre 2012, n. 190, la c.d. legge Severino, dalla trasformazione di un altro organismo pubblico, ossia la Commissione per la valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche (CIVIT), creata nel 2009. La nascita di un organismo di vigilanza sulla corruzione è in ritardo di circa un ventennio nei confronti di altri Paesi europei quali Regno Unito, Spagna e Francia, che già prima degli anni novanta si avvalevano di controlli interni alle amministrazioni e controlli esterni affidati ad organi indipendenti, similari all'ANAC.

Il ruolo primario svolto dall'ANAC in materia di anticorruzione si focalizza sui settori considerati particolarmente a rischio dagli indicatori, e su quelle attività reputate più utili per il contrasto di pratiche illecite, ossia appalti, vigilanza e regolamentazione, con particolare riguardo ai contratti pubblici. Il sistema di controllo dell'Autorità ha consentito una maggiore discrezionalità alle

[50] In tal senso, Ufficio dell'Alto Commissario Anticorruzione, *Il fenomeno della corruzione in Italia*, 2007, studi sulla "mappa del fenomeno" in Italia, p. 16, ove si afferma "la corruzione genera corruzione, secondo un processo diffusivo in senso orizzontale e verticale, quantitativo e qualitativo".

stazioni appaltanti ed una regolamentazione meno rigida delle gare d'appalto. La concentrazione di più funzioni in capo all'ANAC, sia nel campo della vigilanza dei contratti pubblici che della trasparenza, ha indubitabilmente migliorato il livello organizzativo, precedentemente frazionato fra più organismi, al fine di contrastare la corruzione. L'autorità svolge, nello specifico, compiti di vigilanza, controllo e accertamento, con potere di sanzionare eventuali irregolarità perpetrate dai partecipanti ad una gara d'appalto, e di segnalare illeciti all'autorità giudiziaria. Si occupa, poi, del rispetto degli obblighi di trasparenza della Pubblica Amministrazione, del controllo dei Piani triennali, incompatibilità ed inconferibilità di funzioni pubbliche, nonché conflitto di interessi dei funzionari. Di grande rilevanza è il potere dell'ANAC, in caso di delitti contro la Pubblica Amministrazione, di proporre al Prefetto competente il commissariamento degli appalti affidati illecitamente[51]. Ratio di tale potere conferito all'Autorità è di evitare l'interruzione dei lavori pubblici permettendone il completamento, in una logica di controllo e sorveglianza negli appalti, ma nel contempo di efficienza e di tutela delle opere pubbliche. L'attività dell'ANAC, in particolare per ciò che attiene il procurement pubblico, non può essere considerata come una delega di poteri dovuta a contingenze meramente emergenziali, ma all'opposto deve rappresentare un'assunzione di responsabilità in una materia complessa, che si affida a rimedi strutturali nel medio e lungo periodo, e non estemporanei e propagandistici. L'ANAC, avente fini preventivi più che sanzionatori, non limita la sua funzione al controllo ed alla repressione dei comportamenti illeciti, ma si focalizza su una verifica di accountability[52] dell'Amministrazione Pubblica, intesa quale responsabilizzazione nell'abito del proprio ruolo, da parte di ogni soggetto che ne fa parte o che la rappresenta.

La vigilanza sul rispetto della normativa sulla trasparenza è un compito essenziale, svolto dall'ANAC, per la tutela dei diritti dei cittadini, quali l'accessibilità agli atti, dati e documenti delle Pubbliche Amministrazioni, partecipazione a concorsi e gare pubbliche, sburocratizzazione e semplificazione delle procedure pubbliche. Le funzioni consultive delle amministrazioni, la regolazione in materia anticorruzione e l'attività di controllo riguardo gli incarichi pubblici, rappresentano un altro aspetto di cui si occupa l'ANAC. Ma è in materia di contratti pubblici che l'Autorità svolge il ruolo più attivo: oltre alla vigilanza, essa esercita un'attività consultiva che si concretizza in pareri sulle normative vigenti e sull'emanazione di nuove disposizioni, impegno nel

[51] ANAC, *La corruzione in Italia (2016-2019) Numeri, luoghi e contropartite del malaffare*, p. 2.
[52] Sull'importanza dell'accountability si consulti: Bustin G., *Accountability: The Key to Driving a High-Performance Culture*, 2014.

risolvere il precontenzioso durante le procedure di gara, supporto e sostegno alle amministrazioni, rendendo disponibili alle stazioni appaltanti bandi-tipo, capitolati e contratti-tipo, strumenti di regolamentazione flessibile, ossia i c.d. atti di *soft law*.

Di particolare rilevanza è la disponibilità da parte dell'ANAC di banche dati capaci di indicare anomalie e conflitti di interessi, indispensabili per l'individuazione di situazioni di rischio, le c.d. *red flags*. A tal fine vengono utilizzate moderne tecnologie di raccolta dati ed analisi degli stessi per la ricerca di situazioni anomale, cui consegue una vigilanza più stringente da parte dell'Autorità e degli organi preposti. Ciò rappresenta, inequivocabilmente, un nuovo punto di partenza nelle moderne strategie di prevenzione del rischio di corruzione[53].

Nonostante la rilevanza, utilità e nobiltà della funzione svolta dall'ANAC, alcune perplessità e critiche vengono ancora sollevate nei suoi confronti da autorevole dottrina, con particolare riferimento alle nomine dei vertici dell'organo da parte della politica[54]. Ciò implica il sorgere di interrogativi sulla sua effettiva indipendenza. Altre critiche, meno condivisibili delle precedenti, mosse all'Autorità, riguardano il suo contributo al rallentamento nel completamento delle opere pubbliche, l'aver cagionato un'ulteriore burocratizzazione dell'amministrazione, ed infine di aver sgravato la classe politica del dovere di buona amministrazione[55].

---

[53] Sul punto Raffaele Cantone, presidente dell'ANAC dal 2014 al 2019, I*l sistema della prevenzione della corruzione in Italia*, in *Diritto Penale Contemporaneo*, 2017, p. 8, afferma "In sintesi, si avverte una logica complessiva che connota nel senso dell'anticorruzione l'intera strategia nazionale di recepimento delle regole europee in materia di contratti pubblici. In un disegno, in sostanza, nel quale da un lato il codice dei contratti è conformato in modo penetrante dalle esigenze dell'anticorruzione e d'altra parte il ruolo dell'Autorità si pone sempre più quale strumento e motore di legalità nel sistema dei contratti pubblici: soggetto portatore di un interesse generale alla legalità, titolare per questo di una legittimazione straordinaria, fino a disporre, nel processo amministrativo, di un ruolo quasi assimilabile a quello di un pubblico ministero, con la possibilità, introdotta da una norma 2017, di impugnare i bandi di gara".

[54] Il Presidente dell'ANAC viene nominato su proposta del Ministro per la Pubblica Amministrazione, di concerto col Ministro dell'Intero e della Giustizia. Ciò lo colloca, almeno su un piano teorico, in connessione con l'attività di Governo, creando dubbi circa l'indipendenza sul piano politico. I quattro membri del collegio, poi, sono nominati con decreto del Presidente della Repubblica su deliberazione del Consiglio dei ministri, previo parere favorevole dei due terzi dei componenti le Commissioni parlamentari competenti.

[55] Fra le critiche più autorevoli ed aspre nei confronti dell'ANAC, si possono sicuramente citare quelle di Sabino Cassese, che il 21 gennaio 2017 in un'intervista al Foglio affermava "la disciplina dei contratti pubblici è scritta dall'angolo visuale della corruzione, ciò che fa perdere di vista gli altri obiettivi. La legislazione degli ultimi anni è sostanzialmente ispirata al principio del sospetto generalizzato, che è l'anticamera dell'autoritarismo […] l'Autorità anticorruzione procede alla cieca, assume che tutti siano sospetti di corruzione, che questa si possa annidare dovunque". Severe critiche del Prof. Cassese riguardavano i dati raccolti ed analizzati dall'ANAC, poiché "sapere come evolvono nel tempo, come sono distribuiti sul territorio i fenomeni corruttivi insegnerebbe molto. Poi bisognerebbe aver dati meno impressionistici sugli snodi e sui luoghi dove si sviluppa la corruzione". Enuclea, poi, gli effetti a cui può condurre la centralizzazione dei compiti dell'ANAC, affermando che "Creando questo moloch, la classe politica si è sgravata del compito della buona amministrazione", nonché le conseguenze negative "La prima è la relativa stagnazione delle opere pubbliche. La seconda l'allungamento delle decisioni. La terza l'imposizione di obblighi amministrativi spesso macchinosi anche su amministrazioni minuscole", concludendo che l'ANAC sia "una entità

Il ruolo dell'ANAC viene rafforzato nel 2016 con il Codice dei contratti pubblici (D.lgs. 18 aprile 2016 n. 50). In particolare l'art. 213 del predetto decreto legislativo attribuisce all'Autorità la vigilanza e il controllo sui contratti pubblici e l'attività di regolazione degli stessi, quello di vigilare affinché sia garantita l'economicità dell'esecuzione dei medesimi, il potere di segnalare al Governo e al Parlamento fenomeni particolarmente gravi di inosservanza o di applicazione distorta della normativa di settore, ovvero il potere di vigilare sul divieto di affidamento dei contratti attraverso procedure differenti da quelle ordinarie. Direttamente collegato alla funzione di vigilanza è altresì il compito assegnato all'Autorità in ordine alla tenuta di elenchi ed albi dei soggetti che operano nel settore dei contratti pubblici, nonché l'unificazione presso l'Autorità stessa, delle banche dati nelle quali dovranno essere raccolte tutte le informazioni relative agli appalti nazionali centrali e locali. Un patrimonio informativo completo degli affidamenti operati dal complesso delle stazioni appaltanti sul territorio nazionale consentirà all'Osservatorio, che opera in seno all'Autorità, di individuare specifici settori che presentano criticità sul piano del rispetto delle procedure ad evidenza pubblica, su cui è necessario focalizzare l'attività di vigilanza[56].

Uno strumento di particolare rilevanza per la progettazione di strategie di contrasto è il piano di prevenzione della corruzione, articolato su due livelli: nazionale e territoriale. Di livello nazionale è il PNA, ossia il Piano Nazionale Anticorruzione, che disegna la prevenzione come processo di *risk assessment*[57]. È, questo, un piano triennale tramite cui l'ANAC fornisce alle Pubbliche Amministrazioni la linea da seguire per l'identificazione del rischio, la sua analisi e il contenimento con misure adeguate, secondo un principio di prevenzione della corruzione, nonché indirizzo e supporto per il contrasto del fenomeno. Esso ha la specifica funzione di promuovere l'adozione di misure di prevenzione della corruzione, individuandone i principali rischi ed i relativi rimedi, con l'indicazione di obiettivi, tempi e modalità di adozione ed attuazione delle misure di contrasto dei fenomeni corruttivi. Il PNA distingue le misure di prevenzione della corruzione in generali e specifiche: sono generali le misure che incidono sul sistema della prevenzione della corruzione, intervenendo su settori che riguardano in modo trasversale tutte le pubbliche amministrazioni;

ambigua. Dice di esser un'autorità indipendente, ma opera anche d'intesa con i ministeri, o per loro delega; dà pareri al governo; suggerisce le politiche", mettendone, così, in dubbio l'indipendenza.

[56] Cfr. Nicotra I.A., *L'autorità nazionale anticorruzione tra prevenzione e attività regolatoria*, Giappichelli Editore, 2016, p. 56 e ss.

[57] Sull'argomento, Rausand M., Haugen S., *Risk Assessment. Theory, methods and applications*, Wiley Editore, aprile 2020.

sono invece specifiche quelle misure che incidono su problemi riguardanti il contesto di riferimento in cui opera l'amministrazione, il suo settore, le sue peculiarità. L'ultimo PNA ha sistematizzato il processo di gestione del rischio rendendolo maggiormente efficiente, confermando la distinzione tra aree di rischio generale e aree di rischio specifiche, ed evitando analisi standardizzate poiché si sono tenute in considerazione le differenze fra le varie amministrazioni[58].

A livello locale ciascuna amministrazione è tenuta a predisporre un proprio piano, coerente con quello nazionale, il Piano Triennale di Prevenzione della Corruzione (PTPC) da cui ha avvio la realizzazione di previsioni vincolanti. Mentre il PNA è un piano tramite cui l'ANAC fornisce alle Pubbliche Amministrazioni la linea da seguire per l'identificazione del rischio, la sua analisi e il contenimento con misure adeguate, secondo un principio di prevenzione della corruzione, nonché indirizzo e supporto per il contrasto del fenomeno, il PTPC è un documento che definisce la strategia di prevenzione della corruzione nell'ambito della singola amministrazione, attraverso l'analisi dell'organizzazione, delle regole e prassi. Il PTPC è un documento di natura programmatica includente le misure obbligatorie e non, in un'ottica di coordinamento dei vari interventi.

Soggetto cardine di questo meccanismo è il RPCT (Responsabile della Prevenzione della Corruzione e della Trasparenza) con il compito di adottare, in funzione del piano, le specifiche misure di prevenzione necessarie al contenimento dei rischi, assicurando l'efficacia delle azioni di prevenzione. Compiti principali del PTPC sono: individuare le aree a maggior rischio corruzione e conflitto d'interessi (c.d. risk assessment); prevedere obblighi d'informazione e trasparenza; monitorare le situazioni di incompatibilità e conflitto di interessi; prevedere meccanismi di controllo idonei a prevenire il rischio corruzione. Le funzioni specifiche del RPCT attengono alla: predisposizione del PTPC e sottoposizione dello stesso all'organo di indirizzo per l'approvazione; verifica dell'efficace attuazione del PTPC e sua idoneità, e proposta di modifiche allo stesso, quando sono accertate violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione dell'amministrazione; verifica dell'effettiva rotazione degli incarichi negli uffici maggiormente esposti ai reati corruttivi e definizione delle procedure appropriate per

[58] Il Piano è completato da tre allegati, specificamente dedicati: alla gestione dei rischi corruttivi, alla rotazione ordinaria del personale ed alla sistematizzazione dei riferimenti normativi sul ruolo e sulle funzioni del Responsabile della prevenzione della corruzione e della trasparenza.

selezionare e formare i dipendenti destinati ad operare nelle aree a rischio corruzione; redazione della relazione annuale recante i risultati dell'attività svolta, tra cui il rendiconto sull'attuazione delle misure di prevenzione definite nei PTPC; attività di controllo sull'adempimento da parte dell'amministrazione degli obblighi di pubblicazione e informazione previsti dalla normativa vigente. Il Responsabile della Prevenzione della Corruzione e della Trasparenza si occupa, inoltre, dei casi di riesame dell'accesso civico e cura la diffusione della conoscenza dei Codici di comportamento nell'amministrazione, il monitoraggio annuale della loro attuazione, la pubblicazione sul sito istituzionale e la comunicazione all'ANAC dei risultati del monitoraggio. Le responsabilità del RPCT sono stabilite dagli articoli 12 e 14 della legge n. 190 del 2012. Secondo l'art. 12 in caso di commissione, all'interno dell'amministrazione, di un reato di corruzione accertato con sentenza passata in giudicato, il RPCT risponde per responsabilità dirigenziale[59], nonché sul piano disciplinare, oltre che per il danno erariale ed all'immagine della Pubblica Amministrazione, salvo che provi di avere predisposto, prima della commissione del fatto, il PTPC e di aver vigilato sul funzionamento e sull'osservanza del Piano stesso. Per l'art. 14 della legge Severino, invece, in caso di ripetute violazioni delle misure di prevenzione previste dal Piano, il RPCT risponde per responsabilità dirigenziale, nonché a livello disciplinare per omesso controllo, salvo che provi di avere comunicato agli uffici le misure da adottare e le relative modalità. La violazione, da parte di tutti i dipendenti dell'amministrazione, delle misure di prevenzione previste dal Piano, costituisce illecito disciplinare.

Il punto di forza di questo sistema è l'esistenza di un equilibrio dato da una pluralità di nodi e funzioni, non agenti solo a livello centralizzato, ma che coinvolgono ogni singola amministrazione, in un'ottica di prossimità. Tali componenti dialogano grazie all'ANAC, intesa quale centro di coordinamento nazionale dell'attività di prevenzione della corruzione in Italia. Tramite il Piano, ciascun ente può attivare meccanismi di prevenzione già rodati, quali la rotazione del personale, utili ad evitare il consolidamento di situazioni di rischio di conflitto di interessi. Nel Piano triennale assumono particolare rilievo le linee guida indirizzate alle amministrazioni e agli enti destinatari della legge n. 190 del 2012, con finalità di supporto nell'applicazione della normativa sulla trasparenza e prevenzione alla corruzione e l'elaborazione di indicatori di inefficienza della spesa pubblica e di rischio corruttivo[60]. La metodologia utilizzata per l'analisi del rischio è volta ad

[59] Ai sensi dell'articolo 21 del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni.
[60] ANAC, documento di Rappresentazione delle funzioni dei macro-processi e dei processi.

assicurare una precisa rappresentazione delle informazioni rilevanti, al fine di identificare e valutare il rischio di corruzione, e poter di conseguenza rafforzare la strategia preventiva. Non ci si può, infine, esimere dal rimarcare la rilevanza del ruolo che svolgono oggi i codici di comportamento, dedicati ai dipendenti della Pubblica Amministrazione, ancor più minuziosi della legge nello stabilire regole sul conflitto d'interessi, i quali comminano sanzioni e provvedimenti disciplinari nei confronti di coloro che compiano irregolarità o omissioni, anche in caso di situazioni non penalmente rilevanti.

1.1.3. Il conflitto di interessi e il connubio indissolubile con la corruzione

Il conflitto di interessi corrisponde alla particolare condizione in cui un soggetto, nello svolgimento di un'attività, è tenuto a realizzare un interesse primario che contrasta con un suo personale interesse[61]. Il contesto in cui maggiormente proliferano tali conflitti sono indubitabilmente le società pluralistiche, nelle quali imperano princìpi liberali e di autonomia dei privati, tutelati dalle norme costituzionali. Sin dalle origini, tuttavia, punto fondamentale del pensiero liberale è un progetto di società in cui non vi sia il cumulo di potere istituzionale e politico con il potere proprietario dovuto ad una determinata posizione economica. Quello che oggi chiamiamo "conflitto di interessi" è, pertanto, un'anomalia, o meglio una degenerazione delle moderne società liberali. Difficilmente, però, tale degenerazione viene combattuta. I gruppi sociali hanno storicamente cercato di arginare il problema della separazione fra potere politico e giudiziario, fra potere esecutivo e legislativo, ma non si è, specialmente in Italia, risolto il problema, altrettanto importante, della separazione fra potere economico e potere politico o amministrativo, almeno nel caso in cui esso confligge con l'interesse personale del soggetto investito di una decisione pubblica. Da ciò si può facilmente dedurre quanto sia importante nel nostro Paese una disciplina giuridica che tenga in considerazione i valori in conflitto fra loro, garantendo la partecipazione di tutti i cittadini alla vita politica e sociale in un'ottica di eguaglianza sostanziale, ma nello stesso tempo prevenendo pericolose collisioni fra interesse pubblico ed individuale.

[61] Nonostante risalga agli anni novanta, ancora attuale è la definizione di conflitto di interessi di D.F. Thompson, secondo cui "Il conflitto di interessi è una situazione in cui un interesse secondario (finanziario o non finanziario) di un agente pubblico tende ad interferire con l'interesse primario dell'amministrazione verso cui l'agente ha precisi doveri e responsabilità", Thompson D.F., *Understanding financial conflicts of interest*, in *New England Journal of Medicine*, 1993, p. 573.

L'OCSE ha individuato tre tipi di conflitti di interessi: quello reale, detto anche attuale, che implica un conflitto tra la missione pubblica e gli interessi privati di un funzionario pubblico, che potrebbero influire sull'assolvimento dei suoi obblighi e delle sue responsabilità; apparente, quando vi è la sola percezione dall'esterno che gli interessi privati di un funzionario pubblico possano influire sull'assolvimento dei suoi obblighi; potenziale, che si verifica quando un funzionario pubblico ha interessi privati che potrebbero far sorgere un conflitto di interessi nel caso in cui questi dovesse assumere in futuro responsabilità specifiche. La presenza di un conflitto di interessi, qualunque sia la tipologia, non è di per sé illegale. Vi è, invece, un generale divieto di partecipare a una procedura pur essendo a conoscenza di un proprio conflitto di interessi. È, pertanto, necessario comunicare i potenziali conflitti appena se ne viene a conoscenza ed adottare le misure preventive adeguate. A tal fine i membri del personale che gestiscono procedure pubbliche devono essere messi a conoscenza dall'amministrazione di eventuali e potenziali situazioni di conflitto di interessi, delle implicazioni che ne conseguono e del modo di procedere in questi casi, nonché delle eventuali sanzioni previste. La formazione continua e l'informazione possono, difatti, mantenere ed accrescere la sensibilizzazione del personale e quindi far sì che esso sia sempre consapevole di possibili nuove situazioni di conflitto di interessi. All'informazione deve essere abbinata la responsabilizzazione dei dipendenti pubblici. Il principale strumento col quale si concretizza il connubio informazione/responsabilizzazione è, indubbiamente, l'autodichiarazione di assenza di conflitti di interessi. Essa assume particolare rilievo con le procedure d'appalto. Le verifiche ed i controlli su tali dichiarazioni di assenza di conflitti di interessi devono essere sia interni che esterni alla specifica amministrazione, permanenti e periodici, e anche a campione, ma devono avvenire comunque in maniera specifica in ogni situazione concreta ad alto rischio di conflitto di interessi in ottemperanza all'art. 6-bis della legge n. 241 del 1990[62].

I fenomeni corruttivi sono strettamente legati al conflitto di interessi, poiché quest'ultimo ne è, attualmente, una delle principali cause. La corruzione è, difatti, sempre più alimentata dalla presenza del conflitto di interessi, e si concretizza nell'abuso o nell'omissione della funzione pubblica per fini individuali o privati. Per aversi un conflitto di interessi è sufficiente la presenza di un interesse secondario che tende ad interferire in modo reale, potenziale o apparente con un

[62] L'art. 6-bis della l. n. 241/1990 stabilisce che "il responsabile del procedimento e i titolari degli uffici competenti ad adottare i pareri, le valutazioni tecniche, gli atti endoprocedimentali e il provvedimento finale, devono astenersi in caso di conflitto di interessi, segnalando ogni situazione di conflitto, anche potenziale".

interesse primario. Il conflitto di interessi si distingue dalla corruzione poiché non è un comportamento, ma una situazione di fatto, un insieme di circostanze che creano o aumentano il rischio che gli interessi primari possano essere compromessi dalla prevalenza di quelli secondari[63]. Tuttavia la corruzione è, nella maggior parte dei casi, la degenerazione di un conflitto di interessi, che si concretizza con il prevalere di un interesse secondario personale nei confronti di un interesse primario collettivo in contrasto con esso[64]. Prima di tale degenerazione si ha una semplice presenza di interessi in conflitto, anche solo in modo potenziale o apparente, non corrispondente ad alcun illecito o comportamento di per sé penalmente rilevante[65]. Il Consiglio di Stato ha affermato, secondo un costante orientamento[66], che "il conflitto di interessi non consiste quindi in comportamenti dannosi per l'interesse funzionalizzato, ma in una condizione giuridica o di fatto dalla quale scaturisce un rischio di siffatti comportamenti, un rischio di danno. L'essere in conflitto e abusare effettivamente della propria posizione sono due aspetti distinti". Per consolidata giurisprudenza amministrativa la sussistenza di un conflitto è, peraltro, indipendente dal vantaggio che il singolo ne possa conseguire. Se gestito in maniera corretta, il conflitto di interessi non si tramuta necessariamente in un evento corruttivo: è questo il motivo per cui le attuali regolamentazioni anti corruzione si concentrano sulla prevenzione e sulla gestione del rischio, più che sulle sanzioni per i fatti illeciti, già rientranti nella fase giudiziaria. Peraltro lo stesso Consiglio di Stato ha recentemente ribadito che "ciò che rileva è il conflitto che in astratto (potenziale) può verificarsi e che è, di contro, ininfluente che esso si sia nel concreto realizzato, ove si consideri che gli obblighi imposti al pubblico dipendente mirano a garantire la trasparenza e l'imparzialità dell'azione amministrativa e, ad un tempo, a prevenire fenomeni di corruzione"[67].

[63] Cfr., Thompson J.D., *Organization in action*, 2009.

[64] Secondo Di Carlo E., *Il conflitto di interessi nelle aziende. Linee guida per imprese, amministrazioni pubbliche e non-profit*, Giappichelli, 2020, p. 46 ss., l'elemento che muta nel passaggio da conflitto di interessi a corruzione è la tendenza dell'interesse secondario ad interferire con quello primario, pertanto "il conflitto di interessi è una situazione di rischio in cui l'interesse secondario tende a interferire con l'interesse primario, nella corruzione la situazione di rischio si è trasformata in un abuso di potere, che ha visto prevalere l'interesse secondario su quello primario".

[65] Cfr. Carney G., *Working Paper, Conflict of interest: Legislators, Minister and Publical Officers*, in www.trasparency.org, 1998. Secondo l'autore "la corruzione è la fase finale del conflitto di interessi. Si può dire che tutti i casi di corruzione includono il conflitto di interessi, mentre non è sempre vero il contrario. Inoltre, la corruzione è molto spesso un crimine, mentre il conflitto di interessi incorpora un'ampia gamma di comportamenti, la maggior parte dei quali non costituisce reato".

[66] Cons. di Stato, Sez. cons. atti norm., 5 marzo 2019, n. 667. In tal senso anche, Cons. di Stato, sez. V, 14 maggio 2020, n. 3048 e Cons. di Stato, sez. III, 14 gennaio 2019, n. 355.

[67] Consiglio di Stato, sentenza n. 22683 del 2018.

La stessa definizione di corruzione è, oggi, più estesa della mera fattispecie penalistica, poiché include, in un'ottica preventiva, anche il conflitto di interessi e la c.d. *maladministration*. Le norme in vigore alimentano suddetta lettura: secondo il Dipartimento della Funzione Pubblica, nella legge 190 del 2012 si parla di eventi corruttivi come situazioni più ampie della fattispecie penalistica, in cui venga, comunque "in evidenza un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite"[68]. Il campo di intervento di definizione della corruzione, dal rilievo penalistico sempre vincolato alla personalità della responsabilità, nel tempo si è dilatato fino a ricomprendere aspetti organizzativi e pluralistici, frutto di una diversa logica di prevenzione, oltre che di repressione[69]. L'accento si sposta sempre più dall'illecito già consumato al rischio, con una strategia di contrasto rivolta al conflitto di interessi, anche solo apparente. Nell'orbita delle recenti politiche anti corruzione di carattere preventivo vengono, così, sempre più in rilievo le tematiche sul conflitto di interessi, ed in particolare la circoscrizione di aree che costituiscono terreno fertile per i comportamenti corruttivi.

In tale ottica gioca un ruolo principale la trasparenza dell'attività amministrativa[70]. Essa è, difatti, alla base della logica di prevenzione della corruzione, quale mezzo privilegiato per l'individuazione e l'emersione del conflitto di interessi, secondo una dialettica inversa a quella del secolo scorso: non è l'amministrazione a dover controllare il cittadino, ma è, viceversa, il cittadino a svolgere l'attività di controllo nei confronti dei pubblici poteri. Tale controllo è strutturato principalmente su due modelli: gli obblighi di pubblicazione sul portale dell'ente nella sezione dedicata all'amministrazione trasparente, in un'area facilmente individuabile ed aperta a tutti gli utenti, oggetto di disciplina specifica nella legge n. 33 del 2013, e l'accesso civico generalizzato, introdotto col d.lgs. n. 97 del 2016.

Nel Piano stesso di prevenzione della corruzione, un primo gruppo di misure è volto a contenere i conflitti di interessi, con particolare attenzione ai comportamenti del funzionario pubblico, quale punto di partenza e base per il contrasto alla corruzione. Proprio dai Piani territoriali si evince

[68] Circolare n. 1 del 25/1/2013 del Dipartimento della Funzione Pubblica.

[69] In tal senso, Cantone R., *Il sistema della prevenzione della corruzione in Italia*, in *Diritto Penale Contemporaneo*, testo della prolusione tenuta alla inaugurazione dell'a.a. 2017/2018 del Dipartimento di Scienze politiche dell'Università degli studi di Perugia, p. 4 e ss.

[70] Sull'argomento: AA.VV., *Legislazione anticorruzione e responsabilità nella pubblica amministrazione*, Cerioni F., Sarcone V. (a cura di), Giuffré Francis Lefebvre, 2019, p. 56 ss.; Cingari F., *Repressione e prevenzione della corruzione pubblica. Verso un modello di contrasto "integrato"*, G. Giappichelli Editore, Torino, 2012, p. 112 ss; Della Torre G., *Politica e amministrazione della spesa pubblica: controlli, trasparenza e lotta alla corruzione*, Atti del LIX convegno di studi di scienza dell'amministrazione, Giuffré, 2014, p. 32 ss.

l'indissolubile legame fra corruzione e conflitto di interessi. La prevenzione ai fenomeni corruttivi nasce, difatti, proprio dalle situazioni di rischio, ed è pertanto necessario sostenere l'emersione di interessi privati confliggenti con la tutela dell'interesse pubblico.

Per un efficace contrasto alla corruzione è necessario un elemento di disincentivazione molto forte, dato dalla elevata probabilità di individuazione delle attività corruttive con conseguente alto rischio di incorrere nella sanzione giuridica penale, ed una credibile rappresentazione della sanzione come deterrente. Ma per una lotta alla corruzione che dia risultati positivi è necessario considerare anche quelle circostanze, che se pur non previste come reato dal codice penale, coincidano con quelle situazioni di "maladministration", che l'ANAC nel Piano Nazionale Anticorruzione del 2015 ha identificato con l'assunzione di decisioni devianti dalla cura dell'interesse generale a causa del condizionamento improprio da parte di interessi particolari. Occorre, pertanto, considerare l'opportunità e monitorare, altresì "comportamenti che, anche se non consistenti in specifici reati, contrastano con la necessaria cura dell'interesse pubblico e pregiudicano l'affidamento dei cittadini nell'imparzialità delle amministrazioni e dei soggetti che svolgono attività di pubblico interesse"[71]. Quanto affermato dall'ANAC è indiscutibile, ed è unanimemente accettato e corroborato dai dati statistici dei procedimenti giudiziari. D'altronde la Circolare n. 1 del Dipartimento della Funzione Pubblica già nel 2013 stabiliva: "Il concetto di corruzione deve essere inteso in senso lato, come comprensivo delle varie situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati. Le situazioni rilevanti sono quindi evidentemente più ampie della fattispecie penalistica, che, come noto, è disciplinata negli artt. 318, 319 e 319 ter, c.p., e sono tali da comprendere non solo l'intera gamma dei delitti contro la pubblica amministrazione disciplinati nel Titolo II, Capo I, del codice penale, ma anche le situazioni in cui – a prescindere dalla rilevanza penale – venga in evidenza un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite"[72]. Stanti tali premesse, indiscutibile viene alla luce in maniera prorompente, l'intreccio fra pubblici poteri, fenomeni corruttivi e conflitto d'interessi.

[71] Autorità Nazionale Anticorruzione, Aggiornamento 2015 al Piano Nazionale Anticorruzione, Determinazione n. 12 del 28 ottobre 2015, p. 7.
[72] Circolare n. 1 del Dipartimento della Funzione Pubblica del 25/01/2013.

La crescente attenzione al conflitto di interessi in materia di prevenzione contro la corruzione è palese anche nel Codice dei contratti pubblici del 2016. Ne è un esempio l'art. 42 del codice, il quale impone alle stazioni appaltanti l'adozione di misure adeguate, volte a "prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione degli appalti e delle concessioni". A questo si aggiunge la volontà del codice di escludere dalle gare pubbliche, sempre nel rispetto della concorrenza, imprese a rischio poiché legate a vicende di corruzione, riciclaggio, frode, e di imporre a soggetti che si trovino in situazioni di conflitto d'interessi di darne comunicazione alla stazione appaltante ed astenersi dalla procedura di aggiudicazione, a fronte di una responsabilità amministrativa, nonché penale. La legge Severino prevede, poi, l'adozione di modalità di monitoraggio di eventuali rapporti o relazioni di parentela o affinità sussistenti tra i titolari, gli amministratori, i soci e i dipendenti dei soggetti stipulanti con le amministrazioni contratti, o interessati a procedimenti di autorizzazione, concessione o erogazione di vantaggi economici e i dipendenti dell'amministrazione stessa. È, tuttavia, la stessa ANAC ad ammonire che "nel nostro ordinamento non esiste una norma che preveda analiticamente gli elementi costitutivi e le diverse ipotesi della fattispecie di conflitto di interessi"[73].

1.2. La normativa italiana sulla corruzione e sul conflitto di interessi

1.2.1. Le leggi anticorruzione

La struttura fondamentale dell'attuale sistema anticorruzione discende dalla l. n. 190 del 6 novembre 2012, la c.d. legge Severino, la quale oltre a novellare significativamente il previgente d.lgs. n. 165 del 2001, ha introdotto nuove forme di prevenzione contro il malaffare nella Pubblica Amministrazione, come la disciplina sul c.d. whistleblowing e il divieto di revolving doors. La legge, con titolo "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", viene approvata in un periodo della vita del Paese caratterizzato da misure emergenziali di contrasto alla crisi economica e alla disoccupazione. Essa viene, difatti, varata più come provvedimento emergenziale e temporaneo che in qualità di rimedio strutturale per arginare l'endemico problema della corruzione. Obiettivo della legge è di adottare strumenti sanzionatori più severi contro la corruzione e l'illegalità nell'amministrazione, ma soprattutto prevenire il fenomeno rafforzando la trasparenza ed il controllo da parte degli stessi cittadini, in

[73] Faq Anac, aggiorn. 30 dicembre 2021, www.anac.it.

un'ottica di riallineamento con gli standard degli altri Paesi occidentali. Viene innanzi tutto istituita, in attuazione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione[74] e della Convenzione penale sulla corruzione[75], un'Autorità nazionale anticorruzione con precise prerogative, quali l'analisi delle cause della corruzione e gli interventi per contrastarla, l'esercizio di funzioni di vigilanza e controllo, l'approvazione di un piano di prevenzione a livello nazionale, l'emanazione di provvedimenti sulla trasparenza. Accanto ad essa, altri organi vengono onerati di precisi ruoli di supporto in materia di corruzione, come il Dipartimento della funzione pubblica, i Prefetti, le Pubbliche amministrazioni centrali, le Regioni e gli Enti locali, ed infine la Scuola superiore della Pubblica Amministrazione limitatamente al settore della formazione.

Di particolare rilevanza è l'individuazione da parte dell'organo di indirizzo, prevista al comma 7, art. 1 della legge 190/2012, fra i dirigenti amministrativi, della figura del Responsabile della prevenzione della corruzione e della trasparenza (RPCT) che ha, come compito primario, quello di segnalare agli organi preposti le disfunzioni inerenti l'attuazione delle misure di prevenzione e trasparenza ed indicare agli uffici competenti all'esercizio dell'azione disciplinare quei dipendenti che non hanno attuato correttamente le relative misure. Questi, alla fine di ogni anno propone il Piano triennale di prevenzione della corruzione, provvede alla sua effettiva attuazione, verifica la rotazione degli incarichi ad elevato rischio di corruzione. La violazione da parte dei dipendenti dell'amministrazione, delle misure di prevenzione previste dal Piano triennale, costituisce illecito disciplinare.

Uno dei punti su cui insiste maggiormente la legge n. 190 del 2012 è quello della trasparenza ed imparzialità della Pubblica Amministrazione, anche in attuazione del comma 2 dell'art. 97 della Costituzione. L'imparzialità della P.A. viene garantita tramite l'obbligo, previsto dalle novelle effettuate dall'art. 1 comma 41 della l. n. 190/2012 alla legge n. 241 del 1990 con l'aggiunta dell'art. 6 bis, di astensione del funzionario i cui interessi siano direttamente coinvolti nel procedimento. L'articolo in parola mostra, con l'obbligo di astensione e segnalazione di conflitto di interessi anche soltanto potenziale, l'inequivocabile volontà del legislatore di ostacolare *ab origine* il verificarsi di situazioni idonee, pur solo in astratto, a compromettere l'immagine, l'imparzialità ed il buon andamento dell'apparato amministrativo. Per l'art. 6 bis della legge n. 241 del 1990 "Il responsabile del procedimento e i titolari degli uffici competenti ad adottare i

[74] ONU, Convenzione del 31 ottobre 2003, ratificata ai sensi della legge n. 116 del 3 agosto 2009.
[75] Convenzione Strasburgo, 27 gennaio 1999, ratificata ai sensi della legge n. 110 del 28 giugno 2012.

pareri, le valutazioni tecniche, gli atti endoprocedimentali e il provvedimento finale devono astenersi in caso di conflitto di interessi, segnalando ogni situazione di conflitto, anche potenziale". Il succitato precetto ha dato attuazione nell'ordinamento nazionale all'art. 8 comma 5 della Convenzione ONU adottata dall'Assemblea generale il 31 novembre 2003, conosciuta come convenzione di Merida e ratificata dall'Italia con legge n. 116 del 2009[76]. L'art. 6 bis della legge n. 241/1990 ha, inoltre, recepito le indicazioni e le raccomandazioni provenienti da importanti organismi internazionali, quali il c.d. gruppo GRECO[77] del Consiglio d'Europa, e l'Organizzazione per la cooperazione e lo sviluppo economico, la quale ha predisposto apposite linee guida per la gestione del conflitto di interessi nei pubblici servizi.

La trasparenza amministrativa costituisce un livello essenziale delle prestazioni concernenti i diritti sociali e civili previsti dalla lettera m) del secondo comma dell'art. 117 della Costituzione. Essa è assicurata mediante la pubblicazione nella pagina web della specifica amministrazione, di tutte le informazioni relative ai procedimenti amministrativi secondo criteri di semplicità ed accessibilità, nel rispetto della protezione dei dati personali dei soggetti coinvolti. In particolare, nell'ambito del procurement pubblico, le stazioni appaltanti sono tenute a pubblicare in una pagina web accessibile a tutti gli utenti, le informazioni complete relative a bandi di gara ad evidenza pubblica, ossia: l'oggetto del bando, la struttura proponente, l'elenco degli operatori e l'aggiudicatario, l'importo di aggiudicazione e quello liquidato, i tempi di completamento dell'opera. Nell'ambito della trasparenza amministrativa è, poi, da annoverare l'obbligo dell'amministrazione di pubblicazione dei bilanci e costi di realizzazione delle opere pubbliche. Altre importanti modifiche alla legge 241 del 1990 sono previste al comma 37, art. 1 della legge 190 del 2012, il quale prevede che ove siano soggetti privati ad essere preposti all'esercizio di attività amministrative, questi sono tenuti ad assicurare un livello di garanzia non inferiore a quello cui sono tenute le Pubbliche Amministrazioni in tema di prevenzione alla corruzione.

Il comma 42 della legge 190 del 2012 rende più restrittiva la disciplina previgente, prevista dall'art. 53 d.lgs. n. 165 del 2001, in materia di incompatibilità al fine di evitare cumuli di incarichi e conflitti

[76] L'art. 8 comma 5 della Convenzione di Merida stabilisce che "Ciascuno Stato Parte si adopera, se del caso e conformemente ai principi fondamentali del proprio diritto interno, al fine di attuare misure e sistemi che obblighino i pubblici ufficiali a dichiarare alle autorità competenti, in particolare, ogni loro attività esterna, impiego, investimento, bene e ogni dono o vantaggio sostanziale dal quale potrebbero risultare un conflitto di interessi con le loro funzioni di pubblico ufficiale".

[77] Gruppo di Stati contro la corruzione, organo di controllo del Consiglio d'Europa, per la prevenzione e repressione dei fenomeni corruttivi, istituito nel 1999.

di interessi, disponendo altresì regole di trasparenza riguardanti i relativi compensi. Le informazioni relative a consulenze ed incarichi presenti nelle banche dati sono trasmesse e pubblicate dalle amministrazioni in tabelle riassuntive in formato aperto, in modo da permettere la libera consultazione e l'analisi anche a fini statistici. Nella stessa direzione sono orientati i commi 49 e 50, che prevedono l'adozione di una disciplina in materia di attribuzione di incarichi dirigenziali da conferire a soggetti interni ed esterni e della relativa responsabilità amministrativa, che rimuova possibili incompatibilità tra tali incarichi con quelli pubblici elettivi o con la titolarità di interessi privati in conflitto con la funzione pubblica.

Secondo quanto disciplinato dalla legge Severino del 2012 è il Governo che deve assolvere il compito di definire un codice di comportamento dei dipendenti delle Pubbliche Amministrazioni al fine di prevenzione dei fenomeni corruttivi, assicurare la qualità dei servizi e la tutela dell'interesse pubblico, nonché il rispetto dei doveri costituzionali di diligenza, lealtà, imparzialità[78]. Il codice di comportamento prevede una sezione specifica dedicata ai doveri dei dirigenti: in primis il divieto di accettare o chiedere, a qualsiasi titolo entro i limiti della propria funzione pubblica e per l'espletamento dei compiti loro affidati, compensi o altre utilità, con l'unica eccezione dei regali di cortesia, a patto che siano di modico valore[79]. La violazione dei doveri previsti nel codice di comportamento e nel Piano di prevenzione sono fonte di responsabilità disciplinare, potendo concludersi anche con il licenziamento per giusta causa o per giustificato motivo soggettivo, ovvero responsabilità civile, amministrativa e penale. Ciascuna Pubblica Amministrazione integra il codice predisposto dal Governo, con un proprio codice di comportamento specifico. Il rispetto di entrambi i codici viene fatto valere dai dirigenti responsabili di ogni amministrazione[80]. Si vuole, in tal modo, porre l'accento sulla responsabilità disciplinare del dipendente per violazione dei propri doveri professionali, conferendo, così, maggiore rilevanza all'etica pubblica, alla prevenzione interna all'amministrazione, alla specificazione dei doveri degli impiegati per tipologie di amministrazione e settori di intervento, nonché maggiore flessibilità degli strumenti di individuazione del conflitto di interessi. Difatti il codice di comportamento dovrebbe essere inteso esso stesso come strumento

[78] I commi 44 e 45 dell'art. 1 della legge n. 190 del 2012 hanno novellato l'art. 54 del d.lgs. n. 165 del 2001 in materia di codici di comportamento.

[79] Per modico valore si intende, ex art. 4 comma 5 del D.P.R. 62/2013, un bene di valore non superiore ad una cifra di 150 euro complessivi annui, ferma restando, per le singole amministrazioni, la possibilità di adottare limiti inferiori, fino a sancirne il totale divieto.

[80] In materia di codici di comportamento nell'Amministrazione pubblica, Carloni E., *I codici di comportamento*, in *Il lavoro nelle pubbliche Amministrazione*, riv. trim., Giappichelli, 2017.

dell'anticorruzione, e quindi come misura di prevenzione che costituisce la struttura fondamentale del nuovo impianto, insieme alle misure di trasparenza, alle incompatibilità ed al sistema dei piani anticorruzione, con i quali dialoga[81]. Ciò conferisce una prospettiva dinamica al codice di comportamento, che si adatta alla progressiva emersione di una dimensione prettamente organizzativo-gestionale dell'etica pubblica, strettamente legata alla prospettiva del miglioramento delle performance dell'amministrazione e alla riduzione delle situazioni di maladministration[82].

Una importante novella all'art. 53 del d.lgs. n. 165 del 2001, ha disciplinato per la prima volta in Italia il divieto di pantouflage, o revolving doors, con l'inserimento del comma 16 ter, il quale prevede che i dipendenti che negli ultimi tre anni di servizio hanno esercitato poteri autoritativi o negoziali per conto delle Pubbliche Amministrazioni non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati, destinatari dell'attività dell'amministrazione stessa. Il comma 51 introduce, poi, un'espressa tutela del c.d. whistleblower, ossia del dipendente pubblico che segnala illeciti di cui sia venuto a conoscenza durante lo svolgimento della propria attività lavorativa. Sempre in un'ottica di prevenzione alla corruzione e maladministration, la legge 190 del 2012 dispone l'esclusione dalle commissioni e dall'assegnazione di pubblici uffici di rilievo, di soggetti condannati, anche con sentenza non passata in giudicato, per delitti commessi dai pubblici dipendenti contro l'amministrazione.

Nonostante nella legge 190 del 2012 prevalga l'orientamento alla prevenzione degli illeciti contro la Pubblica Amministrazione, notevoli sono le modifiche della anche in ambito repressivo dei fenomeni corruttivi. Il comma 62 dell'art. 1, nel modificare la legge n. 20 del 1994, stabilisce che nel giudizio di responsabilità per danno all'immagine dell'amministrazione derivante dalla commissione di un reato accertato con sentenza passata in giudicato, l'entità del danno si presume pari al doppio del valore dell'utilità illecitamente percepita dal dipendente. In tali giudizi il sequestro conservativo è applicato in tutti i casi di fondato timore di attenuazione della garanzia del credito erariale. In ambito strettamente penalistico[83], la legge 190/2012 distingue la corruzione propria, relativa al compimento di un atto contrario ai doveri di ufficio del pubblico

[81] Cfr. Merloni F., *I piani anticorruzione e i codici di comportamento*, in *DPP*, 2013, 8S, 4 ss.
[82] Cfr. Carloni E., *I codici di comportamento*, in Il *lavoro nelle pubbliche amministrazioni*, 2017, p. 5 ss.
[83] Garofoli R., *La nuova disciplina dei reati contro la P.A.*, in *Diritto Penale Contemporaneo*, 2012, p. 3 ss.

ufficiale o mancato compimento di un atto del suo ufficio, dalla corruzione impropria, relativa alla ricezione indebita di denaro o altra utilità da parte del pubblico ufficiale per il compimento di un atto nell'esercizio delle sue funzioni. Viene, inoltre, ridefinito il reato di concussione, con l'introduzione della fattispecie autonoma di concussione per induzione (art. 319 quater c.p., induzione indebita a dare o ricevere utilità), e limitazione della concussione per costrizione al solo pubblico ufficiale o incaricato di pubblico servizio. L'art. 317 c.p., nella sua attuale formulazione, punisce difatti il reato di concussione solo nell'ipotesi di abuso costrittivo[84], con una pena particolarmente elevata, poiché esercitato mediante violenza o minaccia, esplicita o implicita che "genera grave limitazione della libertà di autodeterminazione"[85]. È stata, poi, aumentata la pena minima per il reato di peculato, per quello di abuso d'ufficio ed altre fattispecie, punita la corruzione fra privati con la pena detentiva da uno a tre anni, introdotta la nuova fattispecie di traffico di influenze illecite, ex art. 346 bis codice penale. Quest'ultima disposizione intende punire le condotte di intermediazione di soggetti terzi nell'attività di corruzione tra il corrotto ed il corruttore[86]. Infine, il comma 63 dell'art. 1 della legge Severino ha previsto l'emanazione del decreto legislativo n. 235 del 31.12.2012 in materia di incandidabilità, ineleggibilità ed automatica decadenza per i parlamentari, rappresentanti di governo, consiglieri regionali, sindaci e amministratori locali in caso di condanna per determinati reati contro la Pubblica Amministrazione[87].

Accanto alla legge 190 del 2012, la quale delinea l'impianto generale anticorruzione fondato principalmente sulla prevenzione, di particolare rilevanza è il d.lgs. n. 33 del 2013 in materia di trasparenza delle pubbliche amministrazioni[88]. Il decreto raffigura un nuovo rapporto fra

[84] Per l'art. 317 c.p. (concussione), così come novellato con legge n. 190 del 2012 e legge n. 69 del 2015 "il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità, è punito con la reclusione da sei a dodici anni".

[85] Cassazione, Sezioni Unite, sentenza n. 12228 del 2014.

[86] Per l'articolo 346 bis c.p. commi 1 e 2 "chiunque, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319-ter, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente fa dare o promettere, a sé o ad altri, denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo, in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio, è punito con la reclusione da uno a tre anni. La stessa pena si applica a chi indebitamente dà o promette denaro o altro vantaggio patrimoniale".

[87] Con referendum del 12 giugno 2022 è stata proposta l'abrogazione di tale disposizione, tuttavia la consultazione popolare ha dato esito negativo per il mancato raggiungimento del quorum, che si è fermato al di sotto del 20 per cento.

[88] D.lgs. n. 33 del 14 marzo 2013 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle Pubbliche Amministrazioni".

corruzione e digitalizzazione, soprattutto per ciò che riguarda la trasparenza nel settore pubblico, intesa non come fine, ma come strumento per il contrasto ai fenomeni corruttivi. Per l'art. 1, difatti, "La trasparenza è intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche". Si crea, così, una differente relazione fra Pubblica Amministrazione e cittadino, in cui è quest'ultimo ad effettuare un controllo capillare dal basso dell'attività amministrativa, e non viceversa. Tale controllo può essere garantito, in primis, con l'accesso libero di ogni soggetto ad atti e documenti dell'amministrazione. La normativa in parola va ben oltre la legge n. 241 del 1990, poiché intende la trasparenza come accessibilità totale e generalizzata ad ogni atto della Pubblica Amministrazione, e non come accesso limitato ad alcuni atti ed a soggetti dotati di particolari requisiti. Ciò in piena sintonia con i princìpi di trasparenza previsti dal Trattato sul Funzionamento dell'Unione Europea, secondo cui "al fine di promuovere il buon governo e garantire la partecipazione della società civile, le istituzioni, gli organi e gli organismi dell'Unione operano nel modo più trasparente possibile"[89].

Una delle più importanti innovazioni del decreto n. 33 è il diritto di accesso civico previsto all'articolo 5, con i soli limiti previsti dall'articolo 5 bis. Originariamente è stata introdotta la sola nozione di accesso civico, distinta da quella di accesso prevista dagli articoli 22 e seguenti della legge n. 241 del 1990. A differenza di quest'ultima, soggetta ad ampie limitazioni quali l'interesse del richiedente e l'obbligo di motivazione, il nuovo accesso civico consta nel diritto da parte di chiunque e senza motivazione, di richiedere dati e informazioni oggetto di pubblicazione obbligatoria da parte dell'amministrazione. A seguito delle modifiche introdotte con il d.lgs. n. 97 del 25 maggio 2016, vengono, poi, distinte due diverse forme di accesso civico: accesso civico "semplice", previsto dall'art. 5, comma 1, d.lgs. 33/2013 e accesso civico "generalizzato", previsto dall'art. 5, comma 2, d.lgs. 33/2013[90]. L'accesso civico semplice consiste nel diritto di chiunque di richiedere all'Amministrazione documenti, dati e informazioni per i quali sono previsti specifici obblighi normativi di pubblicazione nel caso in cui gli stessi non siano stati pubblicati. Riguardo

[89] Art. 15 TFUE, Trattato di Lisbona (ex art. 255 TCE).

[90] Sull'argomento, Foà S., *La nuova trasparenza amministrativa,* in *Diritto Amministrativo*, 2017, fasc. 1, pp. 65-99; Aveni A., *Il diritto di accesso agli atti nella pubblica amministrazione*, *aggiornato al D. Lgs. n. 97/2016 e alla giurisprudenza del febbraio 2018*, Editrice La Moderna, 2018; Ponti B. (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni. Commento sistematico al D.lgs. 33/2013 dopo le modifiche apportate dal D.lgs. 25 maggio 2016, n. 97*, Maggioli Editore, 2019.

l’accesso civico generalizzato, invece, il comma 2 dell’art. 5 novellato stabilisce che “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”. L’esercizio del diritto non è sottoposto ad alcuna limitazione quanto a legittimazione soggettiva del richiedente, pertanto l’accesso agli atti può essere effettuato da chiunque, anche persona non avente uno specifico interesse. L’istanza di accesso civico non richiede, inoltre, motivazione, e il rilascio dei dati è gratuito, salvo il rimborso del costo effettivo sostenuto dall’amministrazione per la riproduzione su supporti materiali. Per l’art. 5 bis, l’accesso civico è rifiutato se si rende necessario evitare pregiudizio alla tutela di interessi pubblici prevalenti rispetto alla trasparenza, ossia: sicurezza ed ordine pubblico; sicurezza nazionale; difesa e segreti militari; relazioni internazionali; stabilità finanziaria ed economica dello Stato; conduzione di indagini sui reati; regolare svolgimento di attività ispettive. Anche taluni interessi privati possono rappresentare un limite all’accesso civico generalizzato, ossia: la protezione dei dati personali; la libertà e la segretezza della corrispondenza; gli interessi economici, ivi compresi la proprietà intellettuale, il diritto d´autore e i segreti commerciali. In caso di diniego totale o parziale dell’accesso o di mancata risposta, il richiedente può presentare domanda di riesame al Responsabile della prevenzione della corruzione e della trasparenza, che decide con provvedimento motivato entro 20 giorni, o in alternativa può presentare ricorso al Difensore civico regionale che si pronuncia entro 30 giorni dal ricevimento dello stesso. In ogni caso, avverso la decisione dell’Amministrazione o, in caso di richiesta di riesame, avverso la decisione del Responsabile della prevenzione della corruzione e della trasparenza, è ammesso ricorso al Tribunale Amministrativo Regionale.

Il d.lgs. n. 33 del 2013, c.d. decreto trasparenza, prevede l’obbligo di pubblicazione sul portale dell’ente, in un’area aperta a tutti e secondo modalità di facile consultazione, della sezione dedicata all’amministrazione trasparente. I documenti e i dati oggetto di pubblicazione obbligatoria rimangono nella sezione denominata “amministrazione trasparente” per un periodo di cinque anni e comunque anche per un periodo di tempo maggiore, fin quando producono effetti, restando poi disponibili nella sezione dedicata all’archivio. L’obbligo di pubblicazione attiene a tutti i provvedimenti amministrativi, con particolare riferimento ad: autorizzazioni e concessioni; accordi dell’amministrazione con soggetti privati o altre amministrazioni; scelta del

contraente per l'affidamento di lavori; erogazione di contributi e sovvenzioni. L'obbligo di maggior rilevanza è, tuttavia, quello riguardante la pubblicazione di concorsi, gare d'appalto e prove selettive di assunzione. Solo tramite l'effettiva pubblicità dell'attività dell'amministrazione, che dovrà avvenire in forma sintetica, semplificata, chiara e aggregata, potrà essere favorito un controllo dal basso, da parte di chiunque, compresi coloro che non hanno particolari competenze tecnico-informatiche e amministrative. Ampia parte del decreto è dedicata alla trasparenza quale strumento per il contrasto alla corruzione negli appalti ed all'individuazione del conflitto di interessi, con particolare riguardo ai contratti pubblici di lavori, servizi e forniture (art. 37), realizzazione di opere pubbliche (art. 39), trasparenza del servizio sanitario nazionale (art. 41), interventi emergenziali che comportino deroghe alla legislazione vigente (art. 42)[91].

Per assicurare la trasparenza viene rafforzata la vigilanza, a livello centrale posta in essere dall'ANAC, e a livello diffuso con l'individuazione da parte dell'amministrazione di un Responsabile della prevenzione della corruzione e della trasparenza (RPCT), il quale ha l'onere di verificare sistematicamente l'adempimento degli obblighi di pubblicazione previsti dalla normativa e segnalare i casi di inadempimento, nonché assicurare la regolare attuazione dell'accesso civico, secondo quanto previsto dall'art. 43 del decreto. L'attuazione degli obblighi di trasparenza dell'amministrazione rileva quale elemento di valutazione delle performance dell'ufficio, sia a livello collettivo che personale (art. 44). Altri compiti sono riconosciuti all'OIV, Organismo indipendente di valutazione, cui spetta verificare la coerenza degli obiettivi riguardanti la trasparenza.

Con l'entrata in vigore del Codice della trasparenza del 2013 si è avuto il riordino in un corpo normativo unitario, in attuazione a quanto previsto dalla legge anticorruzione del 2012, delle disposizioni riguardanti gli obblighi di pubblicità e trasparenza delle amministrazioni. Tale riordino si è reso necessario allo scopo di evitare i frequenti casi di sovrapposizione normativa, nonché di semplificare e rafforzare le regole riguardanti gli obblighi di pubblicazione. Per dare maggiore concretezza ai vincoli imposti alle Pubbliche Amministrazioni, è inoltre stato disciplinato il regime sanzionatorio e delle responsabilità per l'inadempimento degli obblighi di pubblicazione. I problemi applicativi del decreto, hanno tuttavia evidenziato numerose criticità[92], in particolare

[91] Cantone R., Merloni F., *Codice dell'anticorruzione e della trasparenza*, Maggioli, 2018, p. 16 ss.

[92] Già nell'aprile 2014 l'ANAC trasmette al Governo un documento sui problemi in materia di prevenzione della corruzione, trasparenza e performance e proposte di semplificazione, individuando un elenco di punti critici della

riguardanti la sostenibilità amministrativa di una disciplina uniforme applicata ad enti estremamente diversificati, nonché le difficoltà di adeguamento delle amministrazioni ai nuovi istituti. Si è reso, pertanto, necessario un nuovo intervento in materia di trasparenza, che semplificasse e rendesse più agevole l'applicazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza. Su delega della c.d. legge Madia[93] viene, così, varato il d.lgs. n. 97 del 2016 che, fermo restando il diritto di accesso civico c.d. semplice, introduce l'accesso civico generalizzato sul modello del Freedom of Information Act statunitense, basato sulla facoltà da parte di chiunque di accedere alle informazioni detenute dalle pubbliche amministrazioni, con i soli limiti ed eccezioni tassativamente previsti dalla legge, secondo un esempio tipicamente anglosassone di *total disclosure*. Secondo tale modello le Amministrazioni Pubbliche detengono un patrimonio informativo comune che, come tale, deve essere accessibile a tutte le persone e la cui disponibilità è funzionale al rafforzamento della trasparenza amministrativa[94], al fine di favorire forme diffuse di controllo ed una più efficace azione di contrasto alle condotte illecite nel settore pubblico. Obiettivo primario della riforma è di rafforzare la partecipazione dei privati alla gestione della cosa pubblica tramite un controllo dal basso, al fine di riaffermare quei principi di legalità e imparzialità che devono sempre essere alla base dell'agire pubblico, nonché migliorare l'efficienza dell'amministrazione contrastando i fenomeni di non corretta gestione delle risorse pubbliche.

Il decreto del 2016 introduce una nuova disciplina sugli obblighi di trasparenza riguardanti i titolari di incarichi politici. Al riguardo l'ANAC ha emanato linee guida per l'attuazione di tali obblighi[95]. Sono state, poi, disposte misure di semplificazione in materia di pubblicità da parte dell'amministrazione, fra cui la possibilità di sostituire la pubblicazione di informazioni con il libero accesso alle banche dati e la soppressione dell'obbligo di adottare il Piano triennale per la trasparenza e l'integrità. Per quanto attiene alle banche dati, le amministrazioni che ne sono titolari pubblicano le informazioni in esse contenute corrispondenti agli obblighi di pubblicazione, ovvero il relativo collegamento ipertestuale, ferma restando la possibilità di continuare a

legge n. 190 del 2012 e soprattutto della n. 33 del 2013 (ANAC, Rapporto sul primo anno di attuazione della legge 6 novembre 2012, n. 190, 27 dicembre 2013, doc. XXVII, n. 8, p. 48).

[93] Legge n. 124 del 7 agosto 2015, recante "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche".

[94] In conformità con l'art. 10 CEDU che, secondo un'interpretazione estensiva operata dalla Corte europea dei diritti dell'uomo (Szabadságjogokért vs. Hungary, 14 April 2009, punto 35) considera il diniego di accesso ai documenti amministrativi un'interferenza nel diritto di ricevere informazioni.

[95] ANAC, delibera dell'8 marzo 2017.

pubblicare sul proprio sito i predetti dati purché identici a quelli comunicati alla banca dati. Per ciò che riguarda la soppressione del Piano triennale per la trasparenza e l'integrità, questo viene inglobato nel Piano della prevenzione della corruzione (PTPC). Vi è da aggiungere che gli obblighi di pubblicazione concernenti i componenti degli organi di indirizzo politico, si estendono anche a cariche non elettive e ad incarichi amministrativi e direttivi. È, difatti, previsto l'obbligo di pubblicazione da parte dell'amministrazione, di informazioni concernenti i titolari di incarichi politici, di amministrazione o di governo, dirigenziali ma con l'estensione anche ad incarichi non dirigenziali, sia dell'atto di conferimento dell'incarico che del curriculum vitae, ed anche dei compensi percepiti. Negli atti di conferimento di incarichi dirigenziali e nei relativi contratti sono riportati gli obiettivi di trasparenza, finalizzati a rendere i dati pubblicati di immediata comprensione e consultazione per il cittadino. In tema di pubblicazione dei bandi di concorso, il legislatore è intervenuto con l'introduzione dell'obbligo di pubblicare anche i criteri di valutazione della Commissione delle prove scritte. Si ha, invece, una semplificazione, con riguardo a premi e incentivi di dirigenti e dipendenti, con obblighi di pubblicazione solo in forma aggregata, al fine di tutelare il dato personale. Sempre in un'ottica di semplificazione non vi è più l'obbligo di pubblicare i provvedimenti concernenti autorizzazioni o concessioni, nonché quelli relativi a concorsi e selezioni, quelli di pubblicazione sulle attività amministrative e controlli sulle imprese, gli obblighi relativi ai dati degli organi di controllo, ed il riferimento al nome del responsabile del procedimento, poiché sarà sufficiente indicare l'ufficio.

La pubblicità delle informazioni, sulla quale il decreto è basato non deve, tuttavia, ledere il diritto alla tutela dei dati personali, pertanto "Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione"[96].

Il d.lgs. n. 97 del 2016 ossia il c.d. FOIA, Freedom of Information Act, interviene, altresì, sul ruolo dell'Autorità anticorruzione ampliandone il potere di vigilanza e sanzionatorio in materia di trasparenza dell'amministrazione. Alle linee guida dall'ANAC sono, difatti, demandate le sanzioni e la regolamentazione di alcuni aspetti della riforma. Viene, così, rafforzato il ruolo degli atti di *soft law* emanati dall'Autorità, atti di indirizzo di livello generale[97]. La normativa lascia, tuttavia,

[96] D.lgs. n. 33/2013 art. 7-bis, co. 4, introdotto dall'art. 7 del d.lgs. n. 97 del 2016.
[97] Aventi validità erga omnes ai sensi della legge n. 400 del 1988.

colpevolmente aperte alcune questioni in materia di riuso dei dati pubblicati (open data), indicizzazione e rintracciabilità degli stessi. Ciò necessita di chiarimenti applicativi, mai avvenuti, rispetto al diritto alla privacy e al bilanciamento degli interessi nel caso di accesso civico generalizzato.

Il d.lgs. n. 39 del 2013[98] stabilisce una serie articolata di cause di inconferibilità e incompatibilità con riferimento ad incarichi amministrativi di vertice, dirigenziali o di responsabilità, nelle Pubbliche Amministrazioni e negli enti di diritto privato a controllo pubblico. Per inconferibilità si intende la preclusione, permanente o temporanea, a conferire gli incarichi a coloro che abbiano riportato condanne penali, anche non definitive[99], per determinati reati contro la Pubblica Amministrazione, a coloro che abbiano svolto incarichi, attività professionali o ricoperto cariche presso enti di diritto privato regolati o finanziati da Pubbliche Amministrazioni, ovvero a coloro che siano stati componenti di organi di indirizzo politico. L'approccio della normativa è di distinguere i ruoli di funzionari burocratici e di indirizzo politico, con regole di inconferibilità dei poteri a determinati soggetti in conflitto di interessi. Non potranno, pertanto, essere conferiti incarichi dirigenziali o di responsabilità in enti pubblici a chi ha recentemente ricoperto incarichi politici. Nella stessa logica volta a prevenire eventuali conflitti di interessi, viene previsto un periodo di raffreddamento per quegli incarichi provenienti da soggetti privati con cui l'amministrazione ha rapporti contrattuali continuati e costanti. La vigilanza sull'osservanza delle norme in materia di inconferibilità e incompatibilità è demandata al responsabile della prevenzione, della corruzione e della trasparenza e all'Autorità nazionale anticorruzione. Il primo ha il compito di contestare la situazione di inconferibilità o incompatibilità e di segnalare la violazione all'ANAC, che procede all'accertamento di singole e specifiche fattispecie di conferimento degli incarichi. Il potere di accertamento dell'ANAC può, tuttavia, essere attivato anche su segnalazione di terzi, ovvero in occasione della richiesta di pareri da parte delle amministrazioni, o infine d'ufficio.

Il D.P.R. n. 62 del 2013 è un regolamento che disciplina il codice di comportamento dei dipendenti pubblici. Il d.lgs. n. 165 del 30 marzo 2001 novellato dal comma 44 art. 1 della legge n. 190 del

[98] Decreto legislativo del 08.04.2013 n. 39 recante "Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190".

[99] La situazione di inconferibilità cessa di diritto ove venga pronunciata, per il medesimo reato, sentenza anche non definitiva, di proscioglimento.

2012 prevede la definizione di un codice di comportamento per i dipendenti delle Pubbliche Amministrazioni al fine di assicurare la qualità dei servizi, la prevenzione dei fenomeni corruttivi e del conflitto di interessi, il rispetto dei doveri costituzionali di diligenza, lealtà, imparzialità e la dedizione all'esclusiva cura dell'interesse pubblico. Con una chiara presa di posizione opposta rispetto al passato, la l. n. 190/2012 chiarisce che la violazione delle regole del codice generale approvato con D.P.R. nel 2013 e dei codici adottati da ciascuna amministrazione dà luogo a responsabilità disciplinare. Un'intera sezione del codice di comportamento è dedicata esclusivamente ai doveri e agli obblighi dei dirigenti.

Il codice, approvato con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro per la pubblica amministrazione e la semplificazione, viene consegnato al dipendente, che lo sottoscrive all'atto dell'assunzione. Per l'ANAC "l'adozione del codice di comportamento da parte di ciascuna amministrazione rappresenta una delle 'azioni e misure' principali di attuazione delle strategie di prevenzione della corruzione a livello decentrato, secondo quanto indicato nel Piano nazionale anticorruzione"[100]. Esso rappresenta un elemento strategico primario e fondamentale del Piano triennale per la prevenzione della corruzione di ogni amministrazione.

L'art. 4 del codice prevede, per tutti i dipendenti pubblici il divieto di chiedere o di accettare, a qualsiasi titolo, compensi, regali o altre utilità, in connessione con l'espletamento delle proprie funzioni o dei compiti affidati, fatti salvi i regali d'uso, purché di modico valore e nei limiti delle normali relazioni di cortesia e consuetudini internazionali. In ogni caso, indipendentemente dalla circostanza che il fatto costituisca reato, il dipendente pubblico non può chiedere per sé o per altri, regali o altre utilità, neanche di modico valore a titolo di corrispettivo per compiere o per aver compiuto un atto del proprio ufficio, da soggetti che possano trarre benefici da decisioni o attività inerenti all'ufficio, né da soggetti nei cui confronti è chiamato a svolgere attività o potestà proprie dell'ufficio ricoperto. Il dipendente non può accettare, neppure da un proprio subordinato, regali o altre utilità, salvo quelli d'uso di modico valore, e non può offrirli neanche ad un proprio sovraordinato. Per regali o altre utilità di modico valore si intendono quelli di valore non superiore, orientativamente, ad euro 150. Di particolare rilevanza, ai fini della trasparenza dell'amministrazione, è il comma 6 dell'art. 4, per il quale al fine di evitare qualsivoglia conflitto

[100] Delibera numero 75/2013 Linee guida ANAC.

di interessi il dipendente non può accettare incarichi di collaborazione da soggetti privati che abbiano, o abbiano avuto nel biennio precedente, un interesse economico significativo in decisioni o attività inerenti all'ufficio di appartenenza. Al personale delle pubbliche amministrazioni sono, poi, rivolte attività formative in materia di trasparenza e integrità, che consentano ai dipendenti di conseguire una piena conoscenza dei contenuti del codice di comportamento, nonché un aggiornamento annuale e sistematico sulle misure, sulle disposizioni e sulle sanzioni applicabili in tali ambiti. Nel rispetto del diritto di associazione, il dipendente ha l'obbligo di comunicare tempestivamente al responsabile dell'ufficio di appartenenza, la propria adesione ad associazioni od organizzazioni i cui ambiti di interesse possano interferire con lo svolgimento dell'attività dell'ufficio.

Gli articoli 6 e 7 riguardano il conflitto di interessi, il dovere di segnalazione di interessi e l'obbligo di astensione. Per l'art. 6 il dipendente, all'atto dell'assegnazione, deve informare per iscritto il dirigente dell'ufficio di tutti i rapporti di collaborazione, diretti o indiretti, con soggetti privati che lo stesso abbia o abbia avuto negli ultimi tre anni. Il dipendente si astiene dal prendere decisioni o svolgere attività inerenti alle sue mansioni in situazioni di conflitto, anche potenziale, con interessi personali, del coniuge, di conviventi, di parenti, di affini entro il secondo grado. Il conflitto può riguardare interessi anche non patrimoniali, come quelli derivanti dall'intento di voler assecondare pressioni attuate dai superiori gerarchici. Per l'art. 7, invece, il dipendente ha un obbligo di astensione dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri, ovvero di suoi parenti, affini entro il secondo grado, del coniuge o di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, ovvero, di soggetti od organizzazioni con cui egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito significativi, società di cui sia amministratore o dirigente, e comunque deve astenersi in ogni altro caso in cui esistano gravi ragioni di convenienza. L'art. 8, rubricato "Prevenzione della corruzione", richiede il rispetto del piano per la prevenzione della corruzione e la collaborazione con il RPCT, conferendo particolare rilievo al c.d. whistleblowing, ossia l'obbligo di segnalazione e denuncia di comportamenti illeciti di cui il dipendente dell'amministrazione sia venuto a conoscenza. Per l'art. 8 "Il dipendente rispetta le misure necessarie alla prevenzione degli illeciti nell'amministrazione. In particolare, il dipendente rispetta le prescrizioni contenute nel piano per la prevenzione della corruzione, presta la sua collaborazione al responsabile della prevenzione della corruzione e, fermo restando l'obbligo di denuncia all'autorità giudiziaria, segnala al proprio superiore gerarchico eventuali situazioni di

illecito nell'amministrazione di cui sia venuto a conoscenza". Con riferimento alla trasparenza, l'art. 9 stabilisce che il dipendente debba assicurare l'adempimento degli obblighi di trasparenza, prestando la massima collaborazione nell'elaborazione, reperimento e trasmissione dei dati sottoposti all'obbligo di pubblicazione sul sito istituzionale. La tracciabilità dei processi decisionali adottati dai dipendenti deve essere, in tutti i casi, garantita attraverso un adeguato supporto documentale, che consenta in ogni momento la replicabilità.

Il d.l. n. 90 del 24 giugno 2014 facente parte della c.d. riforma Madia e recante misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari, amplia gli incarichi dell'ANAC chiamandola a svolgere funzioni di vigilanza, garanzia e trasparenza riguardo specifici avvenimenti ed attività di particolare rilevanza (quali ad esempio l'Expo e le ricostruzioni post terremoto), prevenzione della corruzione all'interno delle amministrazioni e di società partecipate e controllate, attraverso l'attuazione della trasparenza, grazie anche ai poteri di orientamento dei comportamenti e delle attività degli impiegati pubblici. In tale contesto di allargamento dei poteri dell'Autorità Anticorruzione, il decreto dispone l'abolizione dell'Autorità per la vigilanza sui contratti pubblici (AVPC) e trasferisce le funzioni relative all'ANAC, e soprattutto introduce misure di gestione, sostegno e monitoraggio "delle imprese nell'ambito della prevenzione della corruzione". È, quest'ultimo, un meccanismo di commissariamento degli appalti ottenuti in modo illecito, finalizzato a garantire il pubblico interesse al completamento di opere.

Le funzioni di vigilanza e di controllo effettivo, non meramente burocratico e formalistico, divengono il criterio di orientamento dell'intera azione dell'Autorità, in particolare nella prevenzione della corruzione nelle Amministrazioni Pubbliche, nelle società partecipate e controllate, anche mediante l'attuazione della trasparenza, nonché mediante attività di vigilanza nell'ambito dei contratti pubblici e incarichi, evitando al contempo di aggravare i procedimenti con ricadute negative sui cittadini e sulle imprese. Il decreto legge del 2014, inoltre, al fine di evitare conflitti di interessi, vieta l'assegnazione di incarichi dirigenziali a lavoratori privati o pubblici collocati in quiescenza, stabilendo altresì che i magistrati non potranno ricoprire incarichi dirigenziali nella pubblica amministrazione facendo ricorso all'istituto dell'aspettativa.

Di particolare rilevanza è il titolo III "Misure urgenti per l'incentivazione della trasparenza e correttezza delle procedure nei lavori pubblici", che prevede nuove misure di controllo preventivo

contro i fenomeni corruttivi, soprattutto da parte dell'ANAC, con particolare riferimento ai grandi eventi[101], e misure straordinarie di gestione, sostegno e monitoraggio nell'ambito della prevenzione alla corruzione. In presenza di situazioni anomale o sintomatiche di condotte illecite attribuibili ad un'impresa aggiudicataria di un appalto per la realizzazione di opere pubbliche, servizi o forniture, ovvero che esercita attività sanitaria per conto del Servizio sanitario nazionale, il Presidente dell'ANAC informa il Procuratore della Repubblica e, se sussistono fatti gravi e accertati, propone al Prefetto competente del luogo in cui ha sede la stazione appaltante, di ordinare la rinnovazione degli organi sociali mediante la sostituzione del soggetto coinvolto e, ove non vi sia adeguamento nei termini stabiliti, di provvedere direttamente alla straordinaria e temporanea gestione dell'impresa, limitatamente alla completa esecuzione del contratto. È, questo, un passaggio fondamentale del decreto in materia di anticorruzione, poiché impone la sostituzione dei soggetti coinvolti in vicende corruttive o il commissariamento dell'impresa, senza creare nocumento alla puntuale realizzazione dell'opera pubblica. Altri punti importanti riguardano il monitoraggio finanziario dei lavori concernenti infrastrutture strategiche, e la trasmissione all'ANAC delle varianti in corso d'opera relative ad opere pubbliche.

Con la legge n. 3 del 2019, la c.d. Spazzacorrotti, intitolata "Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici", il legislatore ha riformato, in un'ottica di contrasto alla corruzione, la materia dei delitti contro la Pubblica Amministrazione e la disciplina extrapenale sulla trasparenza e controllo di partiti e movimenti politici. La legge rafforza il contrasto dei reati contro la Pubblica Amministrazione con misure di inasprimento sia delle pene principali che accessorie, limitazione ai benefici nell'esecuzione della pena, maggior efficacia delle indagini e strumenti più solidi forniti agli inquirenti. I condannati per reati corruttivi non possono più accedere a misure alternative alla detenzione se non collaborano con la giustizia[102]. Pertanto, in presenza di condanne per i reati in questione, anche ove la pena residua sia uguale o inferiore a quattro anni, sarà emesso ordine di esecuzione per la carcerazione, senza decreto di sospensione. Per poter accedere ai benefici, la collaborazione prestata deve essere utile, concreta

[101] Nello specifico l'Expo di Milano 2015.

[102] L'art. 4 bis dell'ordinamento penitenziario, così come riformulato dall'art. 1 della Legge n. 3 del 2019, prevede che "L'assegnazione al lavoro all'esterno, i permessi premio e le misure alternative alla detenzione previste dal capo VI, esclusa la liberazione anticipata, possono essere concessi ai detenuti e internati" per i delitti di cui agli "artt. 314, primo comma, 317, 318, 319, 319 bis, 319 ter, 319 quater, primo comma, 320, 321, 322, 322 bis" solo nei casi in cui detenuti e internati per tali delitti, collaborino con la giustizia a norma dell'articolo 58 ter ord. penit. o a norma dell'articolo 323-bis, secondo comma, del codice penale.

e rilevante. Viene, poi, potenziato il perseguimento dei reati corruttivi all'estero ed ampliato l'ambito applicativo dei delitti di corruzione internazionale dei pubblici agenti, esteso anche ai funzionari "extra-Ue", ai membri delle assemblee parlamentari internazionali ed ai giudici e funzionari delle corti internazionali. La legge n. 3 consente, inoltre, di mantenere la confisca dei beni in caso di estinzione del reato per amnistia o per prescrizione, e prevede per i delitti di corruzione fra privati e istigazione alla corruzione fra privati la procedibilità d'ufficio. Viene, infine, aumentata la possibilità per gli organi inquirenti di avvalersi delle intercettazioni e di effettuare operazioni sotto copertura.

L'inserimento dei delitti contro la Pubblica Amministrazione in normative appositamente create per il contrasto alle forme più pericolose di criminalità organizzata, è prefigurato dalla previsione dei delitti di corruzione nel c.d. codice antimafia[103]. Vengono aumentate le pene per i reati di corruzione per l'esercizio della funzione ex art. 318 c.p. dalla reclusione compresa nella cornice edittale fra 1-6 anni a 3-8 anni, di appropriazione indebita ex art. 646 c.p. dalla reclusione fino a 3 anni e multa fino a euro 1032 alla reclusione da 2 a 5 anni e multa da 1.000 a 3.000 euro, di indebita percezione di erogazioni a danno dello Stato ex art. 316-ter c.p., con una pena aggravata nel caso in cui a commetterlo sia un pubblico ufficiale o un incaricato di un pubblico servizio che abusi dei suoi poteri, con la reclusione compresa fra 1 e 4 anni. Oltre ad un aumento delle pene principali per i reati di corruzione, vengono inasprite le pene accessorie: l'interdizione dai pubblici uffici e incapacità di contrattare con la P.A. divengono perpetue in caso di condanne superiori a due anni di reclusione, la riabilitazione non produce effetti sulle pene accessorie perpetue, l'incapacità di contrattare con la P.A. può essere applicata all'imputato prima della condanna. È prevista una causa di non punibilità per chi collabora con la giustizia, purché vi sia confessione spontanea da parte dell'interessato. Difatti, per l'art. 323 ter c.p. (Causa di non punibilità), "Non è punibile chi ha commesso taluno dei fatti previsti dagli articoli 318, 319, 319-ter, 319-quater, 320, 321, 322-bis, limitatamente ai delitti di corruzione e di induzione indebita ivi indicati, 353, 353-bis e 354 se, prima di avere notizia che nei suoi confronti sono svolte indagini in relazione a tali fatti e, comunque, entro quattro mesi dalla commissione del fatto, lo denuncia volontariamente e fornisce indicazioni utili e concrete per assicurare la prova del reato e per individuare gli altri responsabili". La non punibilità è subordinata alla messa a disposizione

[103] D.lgs. 6 settembre 2011, n. 159 e ss.mm.

dell'utilità dallo stesso percepita o, in caso di impossibilità, di una somma di valore equivalente, ed all'indicazione di elementi utili e concreti per individuarne il beneficiario effettivo.

Il millantato credito viene abrogato come fattispecie autonoma di reato, ed inglobato nel delitto di traffico di influenze illecite. La riforma operata dalla Spazzacorrotti introduce il regime della procedibilità d'ufficio per le fattispecie di corruzione e di istigazione alla corruzione tra privati, abrogando la parte della norma che prevedeva la procedibilità su querela di parte per i suddetti illeciti. La disposizione si uniforma alle direttive sovranazionali che impongono agli Stati membri UE di adottare tutte le misure necessarie per contrastare la corruzione, anche tra privati, percepita come uno strumento di alterazione della concorrenza. Tale scelta sposta l'oggetto della tutela penale verso interessi di carattere marcatamente pubblicistico.

Per ciò che concerne la trasparenza dei partiti, dei movimenti politici e delle fondazioni politiche, la Spazzacorrotti ha introdotto una serie di norme stringenti sulle donazioni ed essi destinate, al fine di favorire maggiore trasparenza ed impedire giri di denaro occulti e situazioni di conflitto. La legge ha previsto anche l'obbligo nei confronti di partiti e movimenti politici, di pubblicare sul sito internet i contributi ricevuti nonché, prima della consultazione elettorale, il curriculum vitae dei candidati e il relativo certificato penale rilasciato dal casellario giudiziale.

La legge *de qua* è fondata sull'assunto che l'effettività della risposta sanzionatoria non corrisponda unicamente alla fattispecie incriminatrice, ma sia elemento essenziale la fase investigativa ed i relativi strumenti di cui dispongono gli inquirenti[104]. Sul fronte del rafforzamento delle indagini, oltre ad estendere il campo d'azione delle operazioni di polizia sotto copertura, nei procedimenti per delitti contro la Pubblica Amministrazione sono consentite le intercettazioni anche per reati di minore gravità ed anche mediante software, quali i c.d. trojan[105]. Nello specifico, vengono estese le fattispecie di reato per cui sono consentite le intercettazioni, previste dall'art. 266 c.p.p., i presupposti sono meno rigorosi, i termini più ampi, e le modalità operative più agili. Maggiore libertà d'azione hanno altresì, con la nuova normativa, gli agenti sotto copertura, i quali possono inserirsi in un contesto di fatto costituente reato già commesso o del

[104] Nel D.D.L. della c.d. Spazzacorrotti si legge "l'effettività di un'incriminazione dipende non solo dalla formulazione delle fattispecie incriminatrici e dall'entità della pena edittale, ma anche dagli strumenti d'indagine e dai poteri di accertamento che l'ordinamento mette a disposizione degli organi inquirenti e dell'autorità giudiziaria per perseguire efficacemente i reati".

[105] Captatori informatici inoculati su dispositivi elettronici portatili. Sull'utilizzo dei trojan nelle indagini, Antonucci M. (a cura di), *Copia forense e trojan*, NEU, 2017, p. 16 ss.

quale si sono create le condizioni. Tuttavia l'ufficiale di polizia giudiziaria sotto copertura non può sollecitare la commissione di un reato, tramite attività inerenti la figura del c.d. agente provocatore[106].

Ad oltre tre anni dalla sua entrata in vigore, innumerevoli sono le critiche alla Spazzacorrotti. In primis essa privilegia, a differenza delle più importanti normative anticorruzione dell'ultimo decennio (quali la n. 190 del 2012, la n. 33 del 2013 e il d.lgs. n. 97 del 2016), le misure di tipo repressivo, a discapito dell'attività di prevenzione di natura amministrativa, che ha prodotto rilevanti effetti positivi sulla corruzione in Italia a partire dal 2012. Dubbi di costituzionalità della legge riguardano la presunzione assoluta di pericolosità dei reati contro la Pubblica Amministrazione, inseriti fra i reati di allarme sociale previsti ex art. 4-bis comma 1 ordinamento penale. Sotto il profilo del divieto di retroattività della legge penale sfavorevole, si lamenta l'assenza di una disciplina transitoria che limiti l'applicabilità della legge n. 3 del 2019 ai fatti commessi dopo la sua entrata in vigore. Gli effetti retroattivi riguardano principalmente la cancellazione della sospensione dell'ordine di esecuzione e carcere obbligatorio con divieto di accesso ai benefici esterni, a meno di non collaborare con la giustizia, per coloro che hanno commesso reati anche prima dell'entrata in vigore della legge.

1.2.2. Il whistleblowing

In un'ottica di prevenzione dei fenomeni corruttivi, particolare risonanza ha avuto l'introduzione nell'ordinamento della regolamentazione del c.d. whistleblowing, ossia la disciplina del comportamento e le norme a tutela dei dipendenti pubblici ed in generale di coloro che segnalano irregolarità e condotte illecite nella Pubblica Amministrazione e nell'ambito lavorativo privato, di cui siano venuti a conoscenza in ragione della propria attività[107]. La *ratio* di tale tutela offerta al segnalante (c.d. whistleblower) consta nella necessità di garantire quest'ultimo dal rischio di ritorsioni da parte del datore di lavoro o superiori gerarchici, incentivando in tal modo la segnalazione degli illeciti. Oltre agli indubbi effetti positivi del whistleblowing riguardanti il

[106] Cfr. Tescaroli L., *La cd. legge spazzacorrotti: analisi e problematiche delle novità sostanziali e processuali della legge n. 3 del 2019*, in *Questione giustizia – magistratura democratica*, settembre 2019.

[107] Sul punto, Naddeo A., *Il whistleblowing. Nuovo strumento di lotta alla corruzione*, in Fraschini G., Parisi N., Rinoldi D., Roma, 2009, p. 10 e ss, il quale fornisce la definizione di whistleblowing quale "istituto giuridico volto a disciplinare la condotta di quelle persone che segnalano irregolarità o addirittura illeciti penali all'interno del proprio ambito lavorativo".

consolidamento di un'etica della legalità, non trascurabile è l'effetto deterrente dovuto al rischio di essere segnalati e posti sotto indagine, ovvero subire provvedimenti disciplinari[108].

Oggetto del whistleblowing sono tutti quei comportamenti illeciti, illegittimi, scorretti ovvero censurabili. Possono, pertanto, essere segnalati dal whistleblower non solo gli atti illeciti, ma anche tutti quei comportamenti impropri commessi dal dipendente che, anche al fine di curare un interesse proprio o di terzi, devia dalla cura dell'interesse pubblico. La segnalazione non si configura come un obbligo, bensì come un diritto. Gli enti pubblici e le aziende hanno, tuttavia, la facoltà di prevedere l'obbligo per i propri dipendenti di segnalare eventuali illeciti di cui siano venuti a conoscenza. La segnalazione di determinati illeciti si configura, invece, sempre come un obbligo per i pubblici ufficiali o incaricati di pubblico servizio, poiché l'art. 331 c.p.p. sancisce un vero e proprio obbligo di denuncia del reato procedibile d'ufficio di cui essi siano venuti a conoscenza nell'esercizio delle proprie funzioni.

La disciplina sul whistleblowing è stata introdotta in Italia con la Legge Severino, l. n. 190 del 2012[109] intitolata "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" con l'art. 1 comma 51 che ha aggiunto al d.lgs. 165/2001 l'articolo 54 bis (Tutela del dipendente pubblico che segnala illeciti) in base al quale "il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui è venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. Nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato". Se l'ANAC ritiene la segnalazione fondata nei termini chiariti dalla Delibera n. 469 del 9 giugno 2021 "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)" in un'ottica di

[108] L'effetto deterrente del whistleblowing è ampiamente analizzato in J.H. Wilde, *The deterrent effect of employee whistleblowing on firm's financial misreporting and tax aggressiveness, in the accounting review*, september 2017, vol. 92, n. 5, p. 247 ss.

[109] In realtà il whistleblowing era già previsto dall'art. 54 bis del decreto legislativo 165 del 2001, ma non aveva avuto seguito in quanto mancava un sistema effettivo di tutele per il dipendente che segnalava illeciti.

prevenzione della corruzione, può avviare un'interlocuzione con il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell'amministrazione oggetto di segnalazione, ovvero disporre l'invio della segnalazione alle istituzioni competenti, quali l'Ispettorato per la Funzione Pubblica, la Corte dei conti, l'Autorità giudiziaria, la Guardia di Finanza. Nonostante la rilevanza della legge n. 190 del 2012, prima normativa sulla tutela dei segnalatori di illeciti, nella sua formulazione originaria alcune disposizioni apparivano ambigue[110], tuttavia le successive modifiche e le linee guida dell'ANAC, nonché i codici di comportamento delle amministrazioni hanno chiarito i punti più controversi.

Nel 2017 entra in vigore la legge n. 179, interamente dedicata al whistleblowing[111], per una tutela organica e completa di coloro che segnalano illeciti o irregolarità sul luogo di lavoro, ampliando e rafforzando le garanzie già previste dalla legge Severino. Oltre a vietare qualsiasi provvedimento conseguente alla segnalazione avente effetti negativi per il segnalante, essa sanziona con la nullità ogni atto discriminatorio o ritorsivo adottato dall'amministrazione contro colui che segnala le irregolarità. Punto centrale della normativa è, però, l'estensione di determinate tutele del whistleblower, anche nel settore privato. La nuova disciplina sul whistleblowing viene estesa, difatti, dalle amministrazioni pubbliche, enti pubblici economici e di diritto privato sotto controllo pubblico, anche alle imprese private[112]. Le nuove norme stabiliscono che il dipendente che segnala abusi o condotte illecite non può essere soggetto a sanzioni disciplinari, trasferito, demansionato, ed in caso di licenziamento conseguente alla segnalazione dovrà essere reintegrato nel posto di lavoro. L'eventuale licenziamento viene infatti annoverato fra quelli discriminatori e ritorsivi, per i quali è prevista la reintegrazione, nonché un'indennità risarcitoria pari alla retribuzione spettante al lavoratore nel periodo che intercorre fra il licenziamento e l'effettiva reintegrazione. Per gli atti discriminatori viene, inoltre, applicata all'ente ed al responsabile una sanzione, fermi restando altri profili di responsabilità[113]. L'adozione di misure discriminatorie è segnalata al Dipartimento della funzione pubblica, per i provvedimenti di competenza, dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative

[110] La stessa ANAC nella relazione annuale 2014 ribadiva le criticità riguardanti la segnalazione al superiore gerarchico, la riservatezza del segnalante, la tutela del whistleblower negli enti pubblici economici.
[111] Legge 30 novembre 2017, n. 179 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".
[112] L'art. 1 della legge n. 179 del 2017 disciplina la tutela del dipendente pubblico che segnala illeciti, mentre l'art. 2 disciplina la tutela del dipendente o del collaboratore che segnala illeciti nel settore privato.
[113] Cfr. Rugani A., *I profili penali del whistleblowing alla luce della l. 30 novembre 2017 n. 179,* in *Legislazione penale,* 2018.

nell'amministrazione nella quale le stesse sono state poste in essere, RSA o RSU. Viene, poi, tutelata la segretezza e riservatezza dell'identità del denunciante. La segnalazione è sottratta all'accesso agli atti previsto ex art. 22 e ss. della l. n. 241 del 1990 e successive modifiche. Anche nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata senza il suo consenso. Qualora la contestazione sia fondata, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato. Tra le novità della nuova normativa, da rilevare l'introduzione, all'art. 3, di una disciplina che coordina il whistleblowing con l'obbligo del segreto d'ufficio, professionale, industriale ed aziendale, mettendo al riparo il segnalatore di illeciti da responsabilità civile o penale[114], con la previsione di una giusta causa di rivelazione[115].

Con l'entrata in vigore della Legge n. 179 del 2017 è stato introdotto l'obbligo per le amministrazioni e le imprese private, di attivare al proprio interno canali di segnalazione delle violazioni, fra cui almeno uno di essi con modalità informatiche. Tale previsione è confermata, a livello europeo[116], con l'obbligatorietà per le aziende con più di cinquanta dipendenti di dotarsi di canali informatici di segnalazione sicuri. È necessario, difatti, attraverso algoritmi di *crypting* garantire la riservatezza delle informazioni, in sintonia con la normativa sulla Privacy. Sono stati, a tal fine, sviluppati negli ultimi anni innumerevoli software, portali e piattaforme di segnalazione criptati per mantenere l'anonimato del segnalante e proteggere i dati personali[117], e soprattutto senza alcuna necessità di manutenzione e gestione da parte di soggetti esterni, impedendo così ai terzi di poter accedere alle informazioni sull'identità del segnalante. Nonostante le disposizioni specifiche sul whistleblowing si rimarca il basso livello di percezione di un'effettiva tutela da parte dei potenziali segnalanti. L'indagine Eurobarometro 2017 sulla corruzione ha rilevato che l'81 per cento degli europei dichiara di non aver segnalato casi di corruzione di cui è stato vittima o testimone, mentre l'85 per cento ha affermato che la mancata segnalazione di un illecito è dovuta

[114] Con riferimento alle fattispecie di reato di cui agli artt. 326 c.p. "Rivelazione ed utilizzazione di segreti d'ufficio", 622 c.p. "Rivelazione di segreto professionale" e 623 c.p. "Rivelazione di segreti scientifici o industriali", nonché relativamente all'obbligo di fedeltà del dipendente di cui all'art. 2105 c.c.

[115] Borsari R., Falavigna F., *Whistleblowing, obbligo di segreto e "giusta causa" di rivelazione*, in *La responsabilità amministrativa delle società e degli enti*, Plenum, Torino, 2/2018.

[116] Direttiva 1937 del 23 ottobre 2019, riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione".

[117] I software e le piattaforme devono essere conformi ed in linea con il GDPR, ossia la normativa europea sulla tutela dei dati personali.

al timore di conseguenze giuridiche, finanziarie e soprattutto lavorative[118]. Uno studio realizzato per conto della Commissione europea[119] ha, poi, stimato per i soli appalti pubblici, una perdita economica dovuta alla mancanza di protezione degli informatori compresa tra i 5,8 e i 9,6 miliardi di euro annui in ambito UE. Per tale motivo Unione europea, commissioni internazionali e nazionali e studiosi hanno auspicato l'inserimento di un meccanismo premiale per rendere più efficace lo strumento[120]. Lo scrivente nutre, tuttavia forti perplessità con riguardo alla predisposizione di un meccanismo premiale, poiché rischierebbe di inflazionare lo strumento, con segnalazioni false o comunque forzate, effettuate soltanto a scopo di tornaconto economico del whistleblower. Senza considerare, poi, che ciò potrebbe conseguire l'effetto opposto a quello desiderato, poiché la falsa segnalazione per tornaconto personale, dovrebbe necessariamente avere conseguenze giuridiche per l'autore, venendo a costituire un ulteriore deterrente anche per le segnalazioni genuine.

Da evidenziare che in tale materia, pur se in ritardo rispetto ai sistemi di common law, dai quali ha origine la disciplina sul whistleblowing, il nostro Paese ha preceduto l'Unione europea, che soltanto nel 2019 ha adottato la Direttiva n. 1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione". La direttiva europea ha, peraltro, portata più generale, ed oltre a favorire l'emersione di illeciti, persegue un fine di rafforzamento dei princìpi di trasparenza e responsabilità, non solo da parte dei pubblici dipendenti ma di tutti i cittadini dell'Unione, riguardo la violazione della totalità dei diritti tutelati dall'UE. Essa mira principalmente ad uniformare ed innalzare il livello di tutela del whistleblower negli Stati membri. La protezione si ha nei confronti di coloro che segnalino violazioni nell'ambito di applicazione di atti UE, con particolare riguardo ad appalti pubblici e servizi finanziari, ma anche di norme in

[118] Coppola F., *Il Whistleblowing: la "scommessa etica" dell'anticorruzione*, in *Diritto penale e processo*, 2018, 4, p. 481 e ss., secondo cui i disincentivi maggiori sono rappresentati dalle "difficoltà di avanzamento di carriera e di ottenere un nuovo lavoro a causa del blacklisting di cui può essere vittima il segnalante".

[119] Corte dei Conti UE, Parere n. 4/2018 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, pubblicato sulla G.U. UE il 9 novembre 2020.

[120] L'articolo 41 del Reg. UE 2017/1129 riconosce la facoltà degli Stati membri di introdurre incentivi finanziari per i whistleblower. La Commissione per lo studio e l'elaborazione di proposte in tema di trasparenza e prevenzione della corruzione nella pubblica amministrazione, *La corruzione in Italia. Per una politica di prevenzione. Analisi del fenomeno, profili internazionali e proposte di riforma*, 2012, I, p. 78 ss, suggerisce l'introduzione di un sistema che prevede che "a chiunque segnala all'Autorità giudiziaria o alla Corte dei Conti condotte illecite che cagionano danno erariale o all'immagine della pubblica amministrazione, spetta un premio in denaro". Fra gli studiosi si veda Coppola F., op. cit. p. 495 secondo cui "Allo stigma culturale e ai molteplici disincentivi (stick) deve fare necessariamente da contraltare una misura premiale". Negli Stati Uniti il Dodd-Frank Act del 2010 autorizza la SEC a corrispondere incentivi a chi segnali un illecito.

materia di concorrenza e violazioni riguardanti il mercato interno. Devono essere predisposti canali dedicati che tutelino la riservatezza dell'identità del segnalante, nonché la garanzia del *follow-up* con comunicazione dell'esito della segnalazione. Le misure protettive ritenute necessarie riguardano ogni attività ritorsiva nei confronti del whistleblower, dal licenziamento al demansionamento, dal trasferimento alla modifica dell'orario, riduzione della retribuzione, misure disciplinari, sanzioni pecuniarie, discriminazioni, molestie e ostracismo sul luogo di lavoro, mancata promozione ovvero annullamento di permessi o licenze (c.d. misure anti-retaliation). Tra le disposizioni finali è fatta salva la possibilità del singolo Stato membro di fissare livelli di tutela ancor più elevati. La direttiva prevede, tuttavia, agli artt. 3 e 4 una limitazione dell'ambito di operatività alle violazioni in determinati settori espressamente indicati quali: appalti pubblici, trasporti, servizi finanziari, ambiente, salute, privacy, concorrenza, sicurezza dei sistemi informatici.

Fra le norme a tutela del whistleblower bisogna considerare anche il d.lgs. n. 90 del 2017 in contrasto al fenomeno del riciclaggio e del finanziamento al terrorismo. Esso predispone, conformemente alla direttiva europea antiriciclaggio, un'adeguata protezione dei "lavoratori dipendenti che hanno denunciato i loro sospetti in merito a casi di riciclaggio che sono stati vittime di minacce o di atti ostili […] in particolare per quanto riguarda il diritto alla protezione dei dati personali e i diritti ad una tutela giurisdizionale e a una rappresentanza effettive"[121]. In particolare l'art. 48 del decreto legislativo in parola, rubricato "Sistemi interni di segnalazione delle violazioni", stabilisce al comma 1 che "I soggetti obbligati adottano procedure per la segnalazione al proprio interno da parte di dipendenti o di persone in posizione comparabile di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo". Recenti modifiche alla direttiva antiriciclaggio chiedono agli Stati membri di garantire ai soggetti che hanno segnalato un caso sospetto di riciclaggio o di finanziamento del terrorismo, il diritto di presentare denuncia in condizioni di sicurezza presso le rispettive Autorità, nonché l'accesso ad un ricorso effettivo per tutelare i propri diritti[122].

Oltre alle fonti normative e comunitarie, innumerevoli sono gli interventi a livello regolamentare e di soft law che hanno creato un quadro dettagliato delle tutele dei segnalatori di illeciti. Nel settore pubblico, oltre alle Linee guida ANAC del 2015, le Delibere n. 1134 del 2017, del 30 ottobre

[121] Direttiva UE 2015/849 "Quarta direttiva antiriciclaggio", Considerando n. 41.
[122] Direttiva UE 843/2018 "Quinta direttiva antiriciclaggio".

2018 e n. 312 del 2019, sempre dell'ANAC, hanno inasprito, principalmente, il sistema sanzionatorio pecuniario[123]. Nel settore bancario la circolare n. 285 del 2013 ha dedicato un'apposita sezione ai sistemi interni di segnalazione delle violazioni. Nel settore privato hanno prevalentemente un'importante funzione interpretativa le Linee guida di Confindustria del 2014 e la Nota illustrativa del 2018 su "La disciplina in materia di whistleblowing".

Nonostante l'attenzione posta sia a livello comunitario che nazionale nei confronti della tutela dei segnalatori di illeciti, non si possono non rilevare alcune criticità. Con riguardo alla normativa europea l'ambito di intervento nel settore privato viene fortemente ridimensionato con l'esclusione delle piccole imprese fra i destinatari della recente disciplina. A livello nazionale, un punto ancora da chiarire riguarda la garanzia dell'anonimato del segnalante, operante soltanto fino alla chiusura delle indagini, facendo venir meno la riservatezza del whistleblower per gran parte del processo penale. Gli elementi di maggior dissuasione per coloro che vogliono segnalare irregolarità restano, comunque, il rischio di incorrere in una querela per calunnia o diffamazione, ovvero l'impossibilità di mantenere l'anonimato a causa di ispezioni, indagini di tipo amministrativo, procedimenti penali o tributari.

1.2.3. Revolving doors e spoils system

Il divieto di *pantouflage*, o di *revolving doors*, è stato introdotto nel nostro ordinamento nel 2012 dalla legge Severino in materia di conflitto d'interessi e prevenzione della corruzione, per impedire che un dipendente pubblico possa sfruttare la propria posizione all'interno di un'amministrazione per ottenere un incarico presso un'impresa o un soggetto privato verso cui ha esercitato poteri autoritativi o negoziali. La legge 190 del 2012 ha inserito all'art. 53 del d.lgs. n. 165/2001 il comma 16 ter, il quale prevede l'apposizione di un vincolo ai dipendenti dell'amministrazione pubblica nei tre anni successivi alla cessazione del rapporto di lavoro, vietando loro di svolgere attività lavorativa o professionale presso soggetti privati destinatari dell'attività della Pubblica Amministrazione svolta attraverso i medesimi poteri, nei tre anni di servizio precedenti[124]. In tal modo viene contrastato il fenomeno del c.d. revolving doors, tramite

[123] Cfr. De Nicola A., Rotunno I., *Il Whistleblowing*, Cons. dir. AODV, luglio 2019.

[124] Con legge n. 190 del 6 novembre 2012 è stato introdotto il comma 16 ter all'articolo 53 del D.lgs. n. 165/2001, il quale dispone, per ciò che riguarda il divieto di pantouflage, che "I dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'art. 1 comma 2 non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari della pubblica amministrazione svolta attraverso i medesimi poteri. I contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto

cui un funzionario pubblico mira a precostituirsi un *favor* nei confronti di coloro che in futuro potrebbero conferirgli incarichi privati. Come chiarito dall'ANAC, l'intenzione del legislatore mira a contenere il dilagante fenomeno corruttivo connesso al conflitto d'interessi, ed in particolare ad un impiego privato del dipendente successivo al rapporto di lavoro nella Pubblica Amministrazione. Onde evitare qualsivoglia possibilità di elusione del divieto di pantouflage, l'ANAC ha specificato che la definizione prevista dall'art. 53 comma 16 ter D.lgs. 165/2001 di "dipendenti con poteri autoritativi e negoziali", non è limitata ai titolari del potere in quanto dirigenti apicali nell'organizzazione, ma è estesa anche a dipendenti che collaborano all'esercizio di tale potere tramite istruttorie (pareri, certificazioni, perizie) svolgendo attività che incidono in maniera determinante sul contenuto del provvedimento finale, ancorché redatto e sottoscritto dal funzionario competente. Il divieto colpisce, pertanto, non solo il dirigente, ma qualsivoglia funzionario o dipendente con poteri discrezionali o che possa comunque incidere nel procedimento amministrativo, ivi compresi "i soggetti esterni con i quali l'amministrazione, l'ente pubblico o l'ente di diritto privato in controllo pubblico stabilisce un rapporto di lavoro, subordinato o autonomo. Tali divieti si applicano a far data dalla cessazione dell'incarico"[125]. Essi trovano applicazione anche in relazione al personale che nei tre anni successivi alla cessazione del rapporto di lavoro con la Pubblica Amministrazione rivesta il ruolo di Presidente del consiglio di amministrazione di un nuovo operatore economico, partecipando alle gare indette dall'amministrazione presso la quale abbia svolto attività lavorativa. La norma dispone che la violazione del divieto di revolving doors abbia come conseguenza la nullità dei contratti ed incarichi conferiti, stabilendo che "I contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti".

Pertanto, in sede di gara o affidamento di incarichi presso l'amministrazione, è necessaria la sottoscrizione della c.d. clausola di pantouflage. Essa deve essere richiesta dalla Pubblica Amministrazione al soggetto con cui entra in contatto, e consiste una dichiarazione per garantire l'applicazione dell'art. 53 comma 16 ter del D.Lgs. n. 165/2001, introdotto dalla legge n. 190/2012, attraverso cui il destinatario del provvedimento afferma di non aver concluso contratti di lavoro

divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi conferiti".

[125] ANAC, delibera n. 88 del 8 febbraio 2017.

subordinato o autonomo, ovvero non aver attribuito incarichi ad ex dipendenti, che hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni, nel triennio successivo alla cessazione del rapporto. Il destinatario del provvedimento dichiara, inoltre, di essere consapevole che, ai sensi del predetto art. 53 comma 16 ter, i contratti conclusi e gli incarichi conferiti in violazione di tali prescrizioni sono nulli e che è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni, con l'obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti. Naturalmente, le eventuali dichiarazioni mendaci contenute nell'autocertificazione, saranno punite a termini di legge con sanzioni penali.

Alla base di tale divieto vi è, certamente, il principio dell'art. 97 della Costituzione, di trasparenza, buon andamento ed imparzialità della P.A., in una mutata ottica di prevenzione della corruzione tramite il controllo e l'eliminazione di situazioni di conflitto di interessi, evitando uno scorretto esercizio dell'attività istituzionale da parte del dipendente pubblico. Nello specifico, il divieto è finalizzato a contenere il rischio, successivo alla cessazione del rapporto di lavoro, di situazioni di conflitto di interessi e di corruzione connesse all'impiego del dipendente, il quale possa sfruttare la conoscenza delle dinamiche organizzative che connotano gli uffici della Pubblica Amministrazione al fine di trarne vantaggi personali.

Lo *spoils system* è, probabilmente, il sistema che più dimostra il connubio fra potere politico e cariche della Pubblica Amministrazione. Per mezzo di esso, i dirigenti dell'amministrazione ricoprono il loro incarico solo nel periodo in cui è in carica il soggetto politico che li ha nominati, in conformità con quanto stabilito dalla legge n. 145 del 2002, e vengono sostituiti al momento dell'insediamento di un nuovo soggetto politico. Ciò consente al nuovo politico eletto di nominare funzionari di propria fiducia a capo degli uffici dell'amministrazione pubblica. Tuttavia la Corte Costituzionale è stata più volte chiamata a verificare la legittimità dello spoils system nei confronti delle norme della Costituzione. La sentenza n. 103 del 2007 ha dichiarato l'illegittimità della legge 145 del 2002 nella parte in cui prevede che gli incarichi dirigenziali cessino automaticamente con il cambio di vertice. Detto principio è stato confermato dalla sentenza n. 161 del 2008, secondo cui tale meccanismo automatico lede il principio di buon andamento della Pubblica Amministrazione previsto dagli articoli 97 e 98 della Costituzione. La Cassazione sez. lavoro con sent. n. 11015 del 2017, sulla scorta della pronuncia della Consulta, ha precisato che l'applicazione legittima del meccanismo dello spoils system nel contesto degli Enti locali debba fondarsi sugli

imprescindibili presupposti della apicalità e della fiduciarietà del dirigente da nominare, altrimenti il sistema si pone in contrasto con l'art. 97 della Costituzione. Con sentenza n. 23 del 2019 la Corte Costituzionale ha, invece, dichiarato la legittimità dello spoils system con riguardo ai dipendenti comunali. Lo spoils system, con tutta evidenza, si contrappone al sistema meritocratico (*merit system*) in base al quale gli uffici pubblici debbano essere assegnati in relazione al curriculum ed alla valutazione delle capacità dei candidati, con grave nocumento per il principio di trasparenza della P.A., ingenerando, peraltro, maggior predisposizione al conflitto di interessi ed a fenomeni corruttivi.

1.2.4. Legge 215 del 2004 e nuove prospettive legislative sul conflitto di interessi

Fino ai primi anni del terzo millennio, in Italia non è mai stata adottata una normativa sul conflitto d'interessi, tanto che il Parlamento europeo nel 2002 criticava il nostro Paese, affermando l'urgenza di una legge al fine di evitare che "in Italia, permanga una situazione di concentrazione del potere mediatico nelle mani del Presidente del consiglio, senza che sia stata adottata una normativa sul conflitto d'interessi[126]".

Solo nel 2004 entra in vigore la legge n. 215, c.d. legge Frattini, con il supposto proposito di creare una barriera giuridica al conflitto di interessi. La legge in esame, rubricata "Norme in materia di risoluzione dei conflitti di interessi", ha l'intento di risolvere le numerose incongruenze del sistema. Tale risoluzione appare necessaria per il corretto funzionamento degli organi nazionali di governo e della Pubblica Amministrazione, con particolare riguardo al conflitto fra l'interesse pubblico e gli interessi privati dei titolari di cariche di governo. La normativa ha, nondimeno, il limite di circoscrivere il suo ambito soggettivo sul conflitto di interessi al rapporto fra posizione individuale e ruolo politico o di governo, mentre dovrebbe estendersi a qualsiasi posizione investita di potere decisionale che possa eventualmente entrare in contrasto col patrimonio economico individuale del soggetto che la ricopre. L'ambito di applicazione della disciplina in oggetto è, difatti, circoscritto ai soli titolari di cariche di governo[127], nel cui ambito sono ricompresi: il Presidente del Consiglio dei Ministri; i ministri; i vice ministri; i sottosegretari di Stato; i commissari straordinari del Governo. Si è inoltre compiuta la scelta di utilizzare un duplice

[126] Risoluzione del Parlamento europeo del 20 novembre 2002, paragrafo 38.

[127] A norma dell'art. 1 (Ambito soggettivo di applicazione) comma 1, della l. n. 215 del 2004, "I titolari di cariche di governo, nell'esercizio delle loro funzioni, si dedicano esclusivamente alla cura degli interessi pubblici e si astengono dal porre in essere atti e dal partecipare a deliberazioni collegiali in situazione di conflitto d'interessi".

strumento per sanzionare il conflitto di interessi: considerare la posizione personale di conflitto quale elemento oggettivo di pericolo, sancendo preventivamente l'incompatibilità di cariche che possano produrre un potenziale conflitto, ed altresì considerare il comportamento concreto del titolare della carica, incompatibile se dalle sue azioni ne consegua un vulnus per il perseguimento dell'interesse generale. Il compito di accertare tali incompatibilità spetta ad un'autorità garante[128]. Tale duplice soluzione rappresenta, a ben vedere, una contraddizione. Il contrasto al conflitto di interessi avviene, difatti, sia a carattere preventivo oggettivo, che soggettivo comportamentale, tuttavia le due soluzioni sono palesemente in contrasto, in quanto figlie di una visione del conflitto d'interessi diametralmente opposta l'una con l'altra. Ciò in quanto l'incompatibilità oggettiva dovrebbe di per sé evitare la verificazione di casi rientranti nella seconda ipotesi, ossia comportamenti effettivamente e materialmente conflittuali. I due strumenti possono, tuttavia, coesistere se utilizzati in maniera consequenziale e alternativa, e non contemporanea: soltanto nel caso in cui l'incompatibilità oggettiva non riuscisse a fermare il conflitto di interessi, sarebbe necessario il compimento di attività di contrasto nei confronti di quei comportamenti che in concreto ledano l'interesse pubblico.

La legge del 2004 n. 215, all'art. 2, modificato con d.l. n. 44 del 2005, enuclea i casi di incompatibilità del titolare di cariche di governo nello svolgimento del proprio incarico, ossia cariche e uffici in enti di diritto pubblico o imprese private con fine di lucro, attività professionali o di lavoro autonomo in materie connesse con la carica di governo, impieghi di lavoro pubblico o privato. Entro trenta giorni dall'assunzione della carica di governo, il titolare ha l'obbligo di dichiarare all'Autorità garante della concorrenza e del mercato, ogni situazione di incompatibilità. Dall'art. 3 possiamo dedurre una precisa definizione di conflitto di interessi, poiché è stabilito che "Sussiste situazione di conflitto di interessi ai sensi della presente legge quando il titolare di cariche di governo partecipa all'adozione di un atto, anche formulando la proposta, o omette un atto dovuto, trovandosi in situazione di incompatibilità ai sensi dell'articolo 2, comma 1, ovvero quando l'atto o l'omissione ha un'incidenza specifica e preferenziale sul patrimonio del titolare, del coniuge o dei parenti entro il secondo grado, ovvero delle imprese o società da essi controllate, secondo quando previsto dall'articolo 7 della legge 10 ottobre 1990, n. 287, con danno per l'interesse pubblico". Tale definizione è tuttavia, nella sua formulazione pur

[128] L'AGCM, Autorità Garante della Concorrenza e del Mercato, c.d. Antitrust, mentre se l'incompatibilità riguarda i settori delle comunicazioni, e competente anche l'Autorità per le garanzie nelle comunicazioni.

completa e dettagliata, troppo restrittiva poiché limitata al conflitto di interessi nell'ambito delle cariche di governo. È, comunque, sempre da tener presente che il conflitto di interessi, in sé considerato, non rappresenta un illecito e neanche una semplice condotta, ma una mera situazione di fatto. Il d.l. 138/2011 ha ampliato il novero delle incompatibilità delle cariche di governo comprendendovi qualsiasi altra carica pubblica elettiva di natura monocratica (incluso sindaci e presidenti di provincia) relativa ad organi di governo di enti pubblici territoriali aventi popolazione superiore a 5.000 abitanti. Nonostante ciò la norma resta limitata a poche cariche di vertice.

La legge n. 215, all'art. 4, estende, poi, le disposizioni volte a prevenire e reprimere l'abuso di posizione dominante di cui all'articolo 3 della legge 10 ottobre 1990 n. 287, anche nei casi in cui viene compiuta avvalendosi di atti posti in essere dal titolare di cariche di governo, dall'impresa facente capo al titolare medesimo, suo coniuge o parenti entro il secondo grado, ovvero dalle imprese o società da essi controllate. L'Autorità garante della concorrenza e del mercato ha il compito di: accertare la sussistenza di situazioni di incompatibilità; vigilare sul rispetto dei divieti previsti dalla legge n. 215 in materia di conflitto di interessi; promuovere la rimozione o decadenza dalla carica o dall'ufficio del titolare di cariche di governo; sospendere il rapporto di impiego o di lavoro pubblico o privato, nonché l'iscrizione da albi e registri professionali del titolare di cariche di governo.

Una nuova prospettiva sul conflitto d'interessi, almeno con riguardo ai dipendenti pubblici, si è aperta con l'aggiunta dell'art. 6 bis alla legge 241 del 1990, ad opera dell'art. 1 comma 41 della l. n. 190 del 2012. Esso prevede un generale obbligo di astensione del dipendente pubblico, nell'ambito del procedimento amministrativo, al ricorrere di ogni situazione di conflitto di interessi che possa coinvolgerlo[129]. Il principio costituzionale di imparzialità e buon andamento della Pubblica Amministrazione trova uno dei suoi corollari nell'art. 6 bis, imponendo al responsabile del procedimento ed ai titolari degli uffici di astenersi dai propri compiti, qualora ravvisino una situazione di conflitto di interessi. L'obbligo di astensione e di segnalazione trasforma il conflitto di interessi da mera situazione di fatto in un vero e proprio dovere del

[129] Art. 6 bis l. 241 del 1990: "Il responsabile del procedimento e i titolari degli uffici competenti ad adottare i pareri, le valutazioni tecniche, gli atti endoprocedimentali e il provvedimento finale devono astenersi in caso di conflitto di interessi, segnalando ogni situazione di conflitto, anche potenziale".

dipendente pubblico, dal quale può derivare un'omissione giuridicamente rilevante, perlomeno sul piano disciplinare.

Ampliando gli obiettivi ed il campo di azione della suddetta norma, il d.lgs. n. 39 del 2013 introduce una disciplina dedicata in via diretta ed esclusiva al conflitto di interessi nello svolgimento di incarichi amministrativi. Il legislatore del 2013 ha individuato nell'Autorità Nazionale Anticorruzione (ANAC), l'organo principale competente a vigilare sulle violazioni in materia di conflitto d'interessi e trasparenza. Ad esso si aggiungono, per ogni amministrazione, gli RPCT (Responsabili della Prevenzione, della Corruzione e della Trasparenza). L'ANAC ha precisato i compiti dell'RPCT istituito dalla l. n. 190 del 2012, in particolare quelli di indirizzo, controllo, verifica e segnalazione. L'area del settore amministrativo che risulta essere maggiormente sensibile al conflitto d'interessi è quella dei contratti pubblici, poiché i soggetti proponenti l'acquisto sono spesso coloro che utilizzano o comunque traggono vantaggi economici dall'alienazione dei beni, ovvero sono a questi legati da particolari vincoli. Anche gli incarichi e le nomine necessitano di approfonditi controlli, soprattutto nei periodi di transizione ed in caso di legislazione emergenziale.

Nell'ultimo decennio non si può negare, nel nostro Paese, un cambiamento di rotta per quanto riguarda la rilevanza attribuita al conflitto d'interessi, in precedenza colpevolmente sottovalutato con riguardo agli effetti. Il cambiamento in atto è non solo legislativo, ma anche culturale. Ne è dimostrazione l'incremento di segnalazioni di illeciti nella pubblica amministrazione, favorito dalle tutele poste in essere dalla legge al fine di evitare ritorsioni contro i c.d. whistleblower. Anche la maggior trasparenza e la c.d. vigilanza collaborativa fra le Pubbliche Amministrazioni[130] ha segnato un cambio di passo nel contrasto alle situazioni conflittuali, con un conseguente miglioramento della situazione italiana. Nonostante la strada sia ancora lunga per raggiungere i risultati di altri Paesi europei considerati virtuosi, il percorso intrapreso è quello corretto, poiché la corruzione ed il conflitto d'interessi, benché ampiamente presenti, non sono più percepiti come nel passato, quale stabile meccanismo con cui bisogna confrontarsi in ogni rapporto con la Pubblica Amministrazione.

[130] Dall'aprile del 2022 è in vigore il nuovo regolamento predisposto da Anac sulla vigilanza collaborativa, che amplia le possibilità per le stazioni appaltanti di ricorso a tale importante strumento di collaborazione preventiva. La Vigilanza collaborativa è uno strumento di carattere volontario tramite cui le stazioni appaltanti si rivolgono ad Anac prima di indire una procedura di gara, chiedendo un sostegno preventivo nella verifica di conformità degli atti.

Giova, poi, segnalare in prospettiva futura, la previsione di un ulteriore ampliamento del raggio d'azione della disciplina sul conflitto di interessi. Sono, difatti, tuttora all'esame della Commissione della Camera, proposte di legge di iniziativa parlamentare[131] che modificano la disciplina vigente, attualmente contenuta nella legge 215/2004. Tali proposte potrebbero aprire nuovi scenari riguardo il conflitto di interessi, con la previsione di misure più stringenti per i titolari di cariche di governo nazionale, regionale e locale, l'ampliamento dei casi di ineleggibilità alle cariche parlamentari di consigliere regionale e magistrato, la dilatazione delle ipotesi di inconferibilità degli incarichi. Viene, inoltre, previsto un rafforzamento dei poteri di accertamento e vigilanza delle autorità indipendenti (ANAC, AGCM ed AGCOM), ed ampliate le forme di trasparenza rispetto al quadro normativo vigente. È, altresì, disposta la nullità degli atti adottati dal titolare della carica di governo in violazione degli obblighi di astensione, tuttavia il Consiglio dei ministri può convalidare tali atti per motivi di interesse generale. Specifiche sanzioni sono, poi, previste nei confronti delle imprese che hanno conseguito vantaggi dagli atti adottati dal titolare della carica di governo in una situazione di conflitto di interessi. Viene, infine, distinta l'incompatibilità generale da quella patrimoniale, anche per ciò che riguarda gli effetti, rispettivamente della decadenza dall'attività incompatibile con l'incarico di governo, e del conferimento ad una società fiduciaria delle attività indicate come incompatibili dall'Autorità. Ciò che, invece, non è ancora stato preso in considerazione dal legislatore, nonostante i solleciti di ANAC[132], è la predisposizione di un complesso normativo organico, moderno e completo in materia di conflitto di interessi, che preveda analiticamente gli elementi costitutivi e le diverse ipotesi di incompatibilità a svolgere ruoli di potere nella Pubblica Amministrazione.

1.2.5. L'evoluzione normativa in tema di procurement pubblico e appalti

Il codice dei contratti pubblici, d.lgs. n. 50 del 2016, abroga il previgente codice del 2010 (DPR n. 207 del 2010 in attuazione del d.lgs. n. 163 del 2006) nell'ottica dell'impegno per il conseguimento di una maggiore efficacia del procurement pubblico, puntando prevalentemente su tre elementi: la semplificazione, la trasparenza e la qualificazione[133]. Il decreto del 2016 viene adottato su impulso di tre direttive comunitarie, la 2014/23/UE, 2014/24/UE e la 2014/25/UE, le quali evidenziano prioritariamente proprio la necessità di una regolamentazione europea uniforme

[131] In particolare: A.C. 702 Fiano, A.C. 1461 Macina, A.C. 1843 Boccia.
[132] FAQ in materia di anti corruzione aggiornate da ANAC con l'emanazione del PNA 2019-2021.
[133] In tal senso Interlandi M., *Il nuovo codice dei contratti pubblici nella prospettiva dell'e-procurement*, in *Gazzetta Amministrativa*, n. 1, 2018, p. 1.

delle procedure ad evidenza pubblica, e della semplificazione normativa e procedurale per ottenere un incremento dell'efficienza amministrativa. A tal fine, oltre ad una deregolamentazione giova, secondo le direttive, il rafforzamento degli strumenti informatici, con l'effetto di velocizzare le procedure di approvvigionamento ed ampliare la platea di operatori economici, per favorire la concorrenza e limitare il conflitto di interessi degli attori coinvolti. Il legislatore italiano procede, in un'ottica di deregolamentazione, ad una cospicua riduzione del numero di articoli nei confronti del previgente codice del 2010 e all'abrogazione del regolamento attuativo con la sostituzione da parte di atti di c.d. soft law. Tuttavia lo snellimento nei confronti del vecchio codice è solo apparente, poiché nonostante la riduzione da 630 a 220 articoli, il codice del 2016 contiene molti più commi del precedente per ogni articolo, lasciando pressoché invariata la mole normativa, peraltro in evidente violazione del divieto di "gold plating"[134].

Di particolare interesse è, in ottica di semplificazione, l'introduzione del documento di gara unico europeo (DGUE), che consiste in un'autodichiarazione dell'operatore economico, che fornisce una prova preliminare in sostituzione dei certificati rilasciati da autorità pubbliche o terzi. Viene anche codificato l'istituto del soccorso istruttorio, per cui la mancanza, l'incompletezza e ogni altra irregolarità degli elementi e del documento di gara unico europeo, può essere regolarizzata su richiesta della stazione appaltante entro il termine, non superiore a dieci giorni, da questa stabilito. Viene anche previsto che, in caso di inutile decorso del termine di regolarizzazione, il concorrente è escluso dalla gara, e inoltre costituiscono irregolarità essenziali non sanabili le carenze della documentazione che non consentono l'individuazione del contenuto o del soggetto responsabile della stessa. Al fine di ridurre il contenzioso, è stato introdotto (all'art. 120 del Codice del Processo Amministrativo) un nuovo rito abbreviato in camera di consiglio sull'impugnativa dei motivi di esclusione e sono stati previsti rimedi alternativi alla tutela giurisdizionale.

Ampio rilievo riveste, oltre alla semplificazione, anche la trasparenza, che implica l'accessibilità totale ai dati e documenti detenuti dalle pubbliche amministrazioni, "allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche[135]". Con particolare riguardo al settore degli appalti, la trasparenza, così intesa, può

[134] Per la Commissione europea, Smart regulation in the European Union, COM (2010) 543 final, Bruxelles, 8 ottobre 2010, il gold plating è quella tecnica che "va al di là di quanto richiesto dalla normativa europea pur mantenendosi entro la legalità".
[135] Art. 1 d.lgs. n. 33 del 2013.

essere realizzata sia attraverso gli obblighi di comunicazione relativi alle procedure di gara, che attraverso la pubblicazione delle informazioni relative ai procedimenti amministrativi, così come previsto all'art. 29 del codice dei contratti pubblici[136]. Con riguardo alla trasparenza, in particolare, è stato previsto l'obbligo dell'utilizzo della procedura di gara con pubblicazione del bando, anche per i contratti sotto la soglia di rilevanza europea (definita all'art. 35), distinguendo le procedure utilizzabili.

Per quanto attiene alla qualificazione, avente ad oggetto il complesso delle attività che caratterizzano il processo di acquisizione di un bene, servizio o lavoro in relazione a capacità di progettazione, di affidamento e di verifica sull'esecuzione e controllo dell'intera procedura (art. 38 d.lgs. n. 50 del 2016), il codice dei contratti pubblici permette alle stazioni appaltanti e centrali di committenza di certificare la loro professionalità e le capacità acquisite[137]. Tuttavia la parziale inattuazione dell'art. 38 comma 2 del Codice, ha fatto sì che l'ANAC non potesse stabilire le modalità attuative del sistema di qualificazione. Per quanto riguarda la qualificazione degli operatori economici, invece, l'art. 83, comma 10, d.lgs. 50/2016 prevede l'istituzione del sistema di rating di impresa, per il quale l'ANAC rilascia una certificazione, a seguito della valutazione dei curricula degli operatori. In tal modo le stazioni appaltanti sono in grado di valutare le imprese in base alla loro affidabilità secondo i comportamenti precedentemente tenuti, anche in termini di rispetto della legalità rilevato dalla medesima ANAC, in collaborazione con l'Autorità Antitrust, laddove l'art. 213, comma 7, del nuovo Codice dispone che l'Autorità anticorruzione "collabora con l'Antitrust ai fini della rilevazione di comportamenti aziendali meritevoli di valutazione per l'attribuzione del rating di legalità" e che tale rating "concorre alla determinazione del rating di impresa".

In linea generale il codice dei contratti pubblici del 2016 prevede l'introduzione della programmazione degli appalti anche per forniture e servizi, in considerazione: del costo totale

[136] Laddove esplicita che "Tutti gli atti delle amministrazioni aggiudicatrici e degli enti aggiudicatori relativi alla programmazione di lavori, opere, servizi e forniture, nonché alle procedure per l'affidamento e l'esecuzione di appalti pubblici di servizi, forniture, lavori e opere, di concorsi pubblici di progettazione, di concorsi di idee e di concessioni, compresi quelli tra enti nell'ambito del settore pubblico di cui all'articolo 5, alla composizione della commissione giudicatrice e ai curricula dei suoi componenti ove non considerati riservati ai sensi dell'articolo 53 ovvero secretati ai sensi dell'articolo 162, devono essere pubblicati e aggiornati sul profilo del committente, nella sezione "Amministrazione trasparente", con l'applicazione delle disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33".

[137] Cfr. Pajno A., *La nuova disciplina dei contratti pubblici tra esigenze di semplificazione, rilancio dell'economia e contrasto alla corruzione*, in *Rivista italiana diritto pubblico com.*, fasc. 5, 2015, p. 1127 ss.

della fornitura; estensione dell'applicazione del criterio dell'offerta economicamente più vantaggiosa per l'aggiudicazione, e non solo del prezzo più basso; definizione delle modalità di controllo degli appalti; regolamentazione delle attività delle stazioni appaltanti. Il codice rinuncia al sistema degli automatismi cui ci si era affidati dagli anni novanta per ridurre la corruzione, e risultato poi inefficace, anche in considerazione delle vicende giudiziarie degli anni successivi. La convinzione che ridurre la discrezionalità fosse la chiave per sconfiggere la corruzione è risultata, difatti, una mera illusione. La convinzione che il contrasto alla corruzione potesse avvenire con sistemi di automatismo quali il principio del prezzo più basso, non è risultata veritiera, e nel codice del 2016 è stata favorita l'idea dell'offerta economicamente più vantaggiosa. Ciò lascia indubbiamente un margine di discrezionalità alle stazioni appaltanti, ma consente un miglioramento qualitativo di forniture e servizi e limitazione dell'aumento dei costi in fase di esecuzione, e di conseguenza dei tempi di completamento dell'opera, senza tuttavia creare maggiori rischi sul versante della corruzione, sempre che venga attuata una specifica attività di vigilanza e di controllo da parte dell'Autorità anti corruzione.

Tra le misure atte a garantire l'imparzialità vi è la previsione della composizione delle commissioni di aggiudicazione mediante scelta e sorteggio dei nominativi tratti da un albo istituito presso l'ANAC. Per gli appalti di valore inferiore alla soglia comunitaria (individuata all'art. 35 in base alla tipologia di appalto[138]) nonché di minore complessità, rimane la possibilità di nominare componenti interni alla stazione appaltante, nel rispetto del principio di rotazione[139]. Tra le novità previste nel codice dei contratti pubblici vi è il superamento del sistema della c.d. legge obiettivo che aveva la funzione di creare una "corsia preferenziale" per il finanziamento, l'approvazione progettuale e l'esecuzione delle opere definite quali infrastrutture strategiche nazionali. Tale sistema, come emerge dalle relazioni dell'ANAC, non solo non aveva consentito la realizzazione delle opere, ma per effetto delle concentrazioni di potere decisionale, aveva rappresentato un terreno fertile per lo sviluppo di pratiche corruttive. Per tale motivo il codice dei contratti ne prevede espressamente l'abrogazione. Superando la logica dell'urgenza e della specialità, le infrastrutture e gli insediamenti prioritari per lo sviluppo del Paese sono individuati attraverso due strumenti di pianificazione e programmazione generale: il primo, contiene le linee strategiche delle politiche della mobilità delle persone, delle merci e dello sviluppo infrastrutturale del Paese;

[138] Secondo lo stesso articolo 35, comma 3 del d.lgs. n. 50 del 2016, le soglie "sono periodicamente rideterminate con provvedimento della Commissione europea".
[139] art. 77, d.lgs. n. 50 del 2016.

il secondo contiene l'elenco degli interventi relativi al settore dei trasporti e logistica la cui progettazione è valutata meritevole di finanziamento. Inoltre, le grandi opere vengono sottoposte a consultazione pubblica (art. 22), su modello del *débat public* francese.

Altra innovazione del codice sono i criteri di aggiudicazione degli appalti: vengono, così, favoriti gli appalti verdi, aventi minore impatto ambientale. Vi è una diversa disciplina dei contratti sotto soglia, che non superano un certo valore. Col vecchio codice, tali appalti potevano essere assegnati tramite affidamenti diretti o una micro-gara, che però creava una sorta di oligopolio, mentre col codice del 2016 viene favorita la rotazione, chiamando ad ogni gara imprese diverse. Le procedure di aggiudicazione possono essere aperte e ristrette: nelle prime possono partecipare all'offerta tutti coloro che hanno i requisiti richiesti, mentre le seconde richiedono una preselezione a monte. Soggetta a maggiori restrizioni è invece la procedura negoziata, in cui le stazioni appaltanti negoziano solo con alcuni operatori dopo averli consultati: ad essa si fa ricorso ove nella gara non vi siano state offerte regolari o in casi di estrema urgenza. Infine col dialogo competitivo la stazione appaltante avvia un dialogo con le imprese ammesse, in base alle proprie necessità.

La normativa vigente sugli appalti mira prevalentemente ad infrangere la sovrapposizione di corruzione ed inefficienza, tramite misure volte soprattutto a condizionare l'assegnazione dei fondi all'esistenza di progetti ed interlocutori precisi ed affidabili, favorire la più ampia partecipazione alle gare privilegiando le procedure aperte, garantire la massima trasparenza facilitando l'accesso alle informazioni, operare una separazione soggettiva fra fase della progettazione e della realizzazione, istituire osservatori ed avvalersi di banche dati, rafforzare controlli sostanziali sia del settore pubblico che del privato[140]. In ambito legislativo il contrasto alla corruzione e al conflitto di interessi è orientato alla semplificazione delle procedure di appalto ed alla qualificazione, ma anche alla maggior discrezionalità delle amministrazioni in un'ottica di accresciuta trasparenza, ed al ruolo cardine ricoperto dall'Autorità Nazionale Anticorruzione non solo con poteri di vigilanza, ma anche di regolamentazione. Le norme di legge sono, difatti, state affiancate da atti di soft law, ossia linee guida, bandi-tipo e contratti-tipo, predisposti direttamente o indirettamente dall'ANAC. L'ampliamento della discrezionalità delle amministrazioni ed in particolare delle stazioni appaltanti, volto a superare le rigidità della vecchia

[140] In tal senso, Vannucci A., *Come combattere la corruzione in Italia?*, in *Quaderni di Sociologia*, 14, p. 128.

disciplina, è stato bilanciato con misure atte a favorire l'efficienza e l'incremento dell'attività di controllo, ed a garantire l'imparzialità delle commissioni di gara, ad esempio introducendo il criterio della rotazione. L'attività di controllo è stata ripartita in diversi momenti della procedura: in via preventiva rispetto alla fase di programmazione; durante la gara d'appalto da parte del responsabile unico del procedimento, il cui ruolo viene rafforzato ed ampliato[141]; in riferimento agli atti delle procedure di affidamento; infine nella fase successiva all'aggiudicazione, con una verifica a posteriori. È stato conferito maggior rilievo al controllo operato da parte delle stazioni appaltanti e della magistratura amministrativa, ed un potere generale di vigilanza e controllo all'ANAC, il cui compito diventa funzionale all'applicazione dello stesso codice, prevedendo anche un controllo della Corte dei conti, che, in caso di inadempimento, può imporre alle stazioni appaltanti stesse, una sanzione amministrativa pecuniaria.

Il conflitto di interessi negli appalti è disciplinato prevalentemente all'articolo 42 del d.lgs. n. 50 del 2016. Secondo l'articolo in parola si ha conflitto d'interesse quando il personale di una stazione appaltante o di un prestatore di servizi che interviene nello svolgimento della procedura di aggiudicazione degli appalti ha, direttamente o indirettamente, un interesse personale che può essere percepito come una minaccia alla sua imparzialità e indipendenza. Emerge, in tali situazioni, l'obbligo di astensione per tutti i soggetti chiamati ad intervenire nello svolgimento della procedura di aggiudicazione ove esistano delle gravi ragioni di convenienza. Secondo la giurisprudenza, con riferimento all'art. 42, per le sue descritte caratteristiche funzionali, la disposizione in parola è da intendersi come norma lato *sensu* "di pericolo", in quanto le misure che essa contempla (astensione dei dipendenti) o comporta (esclusione dell'impresa concorrente) operano per il solo pericolo di pregiudizio che la situazione conflittuale può determinare[142]. In riferimento al conflitto di interessi negli appalti, la Sezione consultiva per gli atti normativi del Consiglio di Stato, partendo dall'assunto che occorre distinguere situazioni di conflitto di interessi palesi e tipizzate (quali i rapporti di parentela o coniugio), da quelle non tipizzate, ossia le gravi ragioni di convenienza, ha evidenziato che "rilevano sia palesi situazioni di conflitto di interessi, sia situazioni di conflitto di interessi (in questo senso) potenziali, perché tale nozione include non soltanto le ipotesi di conflitto attuale e concreto, ma anche quelle che potrebbero derivare da una condizione non tipizzata ma ugualmente idonea a determinare il

[141] Articolo 31 d.lgs. n. 50 del 2016.
[142] Consiglio di Stato, sez. III, n. 355 del 2019 e sez. V, n. 3048 del 2020.

rischio”[143]. Nella stessa sentenza, il massimo organo di giustizia amministrativa ha puntualizzato l’irrilevanza dell’origine del conflitto di interessi, statuendo che “un conflitto di interessi si determina le volte in cui a un soggetto giuridico sia affidata la funzione di cura di un interesse altrui (così detto interesse funzionalizzato) ed egli si trovi, al contempo, ad essere titolare (*de iure vel de facto*) di un diverso interesse la cui soddisfazione avviene aumentando i costi o diminuendo i benefici dell’interesse funzionalizzato. Non rileva particolarmente se tale interesse derivi da situazioni affettive o familiari o economiche. Per l’inquadramento di teoria generale è sufficiente che sussistano due interessi in contrasto economico: quello funzionalizzato e quello, di qualsiasi natura, dell’agente”.

L’ANAC ha più volte stabilito che le stazioni appaltanti debbano sempre verificare possibili conflitti di interessi ed il rispetto dell’art. 42 del Codice dei contratti pubblici. Nella recente Delibera n. 273 del 7 giugno 2022 l’Autorità ha ribadito che nell’assegnare un appalto occorre sempre verificare che non vi siano conflitti di interesse da parte dei soggetti coinvolti, a qualunque titolo, in tutte le fasi dell’affidamento dei contratti pubblici, compresa la realizzazione dell’esecuzione. Secondo ANAC, infatti, “Costituisce violazione dell’art. 42 co. 5 d.lgs. 50/2016, la condotta della stazione appaltante che omette di assumere prescritte dichiarazioni richieste dall’art. 42 del codice in ordine alla (in)sussistenza dei conflitti di interesse e non assume alcuna iniziativa volta a gestire la situazione di potenziale conflitto di interesse in cui versa il dipendente, comunque nota alla stazione appaltante”.

Nonostante le aspettative, la rivoluzione del codice dei contratti pubblici non ha conseguito i risultati sperati, sia in riferimento alla semplificazione, che al contrasto dei fenomeni corruttivi. Il codice del 2016 ha, così, subìto numerose novelle, in particolare con il d.l. n. 32 del 2019 (c.d. Sblocca cantieri) convertito in legge n. 55 del 2019. Esso nasce dalla necessità di snellire le procedure per l’avvio dei cantieri e superare le lungaggini burocratiche, poiché le disposizioni ancora troppo rigide imposte dal Codice dei contratti pubblici del 2016, hanno rischiato di bloccare la possibilità di avviare nuovi appalti. Proposito del c.d. Sblocca cantieri è l’eliminazione di tutti i precedenti Decreti ministeriali e interministeriali e delle Linee Guida dell’ANAC, in modo da creare un regolamento unitario a cui fare riferimento. Anche le modifiche del 2019 non hanno,

[143] Consiglio di Stato, Sezione consultiva per gli atti normativi, parere n. 667 del 5 marzo 2019, espresso sullo schema delle linee guida Anac aventi ad oggetto “Individuazione e gestione del conflitto di interesse nelle procedure di affidamento di contratti pubblici”.

tuttavia, risolto le criticità della disciplina sugli appalti, pertanto si è più volte avanzata in Parlamento la proposta per una totale revisione. La maggiore priorità per una nuova regolamentazione del procurement pubblico è, indubbiamente, l'emanazione del Regolamento di attuazione previsto dallo Sblocca cantieri in sostituzione della c.d. *soft regulation* su cui aveva puntato il Codice del 2016, e che ha subìto innumerevoli critiche anche a livello parlamentare.

Ulteriori modifiche al Codice del 2016 sono state attuate dal d.l. Semplificazioni/Recovery[144], in particolare in materia di subappalto. Non è più prevista, difatti, una specifica percentuale massima per l'affidamento dei lavori ai subappaltatori, tuttavia le stazioni appaltanti dovranno indicare nei documenti di gara le prestazioni e i servizi affidati in subappalto. Le stazioni appaltanti saranno anche tenute ad indicare quali sono le opere per le quali sarà necessario rafforzare i controlli ed assicurare una maggiore tutela nei confronti dei lavoratori, non solo per assicurare che i subappaltatori lavorino sempre in sicurezza, ma anche per prevenire che questi possano essere legati ad infiltrazioni criminali, a meno che gli stessi non risultino iscritti all'apposita anagrafe antimafia. Inoltre le stazioni appaltanti potranno nominare commissari di gara interni in caso di carenza di soggetti iscritti all'Albo dei Commissari gestito dall'ANAC. Fra le principali modifiche del recente decreto legge vi è anche l'obbligo di prevedere l'esclusione automatica delle offerte anomale in presenza di un numero di offerte ammesse pari o superiore a dieci e la facoltà per i comuni non capoluogo di provincia di bandire le procedure di gara senza ricorrere alle centrali di committenza.

1.2.6. Divieti ed obblighi fondamentali in materia di conflitto di interessi

Fra i principali obblighi in caso di conflitto di interessi vi è certamente quello di astensione dall'esercizio di un determinato potere o dallo svolgimento di un'attività, secondo quanto previsto, non solo dall'art. 6 bis legge 241/1990, dall'art. 42 d.lgs. n. 50/2016 e dal D.P.R. n. 62/2013[145], ma anche dai codici di comportamento e dalle linee guida ANAC. A questo si aggiunga l'obbligo di segnalazione preventiva e motivata del conflitto di interessi da parte del dipendente al proprio superiore (legge 190/2012, art. 6 comma 2 e art. 7 D.P.R. n. 62/2013, ed art. 42 d.lgs. n. 50/2016). L'art. 7 D.P.R. n. 62/2013 prevede anche l'obbligo a carico di ciascun dipendente, all'atto dell'assegnazione all'ufficio, di informare per iscritto il dirigente di tutti i rapporti, diretti

[144] Decreto legge n. 77 del 2021, pubblicato in Gazzetta Ufficiale il 31 maggio 2021.
[145] Nello specifico, D.P.R. n. 62/2013 art. 3 comma 2, art. 6 comma 2, ed art. 7.

o indiretti, di collaborazione con soggetti privati in qualunque modo retribuiti che lo stesso abbia, o abbia avuto negli ultimi tre anni. Per l'art. 13 D.P.R. n. 62/2013 sussiste, poi, l'obbligo in capo al dirigente dell'amministrazione, prima di assumere le sue funzioni, di comunicare all'ufficio personale le partecipazioni azionarie e gli altri interessi finanziari che possano porlo in conflitto di interessi con la funzione pubblica che svolge, e di dichiarare se ha parenti e affini entro il secondo grado, coniuge o convivente che esercitano attività politiche, professionali o economiche che li pongano in contatti frequenti con l'ufficio che dovrà dirigere o che siano coinvolti nelle decisioni o nelle attività inerenti all'ufficio. I dirigenti responsabili hanno anche un obbligo di vigilanza e di controllo sull'assenza di conflitti per ciò che riguarda i dipendenti dell'amministrazione di loro pertinenza[146].

Vi è, inoltre, il divieto, previsto ex art. 35 bis d.lgs. n. 165/2001, per coloro che sono stati condannati, anche in via non definitiva, per i reati contro la Pubblica Amministrazione disciplinati al capo I, titolo II, del libro II del codice penale (peculato, concussione, corruzione, abuso d'ufficio), di far parte di commissioni per l'affidamento di appalti o per l'accesso o la selezione a pubblici impieghi, di essere assegnati agli uffici preposti alla gestione delle risorse finanziarie, all'acquisizione di beni servizi e forniture, o alla concessione o all'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari o attribuzioni di vantaggi economici a soggetti pubblici e privati, ovvero di fare parte delle commissioni per la concessione o per l'attribuzione di vantaggi economici di qualunque genere.

Un ruolo di particolare rilievo nella prevenzione del conflitto di interessi è, oggi, ricoperto dai codici di comportamento delle amministrazioni pubbliche. Essi prevedono un obbligo di verifica da parte del superiore al subordinato in caso di rilevazione di conflitto di interessi e di trasmissione delle decisioni in tema di conflitto di interessi da parte del responsabile dell'ufficio, al servizio gestione del personale ed al responsabile della prevenzione della corruzione e trasparenza (RPCT). In caso di mancata osservanza del codice di comportamento è l'art. 16 del D.P.R. n. 62/2013 a prevedere sanzioni disciplinari ai dipendenti dell'amministrazione ed al dirigente inadempiente[147].

[146] Art. 1 comma 9, legge n. 190/2012.

[147] Per il primo comma dell'art. 16 del D.P.R. n. 62/2013 "La violazione degli obblighi previsti dal presente Codice integra comportamenti contrari ai doveri d'ufficio. Ferme restando le ipotesi in cui la violazione delle disposizioni contenute nel presente Codice, nonché dei doveri e degli obblighi previsti dal piano di prevenzione della corruzione, dà luogo anche a responsabilità penale, civile, amministrativa o contabile del pubblico dipendente, essa è fonte di

1.3. Tecniche di contrasto al conflitto di interessi nel procurement pubblico

1.3.1. Procurement pubblico, conflitto di interessi e digitalizzazione delle procedure

Gli appalti pubblici hanno lo scopo primario di permettere l'acquisizione dal mercato di beni o servizi da parte della pubblica amministrazione che non ne dispone autonomamente, nelle condizioni più vantaggiose in termini di risultati e costi, onde soddisfare un criterio di efficacia ed efficienza. La c.d. "*value for money*", ossia l'ottimizzazione della spesa, ha sempre rappresentato un punto dolente per le finanze pubbliche del nostro Paese. Solo un'accorta e seria strategia nel procurement pubblico può consentire di ottimizzare la gestione degli acquisti, dando nel contempo alle imprese la possibilità di accedere alle forniture pubbliche in una condizione di competizione leale e trasparente. Il bilanciamento fra costi sostenuti e risultati predeterminati in un'ottica di ottimizzazione e razionalizzazione della spesa, deve essere un obiettivo primario della Pubblica Amministrazione. Ciò è possibile principalmente prevenendo i fenomeni corruttivi ed eliminando ogni conflitto di interessi, costanti che troppo spesso hanno caratterizzato le gare ad evidenza pubblica, per la mancanza di attenzione da parte dei pubblici poteri nei confronti delle normative, generalmente incomplete, prive di costanti aggiornamenti ed applicate soltanto parzialmente. L'inerzia nel contrastare il conflitto di interessi ha origine proprio nel disinteresse da parte della politica a sconfiggere il fenomeno, poiché sono gli stessi suoi rappresentanti ad esserne prevalentemente coinvolti ed a beneficiarne maggiormente.

In tale sistema, può risultare utile il controllo dal basso da parte del cittadino nei confronti dei pubblici poteri, in un'ottica di trasparenza e partecipazione. Nonostante i segnali positivi negli ultimi anni in tal senso, grazie alle norme sulla trasparenza nella P.A., la tutela del whistleblower ed il divieto di revolving doors, si rileva comunque una forte ritrosia del cittadino nel denunciare situazioni illecite o quanto meno sospette, poiché troppo facilmente ci si dimentica che lo spreco di denaro pubblico riduce quantità e qualità dei servizi pubblici di cui egli stesso si avvale. L'appalto, quale strumento il cui scopo primario è quello di permettere il conseguimento degli obiettivi di governo della cosa pubblica per una maggiore soddisfazione non solo degli stakeholders, ma di tutti coloro che ne sono coinvolti, anche indirettamente, a partire dai cittadini e dagli utenti, non può più essere considerato dall'operatore economico e dal funzionario

responsabilità disciplinare accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni".

pubblico, un mero mezzo per arricchirsi e per conseguire più o meno leciti vantaggi. Per poter seriamente affrontare la tematica del procurement pubblico in un'ottica di efficienza e concorrenza leale dei partecipanti alla gara, l'appalto non può essere circoscritto al solo processo di affidamento, poiché è costituito da un sistema molto più vasto, che trova il suo vertice nell'individuazione e nel raggiungimento degli obiettivi strategici dello Stato e nel contenimento dei costi per raggiungerli. La competizione fra gli operatori e la scelta di quello più adatto alla fornitura e l'affidamento della gara con i relativi interessi delle aziende coinvolte, sono elementi solo funzionali al raggiungimento degli obiettivi da parte della Pubblica Amministrazione, giacché questi ultimi rappresentano un interesse pubblico, superiore e pregnante, che sovrasta ogni altro interesse personale. Antecedente e prodromica all'affidamento è la fondamentale fase di identificazione degli obiettivi, di pianificazione delle spese, di bilanciamento fra fabbisogni ed impiego di risorse, in sintesi ciò che stabilisce il discrimine, in termini di risultati, di un'amministrazione efficace ed efficiente dalla maladministration[148].

Secondo il parere dell'ANAC le maggiori criticità, che potrebbero essere assunte quale indicatore di ricorrenza dei fenomeni di maladministration, sono: affidamenti illegittimi di appalti, con abuso di procedure d'urgenza, gare deserte, ribassi anomali, offerte plurime riconducibili ad un unico soggetto; inerzia nel bandire nuove gare al fine di prorogare i contratti scaduti; assenza di controlli; assunzioni clientelari; illegittime erogazioni di denaro pubblico; illegittimità nel rilascio di licenze ad autorizzazioni; provvedimenti giudiziari di comodo. Considerando il problema dal punto di vista soggettivo, per gli appalti di importo elevato prevalgono sistemi di turnazione fra aziende e cartelli, mentre per quelli di importi più modesti vengono generalmente coinvolti i livelli bassi dell'amministrazione, quali il direttore dei lavori ed i funzionari pubblici. La preponderanza delle dinamiche corruttive negli appalti pubblici, solleva non pochi dubbi nei confronti dei meccanismi di *deregulation* recentemente introdotti[149]. Rilevanza e complessità del procurement pubblico sono, poi, amplificati in determinati ambiti, quali la gestione dei servizi sociali e sanitari, poiché interessano settori di rilevanza costituzionale e bisogni primari e inalienabili della persona, fra cui spicca il diritto alla salute.

[148] Cassese S., *"Maladministration" e rimedi*, in *Il Foro Italiano*, 1992, p. 243 ss.
[149] In tal senso ANAC, *La corruzione in Italia (2016-2019) Numeri, luoghi e contropartite del malaffare*, p. 5 e ss. Verso tali meccanismi in più occasioni l'ANAC ha manifestato perplessità e preoccupazione.

Una notevole opportunità per rendere il sistema degli appalti pubblici più efficiente, meno corrotto e con minori possibilità di conflitto di interessi è, indubbiamente l'e-procurement, ossia l'utilizzo delle nuove tecnologie in materia di procurement pubblico. L'e-procurement è una modalità di gestione delle procedure negoziali per l'acquisto di beni e servizi, che sfrutta le possibilità offerte dalle moderne tecnologie telematiche, dallo sviluppo della rete internet e dell'e-commerce[150]. Il crescente interesse che ha sollevato a tutti i livelli l'introduzione di sistemi di e-procurement nel settore degli appalti pubblici è ascrivibile alla concreta possibilità, offerta dalla tecnologia di razionalizzare i processi di approvvigionamento e semplificare i passaggi necessari alle procedure di aggiudicazione, nonché effettuare controlli ed ottenere informazioni. L'uso di sistemi tecnologici avanzati per l'acquisto di beni e servizi comporta, poi, indubbi benefici in termini di diminuzione dei costi relativi alla ricerca del prodotto da parte delle amministrazioni aprendo altresì il mercato ad una più ampia concorrenza. L'uso della rete facilita la circolazione delle informazioni e l'accesso alle gare, rafforzando il principio della pubblicità e di *par condicio* delle imprese nella partecipazione alla gara. Infine, affidare la scelta del contraente ad un sistema automatizzato, garantendo la tracciabilità e l'archiviazione digitale di ogni singola fase, contribuisce ad accrescere la trasparenza del processo d'acquisto.

In considerazione dei notevoli vantaggi delle moderne tecnologie negli appalti, è stato pubblicato in Gazzetta Ufficiale il Decreto di Funzione Pubblica del 12 agosto 2021 n. 148 che regolamenta le modalità di digitalizzazione delle procedure dei contratti pubblici, da adottare ai sensi dell'articolo 44 del Codice dei contratti pubblici. Il decreto definisce i principi per la digitalizzazione dei processi di procurement delle Pubbliche Amministrazioni indicando le caratteristiche tecniche dei sistemi telematici per lo svolgimento delle attività connesse alle procedure di acquisto e di negoziazione dei contratti pubblici. Le piattaforme digitali per l'e-procurement, in uso alle stazioni appaltanti, devono rispondere a determinati requisiti funzionali e tecnologici. È, questa, una vera e propria standardizzazione tecnologica che favorisce l'interconnessione e l'interoperabilità dei dati tra le piattaforme di e-procurement esistenti e tra queste e gli organismi di vigilanza e controllo. Ciò costituisce un incontestabile vantaggio sia per le Pubbliche Amministrazioni che per le imprese che operano lecitamente, in quanto gli appalti elettronici contribuiscono in primis a ridurre il

[150] Sull'argomento si può consultare un'ambia bibliografia. A puro titolo esemplificativo: Lysons K., Farrington B., *Procurement and supply chain management*, Pearson, 2020; Nicoletti B., *Procurement 4.0 e trasformazione digitale*, Franco Angeli, 2019; Fiorentino L., La Chimia A.M. (a cura di), *Il procurement delle pubbliche amministrazioni tra innovazione e sostenibilità*, Il Mulino, aprile 2021.

rischio di infiltrazioni malavitose contrastando la corruzione e contribuendo all'emersione del conflitto di interessi, ma anche a migliorare l'efficienza amministrativa, sia diminuendo i costi di gestione delle procedure di gara che riducendo la durata del ciclo dell'appalto e gli oneri amministrativi a carico delle imprese.

1.3.2. Le criticità nell'e-procurement

Nonostante i passi avanti nella semplificazione e nei controlli su illegalità e conflitti di interessi, la digitalizzazione degli appalti pubblici presenta ancora notevoli criticità. In primis, il processo programmatorio previsto dall'articolo 21 del Codice dei contratti pubblici è eccessivamente rigido e statico, e non riesce perciò ad adattarsi al rapido cambiamento e sviluppo delle tecnologie. Nella fase di affidamento, poi, le cause di esclusione previste ex articolo 80[151] del Codice e le relative verifiche di veridicità di quanto dichiarato dagli operatori, rappresentano un vero e proprio "collo di bottiglia"[152] della procedura. Tale problematica potrebbe essere superata con la realizzazione della banca dati unica delle pubbliche amministrazioni. L'ICT e la digitalizzazione del procurement pubblico dovrebbero avere una disciplina specifica e dedicata nel Codice dei contratti pubblici, altrimenti l'inadeguatezza della normativa nel rapporto con l'innovazione può creare notevoli criticità, in particolare nei casi in cui sia necessaria una maggiore rapidità. Altri elementi necessari per rendere l'e-procurement più performante sono la creazione di una centrale di committenza unica, specializzata per gli acquisti ICT, ed un sistema di qualificazione per le stazioni appaltanti con specializzazione nelle ICT. In tal modo vi sarebbe anche una riduzione del numero delle centrali di committenza, oggi troppo elevato.

Un punto fondamentale resta quello della semplificazione e sburocratizzazione, poiché la complessità e farraginosità degli adempimenti amministrativi rappresentano gli ostacoli maggiori per i partecipanti alla gara. L'introduzione di una maggiore flessibilità nell'attribuzione del punteggio economico, di regole che rendano certe le tempistiche di affidamento anche in caso di contenzioso, nonché di forme di incentivazione nei casi di corretta esecuzione dei contratti e delle procedure digitalizzate, renderebbero il procurement pubblico, non solo più equo e fruibile per

[151] L'art. 80 (Motivi di esclusione) comma 5 lettera del d.lgs. n. 50 del 2016 (Codice dei contratti pubblici), prevede espressamente alla lettera d) l'esclusione dalla partecipazione alla procedura d'appalto nei casi in cui "la partecipazione dell'operatore economico determini una situazione di conflitto di interesse ai sensi dell'articolo 42, comma 2, non diversamente risolvibile".

[152] Bertocchini A., Giachi A., Tronu P., *Il procurement pubblico del digitale: dal planning all'execution*, Promo PA Fondazione di Anitec-Assinform, ottobre 2021, p. 8.

le imprese, ma anche più vantaggioso per l'amministrazione. Una maggiore interazione tra gli attori del procurement ICT è necessaria per avere procedure più rapide ed efficaci. In tal senso è l'orientamento del d.l. n. 77 del 2020, il c.d. Decreto Rilancio, il quale ha voluto ridefinire la normativa in un'ottica di semplificazione, nel quadro di una completa digitalizzazione del procurement pubblico entro tempi brevi, agendo altresì sul coordinamento fra gli attori, non solo a livello territoriale, ma anche economico e organizzativo, per una formulazione comune sia dei bisogni che delle procedure, con una standardizzazione delle valutazioni di conformità.

In fase di affidamento, per la velocizzazione delle procedure, è di primaria importanza l'interoperabilità delle banche dati. A tal fine può essere d'aiuto: la clusterizzazione delle informazioni con tecniche di intelligenza artificiale, quali bandi e proposte contrattuali tipizzate ed automatizzate; lo sviluppo di funzionalità che consentano all'operatore di simulare la propria situazione, per verificare se dispone dei requisiti richiesti; rendere interoperabili le risultanze dei diversi enti certificatori; la creazione di un fascicolo virtuale dell'operatore economico in possesso delle banche dati delle Pubbliche Amministrazioni. La banca dati unica in un sistema di interoperabilità consentirà la fruizione di un sistema di controllo e verifica più snello, preciso e rapido, basato sul c.d. principio *once only*, poiché un operatore che ha già partecipato ad una gara, potrà utilizzare i requisiti per la gara successiva senza doverli di nuovo dichiarare. Ciò significa che la PA potrà accedere alle verifiche dei requisiti già effettuate da altre stazioni appaltanti, senza interrogare nuovamente gli stessi soggetti. È, infine, auspicabile la costituzione di un network di e-procurement, con piattaforme autonome ma perfettamente compatibili ed interoperabili, che possano essere condivise fra tutti i fornitori in un regime di parità, e con le stesse amministrazioni[153].

1.3.3. Emersione del conflitto di interessi nel procurement pubblico

Secondo quanto previsto dal comma primo dell'art. 42 del Codice dei contratti pubblici "Le stazioni appaltanti prevedono misure adeguate per contrastare le frodi e la corruzione nonché per individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione degli appalti e delle concessioni, in modo da evitare qualsiasi distorsione della concorrenza e garantire la parità di trattamento di tutti gli operatori economici". Il comma secondo dello stesso art. 42 offre una definizione di conflitto di

[153] Op. cit., Bertocchini A., Giachi A., Tronu P., p. 13 ss.

interessi funzionale al procurement pubblico, affermando che "Si ha conflitto d'interesse quando il personale di una stazione appaltante o di un prestatore di servizi che, anche per conto della stazione appaltante, interviene nello svolgimento della procedura di aggiudicazione degli appalti e delle concessioni o può influenzarne, in qualsiasi modo, il risultato, ha, direttamente o indirettamente, un interesse finanziario, economico o altro interesse personale che può essere percepito come una minaccia alla sua imparzialità e indipendenza nel contesto della procedura di appalto o di concessione. In particolare, costituiscono situazione di conflitto di interesse quelle che determinano l'obbligo di astensione previste dall'articolo 7 del decreto del Presidente della Repubblica 16 aprile 2013, n. 62". Il predetto articolo del Codice Appalti prevede, per il personale della stazione appaltante, non solo un obbligo di adozione di misure adeguate per individuare, prevenire e risolvere ogni ipotesi di conflitto di interesse, ma altresì un obbligo di segnalazione ed astensione, ed un dovere di vigilanza. Gli obblighi di comunicazione e di astensione del personale che si trovi in una condizione di conflitto di interessi è stabilito dal comma 3. La mancata astensione da parte del personale della stazione appaltante è fonte di responsabilità disciplinare, nel rispetto del principio giuslavoristico di immediatezza e proporzionalità della sanzione, ma anche di eventuale responsabilità contabile e civile, nonché amministrativa e penale[154]. Ancor più specifico è il Codice di comportamento dei dipendenti dell'amministrazione, che all'art. 7 stabilisce che il dipendente si astiene dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri, ovvero di suoi parenti, affini entro il secondo grado, del coniuge o di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, di soggetti od organizzazioni con cui egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito significativi, di soggetti od organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di enti, associazioni anche non riconosciute, comitati, società o stabilimenti di cui sia amministratore o gerente o dirigente. Il dipendente si astiene in ogni altro caso in cui esistano gravi ragioni di convenienza. Sull'astensione decide il responsabile dell'ufficio di appartenenza. Quanto alle conseguenze della sussistenza di un conflitto di interessi, l'art. 80, comma 5 lettera d) del Codice dei contratti pubblici prevede che le stazioni appaltanti escludano dalla procedura d'appalto un operatore economico la cui partecipazione determini una situazione

[154] Per il comma 3 dell'art. 42 del Codice dei contratti pubblici, d.lgs. n. 50 del 2016 "Il personale che versa nelle ipotesi di cui al comma 2 è tenuto a darne comunicazione alla stazione appaltante, ad astenersi dal partecipare alla procedura di aggiudicazione degli appalti e delle concessioni. Fatte salve le ipotesi di responsabilità amministrativa e penale, la mancata astensione nei casi di cui al primo periodo costituisce comunque fonte di responsabilità disciplinare a carico del dipendente pubblico".

di conflitto di interesse non diversamente risolvibile, ovvero alla lettera m) l'esclusione dell'operatore economico che si trovi rispetto ad un altro partecipante, in una situazione di controllo analoga a quella delle società controllate o collegate di cui all'articolo 2359 del codice civile.

Ad avviso del Consiglio di Stato anche il potenziale rischio di compromettere l'imparzialità amministrativa è di per sé idoneo a configurare il conflitto di interessi, senza necessità che questo si traduca in un concreto beneficio nell'ambito della procedura. Secondo Palazzo Spada, difatti "Il conflitto di interessi non presuppone la realizzazione di un vantaggio competitivo, ma il potenziale rischio di minaccia alla imparzialità amministrativa"[155] ed in ogni fase in cui viene rilevato, anche in una fase più avanzata o finanche successivamente all'aggiudicazione "non può che trovare applicazione la misura demolitoria, che, secondo la regola generale, colpisce il provvedimento viziato dal conflitto di interessi"[156]. Le violazioni del dipendente che sorgono in funzione del dovere di dare comunicazione alla stazione appaltante di una situazione di conflitto di interessi e dell'obbligo di astensione dal partecipare alla procedura di affidamento sono fonte di sanzioni disciplinari, ferme restando responsabilità di natura civilistica o penalistica. Per il Consiglio di Stato, sez. III, 12 settembre 2019, n. 6150, "il conflitto di interessi può ricavarsi in via presuntiva dall'esistenza di un interesse personale del funzionario e dal ruolo che questi riveste nella procedura di gara tale da consentire di influenzare il risultato, per le informazioni privilegiate che ha a disposizione, ponendo in condizione di vantaggio un concorrente sugli altri". Lo stesso Giudice Amministrativo ha rilevato che ai fini dell'individuazione di una situazione di conflitto di interesse "è sufficiente il carattere anche solo potenziale dell'asimmetria informativa di cui abbia potuto godere un concorrente grazie all'acquisizione di elementi ignoti agli altri partecipanti per il tramite di un soggetto in rapporto diretto con la stazione appaltante, così come anche solo potenziale può configurarsi il conseguente, indebito vantaggio competitivo" (Consiglio di Stato, sez. III, sentenza 20 agosto 2020 n. 5151). Nella stessa sentenza, poi, i Giudici di Palazzo Spada affermano che l'ampia portata della disposizione dell'art. 42 del Codice dei contratti pubblici "consente di ricomprendere nel suo ambito di applicazione tutti coloro che con qualsiasi modalità e anche senza intervenire nella procedura (predisponendone gli atti o facendo parte della commissione giudicatrice) siano in grado di influenzarne il risultato".

[155] Cons. di Stato, sez. III, 14 gennaio 2019, n. 355.
[156] Consiglio di Stato, sez. V, sentenza 28 ottobre 2019 n. 7389.

Un importante chiarimento sui punti più incerti riguardanti il conflitto di interessi nel procurement pubblico, è rappresentato dalle Linee guida n. 15 dell'ANAC, del 5 giugno 2019. La partecipazione alla gara d'appalto da parte di soggetti appartenenti all'amministrazione in situazione di conflitto d'interessi, comporta l'insorgere di responsabilità penali, amministrative e disciplinari. La sussistenza di un conflitto di interessi per cui è obbligatoria l'astensione viene valutata per la sua gravità, se mette in pericolo "l'adempimento dei doveri di integrità, indipendenza e imparzialità del dipendente, considerando, altresì, il pregiudizio che potrebbe derivare al decoro e al prestigio dell'amministrazione di appartenenza"[157]. L'esclusione del concorrente dalla gara, annullamento dell'aggiudicazione e risoluzione del contratto è disposta come *extrema ratio*, qualora fosse impossibile la sostituzione del dipendente in conflitto d'interessi e l'avocazione dell'attività al responsabile del servizio[158]. È prevista la collocazione nei protocolli di legalità e patti di integrità, di prescrizioni a carico di concorrenti e soggetti affidatari, in cui si chiede una dichiarazione di sussistenza/insussistenza di conflitti di interessi con sanzioni in caso di violazione degli impegni sottoscritti, nonché attività formative e di sensibilizzazione del personale delle stazioni appaltanti. Queste ultime individuano preventivamente possibili situazioni di rischio, basandosi sulle indicazioni contenute in una tabella fornita dalla stessa ANAC[159]. La tabella annovera tutte le fasi della procedura, a partire dalla programmazione e progettazione, alla selezione e aggiudicazione, fino all'esecuzione e rendicontazione del contratto e prevede, fra le situazioni di rischio principali: la necessità di ricorrere a procedure motivate dall'urgenza e l'individuazione di lavori complessi; la validazione di un progetto privo dei requisiti richiesti; la definizione dei fabbisogni in base all'interesse personale di un operatore economico; l'anticipazione di informazioni sulla gara fornite ad un operatore economico; la nomina di soggetti compiacenti o la scelta di una tipologia contrattuale ovvero di una procedura di gara che possano favorire un operatore economico; l'inserimento di requisiti particolarmente restrittivi che possano disincentivare la partecipazione ad una gara o di clausole vessatorie; modalità di pubblicazione e di termini per la presentazione delle offerte volte a disincentivare la partecipazione alla gara; verifiche incomplete per avvantaggiare un operatore economico; mancato rispetto del principio della rotazione con inviti frequenti ai medesimi operatori; ricorso a varianti in corso d'opera con l'intento di favorire l'esecutore del contratto; riconoscimento di

[157] Linee guida n. 15 dell'ANAC, del 5 giugno 2019, art. 8 comma 2.
[158] Linee guida n. 15 dell'ANAC, del 5 giugno 2019, art. 9.
[159] Linee guida n. 15 dell'ANAC, del 5 giugno 2019, art.10.

importi non spettanti. Specifiche situazioni di rischio sono individuate nel Piano triennale per la prevenzione della corruzione, all'interno della mappatura dei processi nell'area di rischio "contratti pubblici". Tra le misure atte a prevenire il rischio di interferenza dovuto a conflitti di interesse meritano particolare attenzione quelle relative a obblighi di dichiarazione, di comunicazione e di astensione. È, inoltre, compito del Responsabile della prevenzione della corruzione e della trasparenza, d'intesa con il dirigente competente, monitorare l'effettiva rotazione degli incarichi negli uffici a maggior rischio di corruzione e conflitti di interessi.

In taluni casi può riscontrarsi una particolare forma di conflitto di interessi definita "strutturale", formalmente in linea con le disposizioni di legge in materia di conflitto di interessi poiché non limitata ad una ben definita tipologia di atti o procedimenti, ma generalizzata e permanente, strettamente connessa alle posizioni ricoperte ed alle funzioni attribuite al dipendente o funzionario pubblico. Tale ipotesi di conflitto si realizza allorché nel conferimento di un incarico ad un dipendente della Pubblica Amministrazione, l'imparzialità nell'espletamento dell'attività amministrativa risulta fortemente pregiudicata in modo continuato e sistematico, da preesistenti interessi estranei all'esercizio della medesima. L'importanza di tenere distinto il c.d. conflitto di interessi strutturale dalle altre tipologie, consta prevalentemente nel fatto che i rimedi debbano necessariamente essere differenziati. Difatti con il conflitto strutturale il rimedio dell'astensione potrebbe rivelarsi non idoneo, poiché sarebbe, di fatto, necessaria una continua astensione da parte dello stesso dipendente per ogni incarico a lui affidato con conseguente pregiudizio della continuità e del buon andamento dell'attività amministrativa. Occorre, pertanto, che le amministrazioni predispongano adeguati presidi di prevenzione del rischio. Lo strumento che si è mostrato più utile a tal fine è, indubbiamente, la c.d. segregazione delle funzioni. La segregazione di funzioni, ruoli e poteri è uno strumento fondamentale di *corporate governance*, finalizzato al coinvolgimento dei soggetti con diversi poteri, affinché nessuno possa disporre di poteri illimitati e svincolati dalla verifica di altri soggetti. Essa consiste nell'individuazione delle aree a rischio, e nel conseguente affidamento a più soggetti, delle varie fasi di procedimenti facenti parte di tali aree, avendo cura di assegnare la responsabilità del procedimento ad un soggetto diverso dal dirigente cui compete l'adozione del provvedimento finale. Con la segregazione dei poteri e delle funzioni si ha una distribuzione delle facoltà e responsabilità, favorendo l'attività di controllo di più soggetti sulle fasi più sensibili di ciascun processo.

Il ragionamento in termini di rischio di conflitto di interessi impone una valutazione concreta circa l'esclusione del soggetto in conflitto, quale rimedio volto a garantire il rispetto dei principi di trasparenza e di parità di trattamento tra gli offerenti. Tale valutazione emerge da due prospettive differenti ma convergenti: l'equidistanza della funzione amministrativa dagli interessi personali, ossia l'imparzialità, ed il pregiudizio da parte dei terzi riguardante la percezione di imparzialità dell'amministrazione[160]. Per entrambi i punti di osservazione si ritiene che la soluzione non possa essere orientata soltanto su un piano giuridico, ma debba necessariamente collocarsi su una visione moderna di gestione del rischio. Secondo autorevole dottrina, il problema principale è da riscontrarsi nella astrattezza e mancanza di tassatività delle situazioni che portano all'astensione[161]. Ciò è sicuramente condivisibile al fine di soddisfare esigenze di certezza del diritto, tuttavia emerge, quale elemento maggiormente determinante, non tanto il momento patologico ma la prevenzione tramite la gestione del rischio da parte delle amministrazioni. L'approccio metodologico *risk based* permette, difatti, il rilevamento dei fattori di rischio, valutati in termini di probabilità ed impatto all'interno di scenari[162], per ogni singola amministrazione. Soltanto partendo da tali premesse è possibile sostenere e facilitare l'emersione del conflitto di interessi nel procurement pubblico, agevolando il contrasto alla corruzione in un'ottica di prevenzione.

La mappatura delle aree di rischio rappresenta la prima fase della gestione del rischio, e concerne i processi istruttori e decisionali che conducono all'adozione dei provvedimenti, con l'obiettivo di individuare i probabili conflitti di interessi e prevenire rischi di corruzione connessi a ciascun processo. A tal fine giova operare una distinzione tra conflitti di interessi che emergono in situazioni "conclamate, palesi e soprattutto tipizzate (quali ad esempio i rapporti di parentela o coniugio) che sono poi quelle individuate dall'art. 7 del D.P.R. n. 62 del 2013" e conflitti di interessi "non conosciuti o non conoscibili, e soprattutto non tipizzati che si identificano con le gravi ragioni

[160] L'art. 42 del d.lgs. n. 50/2016 pone particolare attenzione alle implicazioni reputazionali dell'amministrazione, facendo esplicito riferimento ad ogni "interesse che può essere percepito come una minaccia". Al pari, le Linee Guida ANAC 2019 rilevano che l'interesse personale dell'agente, "che potrebbe porsi in contrasto con l'interesse pubblico alla scelta del miglior offerente, può essere di natura finanziaria, economica o dettato da particolari legami di parentela, affinità, convivenza o frequentazione abituale con i soggetti destinatari dell'azione amministrativa. Tale interesse deve essere tale da comportare la sussistenza di gravi ragioni di convenienza all'astensione, tra le quali va considerata il potenziale danno all'immagine di imparzialità dell'amministrazione nell'esercizio delle proprie funzioni".

[161] Cfr. Berrettini A., *Conflitto di interessi e contratti pubblici: un difficile equilibrio tra (in)certezza del diritto e tassatività delle situazioni conflittuali*, in Federalismi, 8 luglio 2020.

[162] Cfr. Di Rienzo M., Ferrarini A., *L'uso degli scenari nella valutazione dei conflitti di interessi potenziali*, in *Spazioetico*, 2020.

di convenienza"[163]. L'emersione del conflitto di interessi di situazioni tipizzate è, grazie all'ausilio degli strumenti informatici e delle banche dati della Pubblica Amministrazione, facilmente rilevabile, mentre maggiori difficoltà possono sorgere per l'emersione di conflitti non tipizzati, poiché basati soltanto sulle gravi ragioni di convenienza, ovvero su un interesse personale che può essere percepito come una minaccia all'imparzialità e indipendenza. Ancor più complessa è l'emersione di situazioni di potenziale conflitto d'interessi, ossia quegli eventi non ancora manifestati ma in grado di evolvere nel tempo fino a divenire situazioni tipizzate[164]. In tali ultimi casi, oltre all'utilizzo degli scenari, è necessario l'incrocio di grandi moli di dati (c.d. big data), grazie alle quali sarà possibile far emergere anche situazioni di potenziale conflitto. A complicare tali operazioni contribuisce, indubbiamente, la centralità del diritto alla tutela dei dati personali ed alla privacy, poiché gli algoritmi che processano quantità enormi di dati provenienti sia dai database pubblici che dalla rete, devono tuttavia trattare in maniera corretta i dati sensibili dei soggetti coinvolti nelle gare d'appalto e dei soggetti terzi.

Da quanto appena detto si può dedurre che la valutazione circa la sussistenza di una situazione di conflitto di interessi sia collegata ad uno scenario relativo ad un determinato soggetto in rapporto alla sua rete di relazioni sia nella sfera professionale che privata. Ciò che si vuole far emergere dalle attività di controllo non è un comportamento del soggetto, ma una situazione cui potrebbero conseguire condotte che favoriscono interessi secondari a danno di quelli pubblici primari. La valutazione di detta situazione di potenziale conflitto può avere come conseguenza l'astensione[165], l'esclusione del concorrente, e come extrema ratio l'annullamento della gara[166]. L'approccio c.d. *risk based* è valutato in funzione della probabilità, ma anche dell'impatto del

[163] Parere del Consiglio sullo Schema di Linee guida aventi ad oggetto "Individuazione e gestione dei conflitti di interesse nelle procedure di affidamento di contratti pubblici", in attuazione dell'articolo 213, comma 2, del Codice dei contratti pubblici del 2016.

[164] Cfr. Di Rienzo M., Ferrarini A., *L'uso degli scenari nella valutazione dei conflitti di interessi potenziali*, in *Spazioetico*, 2020, "le situazioni di "potenziale conflitto" sono, quindi, in primo luogo, quelle che, per loro natura, pur non costituendo allo stato una delle situazioni tipizzate, siano destinate ad evolvere in un conflitto tipizzato (ad es. un fidanzamento che si risolva in un matrimonio determinante la affinità con un concorrente)".

[165] La c.d. disclosure del dipendente dell'amministrazione che, a norma dell'art. 7 del Codice di comportamento deve essere indirizzata al superiore gerarchico, e sulla quale decide il responsabile dell'ufficio di appartenenza o il RPCT.

[166] Lorusso R., *Le condizioni per l'annullamento d'ufficio dell'aggiudicazione di una gara d'appalto*, in *Il diritto Amministrativo*, anno XIV, n. 6. Con riguardo all'annullamento della gara, secondo il TAR Lazio, 14.9.2016, n. 9728, la valutazione dell'irregolarità della procedura va svolta "non ex post, ma ex ante, ovvero con riferimento alla "potenziale" incidenza del sistema di gara sulla par condicio degli operatori, e non solo in relazione alle domande effettivamente pervenute". Pertanto l'amministrazione può correttamente esercitare il potere di autotutela, qualora dubitasse della regolarità della procedura in relazione a vizi che, pur inidonei ad inficiare il provvedimento finale oggetto di autotutela, costituiscano comunque un potenziale elemento di irregolarità del confronto concorrenziale tra gli operatori economici.

potenziale danno all'immagine dell'amministrazione[167]. La configurazione degli interessi primari sarà, pertanto, data da: imparzialità, intesa come equidistanza dagli interessi in gioco; percezione di imparzialità, intesa quale tutela dell'immagine dell'amministrazione; buon andamento, inteso come efficacia delle procedure di selezione dell'aggiudicatario. L'interesse secondario sarà invece quello di avvantaggiare un concorrente della gara. Esso è idoneo a minacciare gli interessi primari. Nella maggior parte dei casi risulta più complessa proprio l'emersione dell'interesse secondario, poiché inizialmente non è sempre agevolmente riconoscibile e può venire alla luce solo in un secondo momento. Necessita, pertanto, di essere monitorato nel tempo, durante tutte le fasi del processo di approvvigionamento ed anche in quelle immediatamente successive alla sua conclusione.

In tali situazioni gioca un ruolo primario, ai fini dell'emersione del conflitto di interessi, il fattore probabilità riguardante il rischio di alterazione della concorrenza, dipendente dall'esistenza di interessi secondari, che possano sorgere da comportamenti successivi allo scenario iniziale. Il rischio viene individuato quale più elevato nell'ipotesi in cui successivamente alla fase di emersione del fabbisogno dell'amministrazione si verificano comportamenti del dipendente quali, ad esempio, inviare una candidatura o costituire una società con un concorrente. Tale situazione è conoscibile dalla stazione appaltante, soltanto per mezzo di una segnalazione interna (whistleblowing), o con l'astensione volontaria da parte del dipendente, ovvero con l'ausilio di algoritmi che analizzano ed incrociano grandi quantità di dati, come i predetti big data analytics. Valutare la probabilità permette di identificare le misure più idonee alla gestione del rischio già durante la fase di emersione del fabbisogno, prima che gli interessi secondari diventino effettivi e non solo potenziali.

Con riferimento alla potenzialità o attualità del conflitto di interessi, la stessa ANAC nelle "Linee guida per l'adozione dei Codici di comportamento nel SSN"[168] offre un chiarimento operando una distinzione fra varie tipologie di conflitto di interessi: attuale, presente al momento dell'azione o decisione dell'agente pubblico; potenziale, il quale può diventare attuale in un periodo successivo; conflitto di interessi apparente, che può essere percepito dall'esterno come tale; diretto, che comporta il soddisfacimento di un interesse secondario del dipendente pubblico;

[167] Cfr. Di Rienzo M., Ferrarini A., *La gestione del conflitto di interessi nei contratti pubblici*, in *Spazioetico*, marzo 2021.
[168] Linee guida per l'adozione dei Codici di comportamento nel SSN, approvate in data 20 settembre 2016 da ANAC, Ministero della Salute e AGENAS.

indiretto, che attiene a soggetti diversi dall'agente pubblico. Pur essendo più pericolosi ed immediati i conflitti attuali e diretti, è certamente più complessa l'emersione di quelli potenziali ed indiretti, poiché meno conoscibili e più inclini a variazioni nel tempo. Le stazioni appaltanti devono essere, pertanto, chiamate ad effettuare valutazioni *ex ante* sul rischio di conflitti e convergenze di interessi: a tal fine sono necessari percorsi formativi del personale allo scopo di migliorare la sua capacità di individuarli, riconoscerli e gestirli[169].

In definitiva la valutazione delle situazioni di conflitto di interessi si basa su un'indagine approfondita sulla minaccia all'imparzialità in termini di probabilità, e sulla minaccia alla percezione di imparzialità in termini di impatto[170]. Secondo il modello d'approccio risk based il conflitto di interessi non può essere affrontato come problema individuale dell'agente pubblico chiamato ad eseguire valutazioni nelle procedure di gara, ma presuppone una responsabilità dell'intera organizzazione. È, questo, un punto nevralgico riguardante il contrasto al conflitto di interessi e la prevenzione dei fenomeni corruttivi: l'allargamento delle responsabilità ad un numero più ampio possibile di soggetti dell'organizzazione, per far sì che più figure professionali si adoperino all'emersione di ogni situazione anomala, ed alla risoluzione di problematiche che potrebbero incidere sul buon andamento dell'amministrazione.

La gestione del rischio riduce l'incertezza rispetto ad una situazione che potrebbe causare un danno, ed in primis riduce il rischio di un evento corruttivo sorgente da un conflitto di interessi[171]. Il c.d. *risk assessment* ossia la valutazione del rischio e l'identificazione dei pericoli che potrebbero avere un impatto negativo sulla capacità di un'organizzazione, consente di prevedere situazioni di conflitto di interessi basandosi su un modello focalizzato sugli interessi secondari e sulla dimensione relazionale ed economica dei soggetti. In essi svolge un ruolo primario il fattore temporale, poiché conflitti e convergenze mutano nel tempo nei confronti degli interessi in gioco. È necessario, pertanto, ai fini dell'emersione dei conflitti, monitorare le relazioni sensibili dei dipendenti dell'amministrazione e le trasformazioni che esse subiscono, nonché gli scenari che si potrebbero generare dando vita ad un conflitto d'interessi prima potenziale, poi attuale e successivamente anche ad un evento corruttivo. In ogni caso è necessario analizzare informazioni

[169] Di Rienzo M., Ferrarini A., *La valutazione del conflitto di interessi nella gestione dei contratti pubblici – Due casi di studio*, in *Azienditalia*, maggio 2019, p. 756 ss.
[170] Id, p. 13.
[171] Il Piano Nazionale Anticorruzione del 2019 parla di convergenze e conflitti di interessi quali "fattori abilitanti" del rischio di corruzione.

sia in possesso dell'amministrazione stessa, come ad esempio i dati riguardanti i dipendenti, ma anche provenienti dall'esterno. Altre informazioni relative alle relazioni interpersonali, come ad esempio le attività lavorative svolte dai familiari del dipendente pubblico, potrebbero essere ricavate direttamente dai dipendenti stessi, rendendo più circostanziate e precise le autodichiarazioni di assenza di conflitto di interessi.

1.3.4. Tecniche di analisi ed elaborazione dati nel procurement pubblico

Con il recente sviluppo delle tecnologie informatiche, con algoritmi sempre più avanzati e con la diffusione dell'intelligenza artificiale, anche il concetto di data analysis, ossia analisi dei dati è oggi mutato, intendendosi con tale locuzione un'operazione informatica che, oltre a permettere di raccogliere e filtrare grandi quantità di dati complessi provenienti da diverse fonti, le razionalizza e relaziona le une con le altre. Le attuali piattaforme di e-procurement permettono l'acquisizione e condivisione di elevate quantità di dati provenienti da diverse fonti, che le tecnologie di intelligenza artificiale possono elaborare superando i tradizionali metodi basati prevalentemente su dati storici, producendo previsioni accurate e scenari complessi riguardanti il rischio.

Un settore in cui l'evoluzione di sistemi informatici di analisi ha avuto maggior sviluppo e particolare efficacia è proprio il procurement pubblico[172], poiché oltre a fornire i tradizionali report di spesa da cui desumere strategie di efficienza dell'amministrazione, ha offerto strumenti di *spend analysis*, ossia l'analisi delle spese, *predictive analytics*, ossia l'analisi di dati per prevedere futuri approvvigionamenti, *prescriptive analytics*, ossia l'utilizzo dei big data per offrire soluzioni agli eventi predittivi, e gestione intelligente dei contratti (c.d. *smart contract*). Con riguardo al conflitto di interessi, poi, l'analisi avanzata consente l'interazione dei dati e lo studio di eventi globali e non, al fine di far emergere situazioni di rischio che possano avere un impatto sulla catena di approvvigionamento e sulla imparzialità dell'amministrazione.

L'intelligenza artificiale, la *robotic process automation* e la *cognitive automation*, permettono oggi di elaborare grandi quantità di dati e simulare funzionalità cognitive dell'uomo, mettendo in correlazione dati ed eventi per estrapolarne delle informazioni, collegarle ed individuare i fattori

[172] La digitalizzazione delle pubbliche amministrazioni ha un ruolo centrale nel PNRR italiano del mese di maggio 2021. Agli interventi in materia di digitalizzazione della Pubblica Amministrazione sono destinate risorse pari a 9,75 miliardi di euro, distribuiti in tre tipologie di investimenti: investimenti per lo sviluppo di servizi digitali; investimenti in dotazioni infrastrutturali per garantire l'interoperabilità e la condivisione di informazione tra le Pubbliche Amministrazioni; investimenti in infrastrutture digitali e cyber security.

di rischio. Le capacità di *interactive learning* del sistema, ossia l'apprendimento automatico incrementale e il *deep learning*, sono indispensabili quando i dati da processare sono estremamente numerosi, poiché consentono lo svolgimento di compiti senza una programmazione specifica preventiva. Le piattaforme di e-procurement, difatti, per la enorme mole di dati da analizzare, devono essere in grado autonomamente, ossia senza intervento dell'uomo, di processare ed estrapolare solo quelli utili per un determinato scopo. Le fonti che alimentano le piattaforme di e-procurement contengono svariati miliardi di informazioni e riguardano la raccolta di: dati dei fornitori; dati interni all'amministrazione, quali analisi e valutazione delle prestazioni, verifiche di documenti e aggiudicazioni di offerte; dati recuperati da sistemi interni come *supply chain*, qualità, sicurezza, ambiente; dati acquisiti in modo automatico e strutturato da Information Service Provider, già certificati, quali gli indici dei prezzi delle materie prime; dati web strutturati e non strutturati che costituiscono una parte preponderante del complesso dei big data, la cui affidabilità è, invero, estremamente variabile, richiedendo pertanto soluzioni avanzate di intelligenza artificiale al fine di filtrare rapidamente tali informazioni.

Grazie ai data analytics ed alla elaborazione con strumenti di intelligenza artificiale, da un enorme volume di dati vengono estratte le informazioni rilevanti ai fini della riduzione del rischio mettendo l'amministrazione in condizioni di far emergere il conflitto di interessi e scegliere la strategia più valida per il contrasto ai fenomeni corruttivi. L'introduzione di sistemi dotati di maggiori capacità cognitive permette, altresì, un'analisi predittiva con la possibilità di stabilire con una certa accuratezza, quali siano gli scenari che presentano maggiori rischi e quale di essi può concretizzarsi con maggiori probabilità.

L'utilizzo delle tecnologie per la gestione dell'intero ciclo di approvvigionamento è uno dei principali obiettivi delle Direttive europee volte ad incrementare la qualità degli appalti in ottica di semplificazione, efficacia, trasparenza e partecipazione. Piattaforme di e-procurement, tecnologia *blockchain* e forme basiche di intelligenza artificiale possono velocizzare l'azione e rendere efficaci e sicuri i correlati processi di verifica, conferendo immutabilità agli elementi sui quali i controlli saranno effettuati. Trasparenza, monitoraggio e maggiori possibilità di verifica, condivisione ed analisi avanzata dei dati per l'emersione del conflitto di interessi sono i punti di forza dell'e-procurement. Tuttavia tali punti di forza, senza un elemento di riequilibrio possono trasformarsi in punti di vulnerabilità, poiché l'utilizzo indiscriminato dei dati di cui è in possesso l'amministrazione e che possono essere da essa raccolti e processati, potrebbe violare il diritto

alla privacy e alla tutela dei dati personali. A tal fine sono necessarie attente e scrupolose linee guida riguardanti i processi di analisi delle informazioni, che limitino l'utilizzo e divulgazione dei dati personali, in un'ottica di contemperamento di esigenze di pubblicità e trasparenza con i confliggenti diritti di tutela della privacy, anche nel rispetto del GDPR emanato dall'UE[173]. In tale ottica l'amministrazione deve procedere ad una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, così come prescritto all'art. 35 comma 1 dello stesso GDPR. Il Regolamento pone particolare attenzione proprio a quei trattamenti che presuppongono l'utilizzo di nuove tecnologie, definendoli "a rischio elevato per i diritti e le libertà delle persone fisiche".

1.3.5. Procedura telematica di segnalazione da parte del whistleblower

Il whistleblowing rappresenta un importante strumento per l'emersione di illeciti ed irregolarità nella Pubblica Amministrazione, in particolare nei settori a maggior rischio di corruzione e conflitto di interessi quali gli appalti ed i concorsi pubblici. L'attività di monitoraggio dell'ANAC ha consentito di rilevare che le segnalazioni pervenute dai whistleblower riguardano principalmente gli appalti, l'affidamento di incarichi amministrativi di vertice ed i concorsi pubblici. Il preoccupante tasso di irregolarità nei contratti pubblici in Italia potrà, nei prossimi anni, subire un forte decremento se si riuscirà a creare un clima di fiducia dei dipendenti pubblici e dei cittadini comuni nei confronti dello strumento della segnalazione. Oltre alle tutele che la legge ed i codici di comportamento delle amministrazioni hanno predisposto a protezione del whistleblower, un elemento che può decretare o meno la riuscita di tale strumento è la semplicità, funzionalità e riservatezza dei canali tramite cui effettuare le segnalazioni. Un importante passo avanti in tal senso è l'aggiunta ai canali tradizionali, della procedura telematica di segnalazione, tramite apposita piattaforma on-line. Oltre ad essere presente una piattaforma istituzionale predisposta dall'ANAC, sicura e *user friendly*, la Direttiva del Parlamento Europeo e del Consiglio europeo del 23 ottobre 2019, n. 1937/0/201, ha imposto alle aziende private con oltre cinquanta dipendenti la predisposizione di una piattaforma per le segnalazioni.

La segnalazione da parte del whistleblower deve essere presentata al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) o all'ANAC unicamente mediante i canali messi a disposizione dall'amministrazione. Essa deve essere circostanziata e vi deve essere la possibilità di identificare il segnalante, per evitare di impegnare l'amministrazione su meri

[173] General Data Protection Regulation, Regolamento 679 del 2016.

sospetti o voci infondate. Le segnalazioni anonime, ossia prive delle generalità del soggetto che effettua la segnalazione, anche se trasmesse con le modalità prescritte, non vengono generalmente prese in considerazione.

Sono ammesse diverse tipologie di segnalazione, secondo il grado di riservatezza che il segnalante richiede gli venga garantito:

a. segnalazioni aperte, in cui il segnalante rivela la propria identità e non chiede di rimanere sconosciuto all'incolpato, prestando consenso alla comunicazione del suo nominativo allorché essa si renda necessaria;
b. segnalazioni esplicite riservate al RPCT, in cui il segnalante rivela la sua identità al RPCT, ma non presta consenso ad informare l'incolpato;
c. segnalazioni a riservatezza rinforzata o esplicite *ex post*, in cui il segnalante presenta una segnalazione identificandosi, ma tale identificazione rimane nascosta anche al RPCT che può conoscere l'identità del segnalante in un secondo momento, solo se indispensabile alla trattazione del caso, mentre l'incolpato non può conoscerla.

La procedura lascia impregiudicata la responsabilità penale, civile e disciplinare del whistleblower nell'ipotesi di segnalazione calunniosa o diffamatoria. Sono altresì fonte di responsabilità, in sede disciplinare o nelle sedi competenti, eventuali forme di abuso della procedura, quali le segnalazioni manifestamente opportunistiche e ogni altra ipotesi di intenzionale strumentalizzazione.

Le segnalazioni possono essere presentate al RPCT mediante consegna diretta di dichiarazione scritta, ovvero verbalmente mediante dichiarazione a voce al RPCT che dovrà redigere apposito verbale, o anche per e-mail o posta tradizionale, ma è preferibile il sistema telematico per il maggior livello di sicurezza e di riservatezza. La piattaforma telematica, fornita dall'ANAC in *open source* per ogni amministrazione, consente la compilazione, l'invio e la ricezione delle segnalazioni di presunti fatti illeciti nonché la possibilità per l'ufficio del Responsabile della prevenzione della corruzione e della trasparenza che riceve tali segnalazioni, di comunicare in forma riservata con il segnalante senza conoscerne l'identità. Il modulo on-line per la segnalazione è semplice da compilare ed al tempo stesso completo e preciso. Offre al whistleblower non solo la possibilità di circostanziare la propria segnalazione, ma anche di aggiungere ulteriori informazioni, comunicare le eventuali misure ritorsive subite, infine di aggiungere allegati a prova della segnalazione,

nonché evidenze multimediali, fra cui video e registrazioni audio. Il canale della piattaforma telematica è estremamente sicuro, in quanto protetto da crittografia asimmetrica simile a quella della posta elettronica certificata, e garantisce la segretezza e l'immutabilità della segnalazione. La piattaforma dispone, poi, di un *firewall* integrato con stringenti regole, che limitano gli accessi e le azioni agli esclusivi compiti dedicati al software, riducendo al massimo i rischi di hackeraggio ed accessi illegittimi ai dati inseriti dal segnalatore.

1.3.6. Aspetti processualpenalistici delle segnalazioni in un'ottica generalpreventiva

In un'ottica non solo di repressione ma soprattutto di prevenzione dei fenomeni corruttivi, la vigente normativa anti corruzione svolge una funzione prevalentemente generalpreventiva, poiché ha, nei confronti dei consociati, un'efficacia deterrente per dissuaderli dal porre in essere comportamenti delittuosi. In tale ambito si inseriscono le norme sul whistleblowing, aventi la finalità principale di creare un canale privilegiato di controlli, posti in essere dagli stessi dipendenti dell'amministrazione, per scoraggiare la commissione di illeciti da parte di colleghi o superiori gerarchici. Nello specifico settore degli appalti il perimetro del whistleblowing si è recentemente ampliato considerevolmente, e forse inaspettatamente, con la legge "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea – legge di delegazione europea 2021", approvata in via definitiva il 2 agosto 2022, che ha per la prima volta in Italia, consentito e protetto le segnalazioni anonime limitatamente ad appalti e riciclaggio, mercato interno e atti che violano le norme in materia di imposta sulle società.

Punto fondamentale del complesso normativo sul whistleblowing è la tutela del segnalante e la segretezza della sua identità. La legge anti corruzione del 2012 si impegna, difatti, a tutelare l'identità del segnalante nel caso di procedimento disciplinare. Essa può essere rivelata solo se necessaria ai fini dell'esercizio del potere disciplinare, mentre nel caso in cui dalla segnalazione abbia inizio un procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti dell'art. 329 c.p.p.[174]. La denuncia del whistleblower è, infine, sottratta al diritto di accesso civico previsto dalla legge su procedimento amministrativo, legge 241/1990 e successive modifiche. Tuttavia le tutele per il whistleblower non sono garantite se è accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o

[174] Secondo l'art. 329 c.p.p. gli atti di indagine sono mantenuti segreti solo fino alla conclusione delle indagini preliminari, ovvero fino al momento in cui la persona sottoposta alle indagini ha il diritto di essere informata di determinati atti compiuti dal Pubblico Ministero.

diffamazione, ovvero la sua responsabilità civile nei casi di dolo o colpa grave. È invece esclusa la responsabilità penale del whistleblower per il reato di rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.), nel caso in cui egli sveli notizie coperte dall'obbligo del segreto d'ufficio al fine di far emergere un illecito.

Secondo la Cassazione penale[175] il contenuto delle rivelazioni del whistleblower non costituisce mero spunto investigativo, bensì assurge al rango di vera e propria dichiarazione accusatoria, in quanto il canale deputato alla segnalazione di possibili violazioni commesse da colleghi garantisce la riservatezza del segnalante ma non è anonimo, poiché il whistleblower è sempre individuabile. Non si dimentichi, poi, che il whistleblower che effettua la segnalazione è a tutti gli effetti un potenziale testimone nel processo penale. In caso di violazione della legge penale per acquisire informazioni al fine di compiere la segnalazione, il whistleblower non sarà ammesso a giustificarsi invocando di avere adempiuto ad un dovere (art. 51 c.p.), in quanto nessuna norma giuridica prevede un dovere giuridico di segnalazione (Cass. Pen., Sez. V, n. 35792 del 2018).

[175] Cass. Pen., Sez. VI, 31 gennaio-27 febbraio 2018, sentenze n. 9041 e n. 9047.

Capitolo 2. Le nuove tecnologie per l'individuazione di corruzione e conflitto d'interessi

2.1. Tecnologia e diritto

2.1.1. L'evoluzione tecnologica a supporto della legalità

Lo sviluppo tecnologico e le ICT (Information and Communication Technologies) in particolare, hanno rivoluzionato ogni sfaccettatura della vita dei cittadini del terzo millennio, compreso il mondo lavorativo e professionale. Anche il settore del diritto è stato travolto dal progresso tecnologico, non solo in sede di formazione della prova (ad esempio con l'analisi del DNA), ma nella stessa attività di *routine* del giurista impegnato nel deposito di atti (ad esempio il processo civile telematico, il deposito di istanze tramite PEC, la firma elettronica per sottoscrivere gli atti). La stretta connessione fra nuove tecnologie e diritto è, così, diventata evidente insieme a tutti i suoi vantaggi, anche per coloro che fino a pochi anni addietro continuavano a negarla, rimanendo legati ad una visione "analogica" del mondo giuridico. È, difatti, innegabile che la convergenza fra diritto e nuove tecnologie informatiche e telematiche rappresenti un arricchimento notevole per il settore giuridico sotto ogni punto di vista, nonché un'opportunità ulteriore per il futuro. Si pensi, a puro titolo esemplificativo, al supporto della tecnologia nel processo penale e civile odierno, alle moderne tecniche investigative ed all'utilizzo di fascicoli e archivi informatici in sostituzione di quelli cartacei. A ben vedere tale rapporto non è unilaterale ma reciproco: da un lato è evidente la trasformazione della disciplina giuridica grazie al supporto dell'informatica, d'altro canto non si deve, tuttavia, dimenticare la necessaria applicazione del diritto anche all'uso delle tecnologie digitali ed alla disciplina informatica, per porre regole certe e predeterminate anche nell'ambito di suddetto settore.

Il supporto che lo sviluppo tecnologico offre al mondo giuridico non riguarda solo il momento patologico, ossia l'ambito processuale del diritto, ma si allarga fino a ricomprendere la legalità in senso generale, e nello specifico la prevenzione dalla commissione di attività illecite. Tecnologie sempre più sofisticate hanno, difatti, non solo rappresentato un valido deterrente per la commissione di illeciti, ma anche consentito di individuare e localizzare preventivamente situazioni ed aree a rischio illegalità, fornendo strumenti per fermare *ab origine* il comportamento vietato. Sono ormai numerosi i Paesi che si servono, con soddisfacenti risultati, di tecniche di

polizia predittiva (c.d. *predictive policing*) al fine di prevenire le attività illecite, mentre più perplessità suscita fra i giuristi l'utilizzo, ancora sperimentale e solo in pochi Paesi nel panorama mondiale, della c.d. giustizia predittiva, ossia la decisione automatizzata in ambito processuale, effettuata sulla base di un software fornito di intelligenza artificiale.

L'impiego delle tecnologie più moderne di machine learning ed intelligenza artificiale deve, tuttavia, avvenire con particolare attenzione e sensibilità, poiché notevole è il rischio di violare i diritti umani fondamentali e discriminare alcune etnie o categorie di persone, dimenticando quei princìpi di eguaglianza e rispetto della dignità e personalità di ogni individuo. Permettere, inoltre, alla macchina di prevalere sul buonsenso, la prudenza, la razionalità, apre la strada a decisioni basate sui risultati logici ma privi di sentimento umano, compiute da un dispositivo comunque congegnato dall'uomo, perciò in ogni caso soggetto ad errori. Una vicenda emblematica sui suddetti rischi è rappresentata dal noto "caso Loomis"[176], nel quale la Corte Suprema del Wisconsin era stata chiamata a pronunciarsi sull'appello del sig. Loomis, la cui pena a sei anni di reclusione era stata comminata dal Tribunale circondariale di La Crosse. Nel determinare la pena i giudici si erano basati sui risultati elaborati da un software chiamato COMPAS (Correctional offender management profiling for alternative sanctions), il quale aveva identificato l'imputato quale soggetto ad alto rischio di recidiva. Nella sentenza, la Corte Suprema conferma la pena affermando che, seppure l'utilizzo di software su cui basare la decisione dei tribunali debba essere ristretto con limitazioni e cautele, il loro impiego nei giudizi di determinazione della pena è del tutto legittimo.

Le immense potenzialità degli algoritmi e dell'intelligenza artificiale non devono essere fuorvianti poiché, come ci insegna il caso Loomis, i risultati dell'analisi dei dati devono essere comunque sottoposti all'interpretazione ed alla lettura effettuate dalla mente umana. Bisogna, infatti, considerare due limiti che li contraddistinguono: l'opacità algoritmica e la mancanza di percezione diretta. Con opacità algoritmica o *black box algorithm* si identifica la difficoltà anche per lo sviluppatore che lo ha progettato nel conoscere i processi per cui un algoritmo giunge ad un determinato risultato, mentre la mancanza di percezione diretta attiene alla presentazione del risultato come mero dato di fatto e non come l'esito di un processo selettivo tra varie

[176] State o Wisconsin vs. Eric L. Loomis, 13 luglio 2016.

possibilità[177]. I risultati di un'analisi dati non sono quindi incontestabili ed indiscutibili, ed il loro utilizzo deve essere ridimensionato qualora entrino in contrasto con il rispetto dei diritti fondamentali della persona.

2.2. Le nuove tecnologie digitali per contrastare la corruzione

2.2.1. Il ruolo di digitalizzazione e open data nel contrasto alla corruzione

La stretta correlazione fra la diffusione delle nuove tecnologie e l'efficacia del contrasto/contenimento dei fenomeni corruttivi è, oggi, innegabile. L'OCSE ha in più occasioni sostenuto l'importanza e l'efficacia dell'utilizzo delle nuove tecnologie digitali per prevenire e combattere la corruzione ed il conflitto d'interessi. A tal proposito il report dell'OCSE "Analytics for Integrity – Data-driven approaches for enhancing corruption and fraud risk assessments" del 2019 sottolinea come la gestione della corruzione sia più efficace con la digitalizzazione, in quanto a differenza del passato l'amministrazione riesce ad analizzare in maniera corretta grandi quantità di dati in suo possesso. In un più ampio disegno di open government[178] e di accountability dell'amministrazione, l'OCSE ha mostrato massimo impegno nella promozione della trasparenza tramite l'incremento dell'impiego di nuove tecnologie. Non vi è dubbio alcuno che al crescere della digitalizzazione si ha un aumento della trasparenza dell'attività amministrativa e maggiori possibilità di controllo, con conseguente decremento di conflitti di interessi e fenomeni legati alla corruzione. Tuttavia la digitalizzazione da sola non basta, poiché per conseguire risultati soddisfacenti, è necessario affiancare ad essa anche un efficace apparato di comunicazione fra i vari sistemi informativi: le amministrazioni sono, difatti, spesso incapaci di comunicare con un sistema centrale e la frammentazione delle banche dati in possesso della P.A. rende impossibile qualsivoglia coordinamento, trasformando preziose informazioni in dati di difficile utilizzazione. I dati in possesso degli enti pubblici rappresentano, difatti, un fondamentale patrimonio informativo di ogni Paese emancipato, ma per rendere effettiva la loro utilità è necessario un continuo interscambio fra essi. È, pertanto, importante ampliare ed aggiornare continuamente

[177] Sul punto, D. Pedreschi, F. Giannotti, R. Guidotti, A. Monreale, L. Pappalardo, S. Ruggieri, F. Turini, *Open the Black Box. Data-Driven Explanation of Black Box Decision Systems*, in *ArXiv Preprint*, N. 1/2018, p. 4 ss., e Y. Citton, *Notre inconscient numérique. Comment les infrastructures du web transforment notre esprit*, in La *Revue du Crieur*, n. 4/2016, e Diakopoulos N., *Algorithmic Accountability Reporting: On the Investigation of Black Boxes. Report, Tow Center for Digital Journalism*, Columbia University, 2013.

[178] Open Government Project (OGP) dell'OCSE. Il 14 dicembre 2017 il Consiglio dell'OCSE ha adottato la nuova Raccomandazione in materia di open government [C(2017)140].

tale patrimonio, incentivare lo scambio fra le amministrazioni e con i privati, nonché promuovere la trasparenza ad ogni livello.

A tal fine acquisiscono sempre più rilevanza per le amministrazioni gli open data[179] ed i big data, enormi quantità di dati disponibili in formato aperto ed accessibili a tutti, nonché la corretta analisi delle relative informazioni in essi contenute. Proprio con l'analisi di massicce quantità di dati, il c.d. *data mining*, in molti Paesi si riescono a monitorare i sistemi di e-procurement al fine di prevenire collusioni evitando conflitti di interessi. Prevenzione della corruzione e valutazione del rischio di conflitti d'interessi costituiscono una base solida per le decisioni sulle strategie amministrative e sull'allocazione di risorse. Un Paese all'avanguardia in tale materia è la Corea del Sud che grazie ad un sofisticato sistema software dotato di intelligenza artificiale avanzata[180], riesce ad analizzare grandi quantità di dati per l'individuazione di eventi corruttivi e conflitti di interessi, permettendo agli analisti di prevenire oltre il 70 per cento dell'illegalità negli appalti pubblici.

A livello europeo la "Strategia in materia di dati"[181] facente parte del pacchetto di misure per il futuro digitale dell'Europa, integra la comunicazione generale su Shaping Europe's digital future, si affianca al Libro Bianco sull'Intelligenza Artificiale (IA) e al Rapporto su sicurezza dei prodotti e regime di responsabilità alla luce degli sviluppi dell'IA, dell'IoT[182] e della robotica, evidenziando il valore dei dati pubblici quale bene comune strategico e primario di un Paese e l'importanza del loro corretto utilizzo. Anche la Direttiva (UE) 2019/1024 del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, insiste sull'importanza del patrimonio informativo della P.A. quale *asset* strategico per lo sviluppo di una nazione, in un'ottica di disponibilità di tali dati ai cittadini ed imprese, in forma aperta a tutti, condivisa e riutilizzabile. È il nuovo concetto di *Open Government Data*, alla cui base vi sono concetti semplici

[179] Sugli open data, a puro titolo esemplificativo, Monino J.L., Sedkaoui S., *Big data, open data and data development*, Willey, 2016; Bolognini L. (a cura di), *Privacy e libero mercato*, Giuffré, 2021; Aliprandi S. (a cura di), *Il fenomeno open data. Indicazioni e norme per un mondo di dati aperti, Ledizioni*, 2014; Cazzanti R., *Open data e nativi digitali*, Libreriauniversitaria, 2016;

[180] Identificato con l'acronimo BRIAS, Bid-Rigging Indicator Analysis System, col quale la Korea Fair Trade Commission riesce ad analizzare grandi volumi di dati di enti pubblici creando un punteggio di probabilità per il c.d. rigging delle offerte, schema fraudolento nelle aste di appalto che porta a offerte non competitive, poiché predisposto da funzionari corrotti.

[181] Commissione europea, Strategia europea in materia di dati, 19 febbraio 2020.

[182] Acronimo di Internet of Things, comprendente gli smart objects, oggetti intelligenti tra loro interconnessi, che hanno la caratteristica di poter scambiare le informazioni. Sull'argomento Za S., *Internet of things. Gli ecosistemi digitali nell'era degli oggetti interconnessi*, Luiss University Press, II edizione, ottobre 2021.

e moderni, quali la disponibilità senza restrizioni di tempo e informazioni, la possibilità di incrociare dati e l'interoperabilità per poterli confrontare e combinare, ed il riutilizzo da parte dei terzi. Tale influenza posta in essere dall'utilizzo dei dati può, tuttavia, apparire pericolosa se non viene effettuato un serrato controllo riguardo dati personali e sensibili della persona. La pubblicità dei dati in formato aperto, accessibile a tutti, la c.d. partecipazione universale, la conoscibilità ed utilizzabilità dei dati da parte di ogni persona, trovano difatti un limite, nel loro utilizzo discriminatorio o tendenzioso, nell'offesa ai diritti dell'uomo e della terza generazione fra cui il diritto alla privacy, la tutela dei dati personali ed il diritto all'oblio.

Gli open data nascono da un principio di trasparenza del settore pubblico, che nel nostro Paese viene introdotto esplicitamente con la legge 241 del 1990 ed è costituzionalmente garantito all'art. 97 comma 2, seppur indirettamente, ove viene sancito che debbano essere assicurati "il buon andamento e l'imparzialità dell'amministrazione". Lo stesso principio di trasparenza è ribadito nell'articolo 1 del d.lgs. 14 marzo 2013, n. 33, così come novellato dal decreto legislativo 25 maggio 2016, n. 97, per cui "la trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche".

Anche il CAD, Codice dell'Amministrazione Digitale, all'art. 2, comma 1 ed art. 50 comma 1, prevede il principio di "disponibilità dei dati pubblici" riprendendo il concetto di formato aperto, ossia dati resi pubblici dalle amministrazioni in formati tali da assicurare a tutti la fruizione, l'utilizzo e il riutilizzo consentendo la partecipazione ed il controllo dei cittadini in un'ottica di trasparenza. Con la modifica dell'articolo 52 del CAD nel 2012, difatti, "i dati e i documenti che le amministrazioni titolari pubblicano senza l'espressa adozione di una licenza si intendono rilasciati come dati di tipo aperto". L'Agenzia per l'Italia digitale (AGID) è il centro di competenza nazionale sul tema degli open data, in coerenza con le politiche di open government. Tra i suoi compiti principali vi è la gestione del catalogo nazionale dei dati di tipo aperto quale strumento di riferimento per la ricerca dei *dataset* resi disponibili dalle amministrazioni, la promozione di politiche di valorizzazione del patrimonio informativo pubblico nazionale e della cultura dei dati aperti.

In un'ottica di partecipazione volta alla verifica dell'azione amministrativa, gli open data agevolano la prevenzione e il contrasto della corruzione generando trasparenza sulle attività pubbliche, sulle decisioni e sulle spese sostenute, consentendo ai cittadini di monitorare il procurement ed il relativo uso di denaro pubblico, nonché il controllo del flusso di fondi pubblici a livello transfrontaliero. Essi sono, altresì, in grado di fornire alle aziende informazioni in tempo reale sul contesto economico di un determinato mercato o settore, consentendo alle stesse di adottare ponderate decisioni di investimento e contribuendo alla costruzione di sistemi organizzativi e contesti lavorativi più aperti, trasparenti e meno corrotti, riducendo altresì il rischio di conflitti di interesse e favoritismi.

La enorme quantità di dati amministrativi in possesso della Pubblica Amministrazione, la relativa analisi ed i dataset finalizzati a descrivere e tracciare processi e attività ritenuti a rischio di corruzione, ha richiesto in maniera crescente un orientamento ad un approccio ai big data basato sulla elaborazione, combinazione, ed analisi di grandi quantità di dati provenienti da fonti eterogenee. L'applicazione di adeguate tecniche di analisi su tali dati ha richiesto solide politiche di trasparenza riguardo le prestazioni e i servizi in termini di spesa pubblica e di scelte organizzative. Il collegamento dei dati in materia di appalti pubblici con altri dati amministrativi riguardanti le aziende private ha, difatti, fornito indicatori sulla capacità amministrativa e la qualità dell'operato della Pubblica Amministrazione. La condivisione delle informazioni aperte da parte dei diversi Stati attraverso gli open data contribuisce, poi, in maniera determinante ad identificare aree critiche e lacune in ambito anticorruzione e ad incentivare la collaborazione a livello globale. L'obiettivo è di consentire un ampio uso dei dati aperti delle amministrazioni pubbliche da parte di chiunque e in ogni luogo, senza limitazioni giuridiche o tecniche e con la necessaria osservanza dei requisiti di sicurezza e privacy. In un'ottica di accountability gli open data, nello specifico, consentono ai cittadini di monitorare il flusso e l'uso del denaro pubblico all'interno dei Paesi di appartenenza, permettendo altresì un confronto con i dati degli altri Paesi per un'analisi comparativa da parte dell'amministrazione, favorendo anche fra i privati una nuova tipologia di responsabilità sociale, che migliora la concorrenza fra le aziende e la qualità di prodotti e servizi. Le informazioni in possesso dell'amministrazione, costituite dai dati forniti dai cittadini, diventano così un bene comune. In tal modo anche i report e le statistiche prodotti dalla stessa amministrazione, devono necessariamente contenere dati aggiornati e autentici, poiché è sempre possibile un controllo da parte del cittadino.

2.2.2. Open data e vantaggi della tecnologia blockchain

Il concetto di open data, dati in formato aperto accessibili liberamente, mira a creare un sistema di condivisione basato sulla interoperabilità tra gli attori coinvolti, per la consultazione e riutilizzazione delle informazioni. La blockchain, *species* del *genus* delle *distributed ledger technologies*, si pone come tecnologia complementare agli open data, supportandoli e valorizzandone la funzione grazie a tre caratteristiche fondamentali: trasparenza, tracciabilità e tutela dei dati. La diffusione di un'architettura di rete basata su registri distribuiti, definita distributed ledger technology ha permesso la ripartizione della potenza di calcolo delle intelligenze artificiali su più nodi (miners) della rete. Grazie a tale tecnologia ogni nodo può essere aggiornato con nuove informazioni, ma sotto il controllo di tutti i membri, che possono visualizzarle e verificarle in *real time*, ma modificarle solo dopo aver ricevuto il consenso da tutte le parti interessate nell'operazione. I dati sono immessi nel sistema dal membro che ne è proprietario, perciò nel pieno rispetto della riservatezza, possono essere visualizzate dagli altri soltanto le informazioni personali sulle quali ha prestato il suo consenso, ed i dati non possono essere modificati retroattivamente. Il controllo reciproco presente in tale sistema di transazioni e l'immutabilità dei dati, generano maggior fiducia fra gli utenti coinvolti nei processi di condivisione e riutilizzo delle informazioni, assicurando la tracciabilità e tutelando il rispetto della privacy. La blockchain è basata su un registro delle transazioni distribuito che consente la tracciabilità dei flussi ed elimina il ruolo degli intermediari, aumentando ulteriormente, in tal modo, la sicurezza e la trasparenza delle operazioni. Essa nasce nel mondo delle criptovalute all'inizio del nuovo millennio ma, nonostante gli esperti del settore, unanimemente, ne esaltino le potenzialità, ha tutt'oggi applicazioni ancora limitate e la sua diffusione stenta a decollare. Punti forti della tecnologia blockchain sono, indubbiamente, la trasparenza delle transazioni e la tracciabilità di ogni attività[183]. I controlli avvengono prevalentemente dal basso, ossia dagli stessi partecipanti. Se utilizzata come piattaforma di gestione di ogni fase negli appalti, con la maggiore trasparenza si riduce notevolmente il rischio generato dal conflitto d'interessi e di conseguenza anche i fenomeni corruttivi. Ad attribuire certezza al contenuto delle interazioni compiute nel sistema è il ricorso ad un meccanismo di firma a doppia chiave asimmetrica e la strutturazione dei

[183] Cfr. Gallone G., *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Diritto dell'economia*, 3/2019, p. 187 ss.

dati in blocchi, tramite una rete di tipo peer to peer[184]. Essendo un registro distribuito e non centralizzato, la registrazione di qualsiasi operazione o scambio deve essere preventivamente approvata da tutte le parti dell'accordo, tramite smart contract[185]. La blockchain, agevolando l'interazione nelle transazioni ed automatizzando ulteriormente i processi amministrativi senza controllo e gestione di organi terzi o autorità esalta, difatti, pienamente le caratteristiche di nuovi ed innovativi strumenti, quali i c.d. smart contract, contratti intelligenti[186] che vengono compilati automaticamente dal sistema in base a determinate condizioni preimpostate dalle parti. Gli smart contract operanti in una blockchain evidenziano, pertanto, prerogative quali la pubblicità dei dati e la certezza delle obbligazioni contrattuali, l'immutabilità delle transazioni, la soppressione di parti di intermediazione[187]**.** Ove sussistessero dei conflitti di interessi, le policy stabilite dagli smart contract sarebbero in grado di impedire il completamento dell'operazione.

Un utilizzo della tecnologia blockchain da parte dell'amministrazione, si è avuto nel settore degli appalti edili di opere pubbliche, che al pari di quello sanitario risulta nel nostro Paese sovraesposto ai fenomeni corruttivi, per mezzo della piattaforma BIM (Building Information Modeling), la quale ha favorito la concorrenza e consentito un maggiore controllo e contenimento delle attività illecite e della spesa pubblica. Caratteristica fondamentale di tale sistema è la collaborazione fra le diverse figure professionali che prendono parte alla realizzazione di un'opera tramite una piattaforma integrata. Tutti i dati rilevanti devono essere disponibili in formati digitali aperti, al fine di non ledere la concorrenza. Tale visione olistica conferisce spazio paritario a tutte le figure coinvolte nel progetto. Ma ciò che più rileva è che il BIM assicura la certezza del controllo di tempi e costi ed una maggiore trasparenza, rappresentando un utile strumento di controllo del conflitto di interessi.

Lo stesso Codice dei contratti pubblici (d.lgs. 50/ 2016) all'art. 23 rubricato "Livelli della progettazione per gli appalti, per le concessioni di lavori nonché per i servizi", al comma 13

[184] Peer to peer è una rete informatica di tipo paritetico in cui i computer degli utenti connessi fungono allo stesso tempo da client e da server. Sull'argomento Wai-Sing Loo A., *Peer-to-peer computing*, Springer, 2006.
[185] Battaglini R., Giordano M.T., *Blockchain e smart contract*, Giuffré, 2019, p. 16 ss.
[186] La definizione degli smart contract quali contratti intelligenti non deve essere fuorviante. L'inquadramento dello smart contract sotto il profilo giuridico è, difatti, tuttora argomento ampiamente dibattuto. L'orientamento prevalente ritiene che non sia necessariamente un contratto giuridicamente inteso, ma lo può essere solo ove ne integri i requisiti. Piuttosto che come accordo esso va, pertanto, inquadrato come un "canale per la conclusione e gestione degli accordi", secondo quanto affermato da Cuccuru P., *Blockchain e automazione contrattuale. Riflessioni sugli smart contract*, in *La nuova Giurisprudenza Civile Commentata*, 2017 p. 107 ss.
[187] Cascavilla A., Galli G., *La blockchain: possibili utilizzi per l'efficienza delle pubbliche amministrazioni*, in *Osservatorio CPI*, Univ. Cattolica del Sacro Cuore di Milano, 5 marzo 2020.

prevede che le stazioni appaltanti dotate di personale adeguatamente formato "possono richiedere per le nuove opere nonché per interventi di recupero, riqualificazione o varianti, prioritariamente per i lavori complessi, l'uso dei metodi e strumenti elettronici specifici di cui al comma 1, lettera h). Tali strumenti utilizzano piattaforme interoperabili a mezzo di formati aperti non proprietari, al fine di non limitare la concorrenza tra i fornitori di tecnologie e il coinvolgimento di specifiche progettualità tra i progettisti". Pertanto il legislatore consente la possibilità alle stazioni appaltanti di richiedere all'appaltatore l'utilizzo di piattaforme integrate progettate con tecnologie blockchain. Per il codice, il Ministero delle infrastrutture e dei trasporti dovrà emanare un decreto che definisca "le modalità e i tempi di progressiva introduzione dell'obbligatorietà dei suddetti metodi presso le stazioni appaltanti, le amministrazioni concedenti e gli operatori economici, valutata in relazione alla tipologia delle opere da affidare e della strategia di digitalizzazione delle amministrazioni pubbliche e del settore delle costruzioni"[188]. La conseguente bozza di decreto ha previsto la subordinazione dell'utilizzo del BIM all'adozione "di un atto organizzativo che espliciti il processo di controllo e di gestione, il gestore del dato e la gestione dei conflitti".

Alla luce di quanto sin qui esposto, vi sono innumerevoli elementi da considerare per valutare il collegamento fra la tecnologia BIM e la prevenzione del fenomeno corruttivo nel mondo degli appalti pubblici. In primo luogo si può affrontare la questione della trasparenza che, rispetto al fenomeno corruttivo, realizza "una misura di prevenzione poiché consente il controllo da parte degli utenti dello svolgimento dell'attività amministrativa"[189]. È evidente l'impatto che l'utilizzo del BIM ha sulla trasparenza degli appalti: avere un'unica fonte d'informazioni circa un'aggiudicazione ed il relativo progetto, con i relativi dati consultabili online da tutte le parti coinvolte, consente un ampio controllo sull'opera e sulle sue caratteristiche. Ciò che assume maggiore rilevanza ai fini dell'efficacia ed efficienza dei progetti gestiti tramite il BIM è la capacità, tramite database, di condividere le caratteristiche degli oggetti informatici rappresentati nel modello e le indicazioni normative, consentendo agevoli controlli automatici dei requisiti di progetto e, quindi, una verifica più ampia e completa. Ciò al fine di tenere sotto controllo gli

[188] Art. 23 comma 13 del d.lgs. 50/ 2016.
[189] Circolare n. 1/2013 del Dipartimento della Funzione Pubblica.

sprechi, i costi, i tempi di realizzazione e le eventuali varianti in corso d'opera[190] riducendo, altresì, al minimo la possibilità di aggiudicarsi una gara attraverso ribassi d'asta.

La progressiva obbligatorietà del BIM negli appalti edili di opere pubbliche ha già sortito effetti benefici indiscussi per quanto riguarda conflitto di interessi e illegalità. L'estensione dell'utilizzo di piattaforme integrate con tecnologia blockchain può migliorare l'efficienza e trasparenza della pubblica amministrazione in tutte le tipologie di appalto, con particolare riferimento al procurement sanitario, settore, al pari di quello delle opere pubbliche, ad alto tasso di corruzione. Di questo parere è il rapporto pubblicato dal World Economic Forum "Exploring Blockchain Technology for Government Transparency. Blockchain-Based Public Procurement to Reduce Corruption", uno studio completo sull'utilizzo della tecnologia blockchain per controllare il corretto svolgimento degli appalti pubblici e ridurre le pratiche illecite[191]. La tecnologia blockchain consente difatti, secondo il rapporto, di conservare registri permanenti delle gare ad evidenza pubblica permettendo di individuare in pochissimo tempo eventuali alterazioni. Il che garantisce la massima trasparenza e verificabilità dei processi in tempo reale. La catena dei blocchi rende più difficile rimuovere le registrazioni delle offerte o modificarle dopo che siano state presentate. Il sistema decentra, poi, il processo decisionale, la supervisione e la tenuta dei registri ridimensionando il potere e l'intervento di autorità che potrebbero essere inclini alla corruzione. Secondo l'Osservatorio europeo sulla blockchain, organo creato dalla Commissione Europea, l'applicazione di tale tecnologia è utile per risolvere problemi cruciali nei rapporti con le Pubbliche Amministrazioni come la fiducia, la trasparenza e la sicurezza. Sempre a livello di Unione europea, le potenzialità in chiave preventiva della blockchain sono state riconosciute attraverso l'adozione della Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle "tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione", Considerando F, ove si legge che essa "può definire un quadro di trasparenza, ridurre la corruzione, rilevare l'evasione fiscale, consentire la tracciabilità dei pagamenti illeciti, agevolare le politiche antiriciclaggio e individuare l'appropriazione indebita di beni". Anche il Ministero dello Sviluppo Economico[192], considera quale principale caratteristica offerta dalla tecnologia blockchain, la riduzione del costo

[190] L'ANAC ha pubblicato il risultato di un'analisi che ha evidenziato un enorme spreco di risorse pubbliche rappresentato dalle varianti in corso d'opera e una grande opacità che favorisce i comportamenti corruttivi.
[191] Lo studio, pubblicato nel giugno 2020 dal World Economic Forum, sostiene la tesi che la tecnologia blockchain sia uno strumento di amministrazione condivisa avente il potenziale per ridurre fortemente le condotte corruttive.
[192] MISE, "Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain. Sintesi per la consultazione pubblica".

della fiducia necessaria al perfezionamento di una transazione, intesa come scambio informativo o di valore, garantendo al tempo stesso la certezza della sua esecuzione.

Per ciò che riguarda il difficile rapporto pubblicità/tutela dei dati, il problema è agevolmente risolvibile grazie alla possibilità di criptare alcuni di essi lasciandone in chiaro altri. Un ultimo, ma non meno importante, vantaggio della blockchain è relativo alla sicurezza: essendo una rete decentrata e distribuita, nessun attacco informatico può impadronirsi di un nodo centrale e far crollare l'intero network[193]. L'esistenza di più nodi preserva, così, il sistema, rendendolo in gran parte immune dai danni compiuti da hacker e soggetti non autorizzati.

2.2.3. Big data e predictive policing nella prevenzione e repressione degli illeciti

I big data analytics sono raccolte di enormi masse di dati eterogenei in quanto provenienti da diverse fonti, da elaborare con tecnologie di analisi massive, allo scopo di ricercare informazioni ed individuare i legami tra fenomeni diversi. L'acquisizione di dati informativi è talmente estesa da richiedere l'utilizzo di moderne tecnologie in grado di estrarne automaticamente il valore, analizzarli, confrontarli e gestirli. I big data sono, pertanto, strettamente legati all'intelligenza artificiale, poiché solo algoritmi estremamente avanzati e sofisticati sono in grado di processare e confrontare automaticamente ed in tempi rapidi quantità di dati così elevate. Le alte potenzialità dei big data hanno fatto sì che il loro utilizzo, originariamente legato alla profilazione degli utenti Internet per fini commerciali, sia stato recentemente ampliato a molti altri campi, anche di interesse pubblico. L'A.I. (intelligenza artificiale) e la disponibilità di un'enorme mole di dati da parte della Pubblica Amministrazione può, difatti, fornire un importante contributo alle operazioni di prevenzione dei crimini, ed in particolare all'identificazione di potenziali rischi corruttivi. I predetti dati sono provenienti da diverse fonti sia interne che esterne alla Pubblica Amministrazione, fra cui informazioni in possesso delle forze dell'ordine e degli enti pubblici, notiziari online, social network, ma anche sistemi a circuito chiuso e di sorveglianza. In un'ottica preventiva di intercettazione delle dinamiche corruttive e situazioni di conflitto di interessi, il legame fra i big data e l'intelligenza artificiale rappresenta un reale ed efficace metodo di contrasto. In particolare, l'applicazione di adeguate e specifiche tecniche di analisi su quantità

[193] Esiste, tuttavia, un rischio conosciuto come "51% attack", che si potrebbe verificare nel caso in cui un hacker prendesse il controllo della maggioranza dei nodi della catena, ma si tratta di un'ipotesi remota. Non vi sarebbe, inoltre, alcuna possibilità di modificare le informazioni precedentemente registrate, considerato che queste sono comunque criptate e accessibili solo tramite le chiavi private dei proprietari.

immense di dati può fornire una serie di opportunità per la definizione di più solide politiche anticorruzione e per la valutazione di prestazioni e servizi in termini di spesa pubblica e di comportamenti organizzativi. A puro titolo di esempio, il collegamento dei dati in materia di appalti e contratti pubblici con i dati amministrativi riguardanti le aziende private operanti sul territorio può fornire indicatori quantitativi e qualitativi per descrivere la trasparenza operativa, la capacità amministrativa e la qualità dell'operato di P.A. e imprese, a molteplici, ed estesi livelli di analisi.

In Italia, ormai da un decennio viene utilizzato da Guardia di Finanza ed Agenzia delle entrate, un software denominato Serpico, che si avvale di tecnologia basata su modelli di algoritmi avanzati, intelligenza artificiale e big data analytics per individuare, tramite il confronto dei dati dichiarati al fisco con il patrimonio posseduto e lo stile di vita dei contribuenti, eventuali evasioni fiscali, lavoro nero ed in generale reati finanziari. Il sistema analizza un'enorme mole di dati di tutti i residenti in Italia, connettendosi alle principali banche dati, fra cui motorizzazione, demanio, catasto, Inps, Inail, Dogane, registri, ecc., ma soprattutto accedendo ai dati bancari per controllare ogni movimentazione. Ciò permette di confrontare, in tempo reale, il reddito dichiarato di ogni residente, con il potere di spesa, ottenendo così informazioni importanti per l'individuazione dell'evasione fiscale, di attività di riciclaggio o altri illeciti di tipo finanziario, ovvero di semplici anomalie che necessitano di ulteriori controlli. Il punto forte di Serpico è insito nelle potenzialità dei big data analytics, ossia l'interoperabilità di enormi dataset e la velocità di calcolo delle operazioni di confronto dei dati di milioni di persone, al fine di individuare ogni irregolarità o caso sospetto riguardante le capacità di spesa di imprese e privati nei confronti dei redditi dichiarati dagli stessi.

L'utilizzo dei big data in materia di repressione e soprattutto di prevenzione del crimine non può non estendersi alle recenti tecniche di predictive policing (polizia predittiva). Tali tecniche si concretizzano nell'utilizzo specifico di algoritmi con grandi masse di dati (appunto i big data analytics), allo scopo di prevedere, con un'analisi predittiva basata sul calcolo probabilistico, il compimento di reati e la localizzazione di aree a maggior rischio[194]. Una previsione sufficientemente accurata diviene possibile grazie ad un modello di trend ricavato dai dati storici

[194] Con riguardo alla localizzazione dei reati, definita "crime hotspot" si veda: A. Babuta, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*, in *Royal United Services Institute for Defence and Security Studies*, 2017, p. 35 e ss.

su basi statistiche. Partendo dall'analisi predittiva è, poi, possibile intervenire mediante un'analisi prescrittiva, cercando di riprodurre le condizioni affinché si verifichino determinati eventi e non altri. Le tecniche di polizia predittiva, nate per il contrasto alla microcriminalità nelle aree urbane a maggior rischio, si sono rapidamente estese, con risultati positivi, anche al contrasto e prevenzione di altre tipologie di illeciti, risultando particolarmente valide nell'individuazione del conflitto di interessi e nella lotta ai fenomeni corruttivi. L'analisi di grandi quantità di dati processati con algoritmi avanzati e l'utilizzo della tecnica di *hot spot analysis*, propria delle attività di polizia predittiva, consente con estrema precisione l'individuazione di aree ed amministrazioni, ma anche di comportamenti e situazioni tipo ove il conflitto di interessi sia già in atto o presunto, ovvero vi sia un notevole rischio di fenomeni corruttivi e illegalità. L'aggregazione dei dati permette, difatti, di sfruttare le caratteristiche di crimini già avvenuti, per facilitare l'attività di indagine o addirittura prevenire crimini futuri, non limitandosi ad individuare aree o condizioni tipo ad alto rischio, la cosiddetta predictive criminal mapping, ossia la mappatura dei rischi di reato, ma facendo luce anche sulle probabili modalità e sul profiling dei soggetti che possono essere gli autori di tali reati.

Ci si chiede, tuttavia, se tali tecniche all'avanguardia siano compatibili con il diritto alla privacy e la protezione dei dati personali. Il pericolo di ingerenze con riguardo alla tutela dei dati personali, derivante dall'immagazzinamento massivo ed analisi di grandi quantità di dati necessari per la profilazione della predictive policing, è un problema concreto richiedente particolare attenzione. Fra gli altri effetti negativi di tale tecnica vi è, poi, il rischio di discriminazione e stigmatizzazione di classi sociali, etnie, quartieri cittadini ed intere aree geografiche[195]. Ciò è spesso frutto di c.d. falsi positivi dovuti all'inaccuratezza, incompletezza e parzialità dei dati processati, ma soprattutto della limitatezza e rigidità degli algoritmi[196]. Le stesse policy per la selezione delle

[195] Giribaldi D., *Discriminazione algoritmica. Intelligenza artificiale, tutti i pregiudizi (bias) che la rendono pericolosa*, in *Agenda Digitale*, 26 febbraio 2019, e Crawford K., *The Hidden Biases in Big Data. Harvard Business Review*, disponibile in: https://hbr.org/2013/04/the-hidden-biases-in-big-data, 01 aprile 2013.

[196] Anche per il Parlamento Europeo (*European Parliament, Report on fundamental rights implications of big data: privacy, data protection, non discrimination, security and law-enforcement, 2016/2225(INI), Committee on Civil Liberties, Justice and Home Affairs*, 20 febbraio 2017), non è trascurabile tale rischio, con l'effetto che «low-quality data and/or low-quality procedures behind decision-making processes and analytical tools could result in biased algorithms, spurious correlations, errors, an underestimation of the legal, social and ethical implications".

informazioni da utilizzare e di quelle da scartare per un'indagine predittiva sono, difatti, frutto di una scelta umana, soggetta pertanto ad errori di valutazione e condizionamenti ideologici[197].

2.3. L'utilizzo dei big data analytics

2.3.1. Big data e intelligenza artificiale

Un determinante supporto all'attività volta all'emersione di fenomeni corruttivi e conflitto di interessi perviene, indubitabilmente, dall'utilizzo delle più moderne tecnologie informatiche e telematiche e, nello specifico, dell'intelligenza artificiale applicata, grazie ad algoritmi complessi, a grandi quantità di dati. A tal proposito si può affermare che negli ultimi anni hanno assunto sempre maggior rilevanza i big data analytics, consistenti in un'enorme mole di dati eterogenei scambiati fra strumenti informatici collegati in rete[198], incrociati e confrontati grazie alle capacità di calcolo dei moderni elaboratori. La peculiarità dei big data consiste nel trattamento automatizzato dei dati al fine di estrapolare, tramite un algoritmo che li processa, analizza e relaziona, informazioni coerenti e correlate fra loro. Ciò che distingue i big data da un semplice insieme di dati è la necessità, per essere processati in tempi tollerabili, di strumenti di elaborazione automatici differenti da quelli tradizionali[199], quali l'intelligenza artificiale, le reti neurali ed il *machine learning*. Valida e completa è la definizione di big data che ci fornisce il Parlamento europeo. Secondo l'organo istituzionale dell'UE i big data indicano la collezione e l'analisi di grandi quantità di dati, inclusi quelli personali, provenienti da una varietà di sorgenti, soggetti a processi automatici per mezzo di algoritmi, il cui incrocio è in grado di generare correlazioni, tendenze e modelli[200]. Punto cruciale è l'estrazione ed organizzazione di dati

[197] In tal senso, Massaro A., Sorbello P., Giraldi A., Grossi L., Notaro L., *Intelligenza artificiale e giustizia penale*, dicembre 2020, p. 85, secondo cui "la quantità di informazioni e di dati raccolti non è altro che il frutto di una rielaborazione dell'essere umano, che, in quanto tale, ingloba vari fattori di parzialità. A livello strutturale, questa circostanza rappresenta un limite effettivo al funzionamento degli algoritmi: questi ultimi, infatti, producono risultati efficaci unicamente in quanto l'input fornito sia di qualità e corrisponda alla realtà fattuale".

[198] Gli scambi di dati tramite Internet hanno avuto negli ultimi anni un incremento impressionante: secondo il Rapporto tecnico dell'International Data Corporation (IDC) del 2017 si è registrato un aumento esponenziale di oltre dieci volte rispetto ai sei anni precedenti, con una stima di 44 milioni di messaggi al minuto e 2,3 milioni di ricerche al minuto soltanto sul motore di ricerca Google.

[199] Il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, *L'intelligenza artificiale al servizio del cittadino*, p. 52, evidenzia che i dati hanno bisogno di "modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise".

[200] Secondo l'European Parliament, *Report on fundamental rights implications of big data*, par. A) "big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics)".

eterogenei in tempi ridotti, allo scopo di acquisire informazioni affidabili e fruibili. Organizzazioni, imprese ed enti pubblici tendono, difatti, a raccogliere qualunque tipo di dato dalla rete, elaborandolo per migliorare i propri processi decisionali e memorizzandolo permanentemente al fine di poterlo proficuamente riutilizzare. A tal fine è necessario un sistema tecnologico potente e flessibile, che in brevissimo tempo possa automaticamente filtrare i dati utili, fornendo risultati organizzati e strutturati[201].

Oltre all'utilizzo originario dell'elaborazione algoritmica di masse di dati nel campo della profilazione di utenti a fini pubblicitari[202], un importante uso recente dei big data è quello in campo scientifico, ed in particolare sanitario, poiché grazie alle banche dati contenenti informazioni genomiche e cliniche di pazienti in forma anonima, si possono acquisire nuove conoscenze su una determinata patologia[203]. In ambito pubblico tali dati possono essere utilizzati per realizzare indicatori economici accurati, stimare le statistiche riguardanti la disoccupazione e rilevarne le cause in ogni singolo settore ed area geografica per poter stabilire un piano strategico basato su dati affidabili, e gestire la sanità a livello nazionale sia sul piano manageriale che su quello ospedaliero riguardante i pazienti[204]. Negli ultimi anni se ne è prospettato, altresì, un massiccio impiego nella ricerca di aree e situazioni sensibili al conflitto di interessi. La tecnologia

[201] Lugmayr A., Stockleben B., Scheib C., Mailaparampil M. (2017), *Cognitive big data: survey and review on big data research and its implications. What is really "new" in big data?*, in *Journal of Knowledge Management*, 21(1), pp. 197-212.

[202] Nel rapporto interlocutorio *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, realizzato da AGCOM nel giugno 2018 finalità in termini generali dei big data è di "accrescere l'efficienza dei processi produttivi, migliorare la capacità decisionale degli amministratori, prevedere più accuratamente le tendenze di mercato e indirizzare in modo molto più mirato (e dunque variamente efficiente) la pubblicità o le diverse proposte commerciali". Nonostante l'espansione in vari settori l'utilizzo più ampio dei big data riguarda ancora la personalizzazione dei prodotti e dei servizi offerti nell'ambito della pubblicità in rete e del commercio elettronico. Ne sono un chiaro esempio le piattaforme che distribuiscono contenuti di e-commerce, le quali propongono ai propri utenti beni e servizi in linea con le preferenze individuali relative alle abitudini del consumatore, utilizzando le c.d. tecniche di search discrimination, ossia di personalizzazione della visualizzazione dei risultati di ricerche on-line. Nell'ambito dell'offerta televisiva Netflix ha ideato e prodotto la serie TV House of Cards, traendone i contenuti dall'analisi del comportamento dei fruitori della propria piattaforma.

[203] Lo studio delle forme della recente emergenza epidemiologica da Covid-19, ha fatto largo uso dei big data. Sul piano economico un recente studio pubblicato dalla Society of Actuaries calcola che il 60% delle aziende sanitarie stia utilizzando l'analisi predittiva all'interno delle rispettive strutture. Anche l'elaborazione di strategie, previsioni e analisi per contribuire a limitare i contagi, passa attraverso l'analisi di grandi quantità di dati. Il maggior contributo dei big data nella battaglia al contagio si è, senza dubbio, registrato nelle fasi di controllo e tracciamento degli spostamenti ed in termini di ricerca di nuovi medicinali e vaccini. In Italia sono utilizzati prevalentemente in chiave di prevenzione, diagnosi e cura. In particolare, una ricerca svolta dall'Istituto ortopedico Rizzoli di Bologna e dall'Alma Mater Studiorum ha trovato una correlazione tra le ricerche sul web sui sintomi più comuni della malattia e la localizzazione dei contagi, rappresentando un efficace strumento di previsione di nuove ondate epidemiche, ai fini di adottare rapide misure di risposta per ogni area a rischio.

[204] Tuttavia l'investimento di Pubblica Amministrazione e sanità nei big data corrisponde soltanto al 6 percento del totale.

è, difatti, ormai ampiamente collaudata anche per quanto attiene alla prevenzione dei fenomeni corruttivi, poiché già da tempo governi, organizzazioni internazionali e società civile sono impegnati nella diffusione e nel perfezionamento di strumenti e metodologie di acquisizione, tracciamento e analisi di informazioni e dati, con il fine principale dell'emersione del conflitto di interessi.

La gestione di quantità di dati così elevate richiede un trattamento automatizzato e rapido capace di esaminare e rielaborare i risultati per fornire analisi concrete, riutilizzabili ed utili per creare modelli su cui basare orientamenti e scelte. Ciò può avvenire solo grazie all'intelligenza artificiale, che permette di individuare dai big data dei trend utili e comparare variabili apparentemente eterogenee trasformandole in dati organici, da cui trarre informazioni e modelli adatti all'elaborazione di orientamenti strategici[205]. L'intelligenza artificiale studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi hardware e software atti a fornire all'elaboratore prestazioni di estrema velocità e compiti di pertinenza dell'intelligenza umana, riprodurne o emularne alcune funzioni, risolvere problemi mediante processi inferenziali. Essa rappresenta un insieme di tecnologie capaci di apprendere, piuttosto che affidarsi meramente alle istruzioni impartite dagli sviluppatori e di fare previsioni al di là della ordinaria capacità umana. Un sistema di intelligenza artificiale ha, difatti, la capacità di processare il contenuto di interi codici giuridici, complessi legislativi e normative, nonché dei casi giudiziari e le peculiarità di ogni attività umana ed imparare a riconoscere i modelli anticorruzione conformi alle disposizioni, considerando anche che alcuni Paesi hanno vagliato la possibilità di un automatico aggiornamento di norme ed eventuali revisioni di leggi e regolamenti, senza alcun intervento umano.

Con riguardo ai big data la prima considerazione riguarda la distinzione delle informazioni in essi contenute, le quali possono avere natura personale e non personale. Meno problematico è il trattamento di dati non personali per i quali trova applicazione il Regolamento (UE) 2018/1807 del novembre 2018 relativo ad un quadro attuabile alla libera circolazione, mentre quelli personali sono soggetti a particolari restrizioni, a cui concorrono il Regolamento Generale sulla Protezione

[205] Secondo la Risoluzione del Parlamento Europeo 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)) "la natura massiva delle operazioni di trattamento reca con sé la necessità che tali insiemi di informazioni (sia memorizzate, sia in streaming) siano oggetto di trattamento automatizzato, mediante algoritmi e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e/o modelli".

dei Dati (GDPR), regole specifiche sulla privacy, ed infine le direttive 2002/58/CE e 2009/136/CE, relative al trattamento dei dati personali e alla tutela della vita privata. È, pertanto, necessario che chi effettua operazioni con i big data distingua, in via preliminare, la natura personale o meno dei dati trattati, al fine di identificare la cornice normativa di riferimento all'interno della quale si trova ad operare. Ovviamente tale operazione viene automatizzata tramite gli algoritmi che filtrano i dati e automaticamente li adattano alla cornice normativa di riferimento. È, comunque, necessaria un'informazione a monte, in particolare agli utenti di Internet, circa il grado di pervasività dei sistemi di acquisizione (quali accesso a rubriche, videocamere, geolocalizzazioni, ecc.) che accumulano dati sulle loro attività on-line.

Per una migliore comprensione del processo di estrazione delle informazioni dai big data, bisogna distinguere tre fasi: quella di raccolta e memorizzazione delle informazioni, la fase di elaborazione ed analisi, ed infine quella di interpretazione ed utilizzo [206]. Con riguardo alla prima fase, quella di raccolta, è necessario porre l'accento sulla enorme quantità di dati eterogenei resi disponibili su Internet in considerazione delle innumerevoli attività compiute on-line dagli utenti (messaggi di posta elettronica, contenuti dei social network, ricerche sui motori di ricerca, acquisti on-line, utilizzo della home banking, contenuti multimediali in rete, ecc.). A questi si aggiungono i dati generati dagli utenti degli smartphone (geolocalizzatori, sensori di movimento), i cookie, che consentono di raccogliere le preferenze degli utenti della rete, e gli open data, accessibili a tutti e prodotti generalmente dagli organismi pubblici. I dati raccolti vengono poi memorizzati, ossia trasferiti nella memoria di un sistema di elaborazione: in tale operazione assume rilevanza la sicurezza e l'integrità del dato. I dati memorizzati, se considerati isolatamente, hanno poca utilità, mentre ne acquisiscono quando sono organizzati e strutturati. Per suddetta ragione assume particolare rilevanza la fase di elaborazione, che tramite l'analisi comporta l'organizzazione rapida di dati grezzi non strutturati, trasformandoli in informazioni ordinate, facilmente reperibili ed interpretabili, ed immediatamente utilizzabili per l'uso cui sono destinate. Tale analisi viene effettuata grazie ad algoritmi avanzati di interrogazione (query) atti a rispondere alle richieste dell'operatore. Ad essi si aggiungono gli algoritmi di apprendimento che hanno il compito di incrociare automaticamente i dati per estrarre specifiche informazioni, nuove conoscenze ed esplorare nuovi scenari, ed il cui funzionamento evolve in base all'esperienza acquisita riuscendo, così, ad ottimizzare i modelli computati sull'elaborazione dei dati analizzati rendendoli sempre

[206] Cfr. AGCOM, *Big data - Interim report*. *Indagine conoscitiva di cui alla delibera n. 217/17/CONS*, giugno 2018.

più accurati. Con riguardo all'ultima fase, quella di interpretazione ed utilizzo di grandi quantità di dati, non si può non rilevare che gli algoritmi di intelligenza artificiale siano in grado di individuare complessi schemi di relazioni, impossibili da analizzare anche da parte di un nutrito team di esperti. Il risparmio in termini di capitale lavorativo umano può essere, poi, impiegato per il monitoraggio, che permette di fornire feedback per il perfezionamento delle successive analisi dati.

L'utilità dei big data non è connessa alla quantità di dati che essi contengono nei dataset, ma alla loro qualità e soprattutto alla capacità degli algoritmi di processarli per estrarne dati organizzati, ossia informazioni utili per scopi commerciali, politici, sociali o istituzionali. Ciò in quanto le informazioni contenute nei dataset sono in gran parte costituite da dati secondari, non raccolti specificatamente per un determinato motivo. Con la c.d. profilazione, raccolta ed elaborazione dei dati inerenti a determinati soggetti al fine di segmentarli in gruppi a seconda del comportamento rilevato, possono essere estratti dei *trend*, ossia informazioni in grado di orientare delle scelte, ovvero creare scenari da cui poter gestire i rischi derivanti da una determinata situazione concreta. È questo lo scopo della funzione predittiva della profilazione, volta ad anticipare bisogni pubblici o privati, e permettere di orientare determinate scelte in funzione delle necessità. Altro punto delicato dei big data è la loro conservazione nel medio termine. Difatti, per essere riutilizzate, le informazioni devono essere corredate di un contesto di riferimento, ossia dei metadati. L'archiviazione digitale deve, pertanto, portare con sé lo storico dei metadati creati nell'estrazione e classificazione, per mantenere intatte le conoscenze acquisite.

La continua raccolta ed analisi dei big data da parte di aziende, enti pubblici e sistemi governativi, pone oggi complessi problemi etici, morali e di privacy. Il "dato" non riporta più difatti, come nel passato, una mera relazione, ma può sollevare notevoli criticità per la società civile, poiché diventa il supporto per erigere modelli predittivi su cui si fonda l'evoluzione del sistema stesso. Alla base dei big data vi è la condivisione di un'enorme quantità di informazioni provenienti da diversi campi della conoscenza umana. Le correlazioni che ne derivano ci permettono di trasformare i dati in informazioni e in conoscenza, attraverso l'applicazione di modelli, fornendo altresì gli strumenti per predizioni in diverse aree. L'automatizzazione delle analisi effettuate dagli algoritmi sembrerebbe rendere superflua ogni attività umana. Così non è, poiché proprio dinanzi ad una quantità così elevata di dati eterogenei emerge la necessità di una capacità di sintesi,

interpretazione degli stessi, osservazione della realtà per poterli convenientemente utilizzare cercando, nel contempo, di ridurre l'impatto delle problematiche etiche che possano sorgere e di preordinare una tutela dei diritti fondamentali e della privacy di ogni individuo. Con l'avvento e la diffusione capillare dei big data non deve essere, perciò, svilita l'attività umana, ma devono essere formate e valorizzate nuove figure professionali con ampie competenze trasversali e conoscenze interdisciplinari, giuridiche, etiche, informatiche e manageriali, capaci di ristabilire un equilibrio fra lo strapotere dei dati e i bisogni della persona[207].

2.3.2. Complessità computazionale, data mininig e machine learning

Le complesse tecnologie di cui si avvalgono i big data analytics richiedono notevoli risorse hardware e software, irraggiungibili per qualsiasi azienda od organizzazione fino a pochi anni or sono. Nell'analisi di grandi quantità di dati sorge un problema di complessità computazionale, ossia di risorse minime necessarie, in termini di tempi e di memoria, per compiere una determinata operazione in funzione di uno specifico input[208]. Essa rappresenta un limite in considerazione del rapporto fra tempi di risposta dell'algoritmo e quantità di dati analizzati, ed è pertanto un punto di riferimento nella progettazione di sistemi di analisi dati. Lo sviluppatore, nel creare un sistema di analisi, dovrà tener conto dell'impegno di risorse, ma anche dell'elaborazione di un sufficiente numero di informazioni per rappresentare risultati affidabili. Ciò necessita di architetture computazionali adeguate, basate sull'intelligenza artificiale, che si avvalgano di tecnologie quali il *data mining* ed il *machine learning*.

Il data mining rappresenta l'estrazione di grandi quantità di informazioni implicite e potenzialmente utili, nonché la loro esplorazione ed analisi, per mezzo di sistemi automatizzati, al fine di scoprire *pattern* significativi, ossia analisi delle associazioni, anomalie e schemi ricorrenti. Consiste, quindi, nel processo computazionale di analisi di grandi *dataset*, e si avvale dell'utilizzo di metodi di machine learning, intelligenza artificiale, reti neurali, clustering, alberi decisionali, statistica e basi di dati, coprendo anche aspetti di gestione del dato e *pre-processing*, modellazione, estrazione e visualizzazione. Il processo di data mining, chiamato KDD (Knowledge

[207] Fra le nuove figure professionali vi è quella del data scientist con competenze interdisciplinari, che provvede all'individuazione delle criticità e miglioramento degli algoritmi attraverso un lavoro di team per eliminare errori, bias e discriminazioni.

[208] Sull'argomento, Ferragina P., Luccio F., *Il pensiero computazionale. Dagli algoritmi al coding*, Il Mulino, 2017; De Mauro A., *Big Data Analytics. Analizzare e interpretare dati con il machine learning*, Apogeo, 2019; Bernasconi A., Codenotti B., Resta G., *Metodi matematici in complessità computazionale*, Springer, 1999.

Discovery in Databases) è composto da varie fasi, fra cui la classificazione dei dati, la clusterizzazione, ossia l'identificazione di gruppi omogenei, l'individuazione di *time series*, ossia serie storiche utili a scopo predittivo, *sequence discovery*, ossia la scoperta di sequenze ricorrenti. Particolarmente indicato negli utilizzi predittivi del data mining è il *naive bayes*, un particolare classificatore di tipo probabilistico che ha la peculiarità di fornire risultati accurati anche in presenza di informazioni incomplete[209].

Il machine learning rientra nell'ambito delle tecnologie di intelligenza artificiale e si occupa di creare sistemi che hanno l'abilità di apprendere in maniera autonoma identificando modelli senza istruzioni esplicite e dirette, migliorando le performance e prendendo decisioni con un intervento umano ridotto al minimo, in base all'elaborazione dei dati che vengono processati. Grazie alla continua raccolta di dati i risultati diventano sempre più precisi ed affidabili, analogamente alle modalità con cui gli esseri umani migliorano grazie all'esperienza. Gli algoritmi di machine learning utilizzano metodi matematico-computazionali per apprendere informazioni direttamente dai dati senza modelli matematici, migliorando le loro prestazioni in modo adattivo man mano che gli esempi da cui apprendere aumentano. Sorge, tuttavia, il rischio che il machine learning arrivi a dilatare errori di valutazione e pregiudizi nell'eventualità di istruzioni, dettate in fase di sviluppo dell'algoritmo, che possano così distorcere la realtà.

Le tecnologie appena descritte sono indispensabili per l'impiego e l'analisi dei big data, ed in forte espansione, per cui se ne prevede nel prossimo futuro un utilizzo sempre più ampio non solo nelle aziende private ma in particolare nel settore pubblico, consentendo di produrre modelli sempre più precisi in tema di riduzione dei rischi e di analisi predittive che permettano di anticipare con probabilità sempre più ampie, comportamenti di soggetti e gruppi sociali. Ciò consentirebbe un considerevole risparmio di denaro pubblico, non solo per la razionalizzazione di costi e tempi, ma soprattutto per l'abbattimento dei costi rappresentati dal malaffare e dalla corruzione.

2.3.3. Acquisizione ed analisi dati e algoritmi di interrogazione

Con l'approccio classico anche una semplice interrogazione SQL (*structure query language*) con operazioni di *join*, selezione e filtraggio dati, se effettuata su un numero elevato di tabelle, potrebbe richiedere tempi eccessivi o addirittura mandare in *crash* il sistema. L'acquisizione,

[209] Scarpa B., Azzalini A., *Analisi dei dati e data mining*, Springer Editore, 2008; Russell M.A., *Data mining nel social web*, Editore Tecniche Nuove, 2011, 172 ss.

memorizzazione ed elaborazione di enormi moli di dati non può, pertanto, essere gestita con le tecnologie informatiche tradizionali, ma necessita dell'utilizzo dell'intelligenza artificiale, ovvero dei c.d. *smart objects*. In tal modo l'analisi può essere effettuata sul *data stream* in tempo reale, per una rapida risposta anche agli algoritmi più sofisticati ed alle *query* più complesse[210].

Oltre all'acquisizione, un momento cruciale è quello dell'analisi, che avviene tramite algoritmi di mining. Ove il flusso di input dei dati presenti elementi di interesse per l'analisi ed elementi non utili ad essa, distinguibili per caratteristiche delineate con precisione, i processi di filtraggio potranno selezionare soltanto le informazioni di interesse e scartare quelle irrilevanti, rendendo più veloci le operazioni e maggiormente accurati i risultati. Dopo una prima selezione dei dati da processare, sarà più agevole e rapida la ricerca delle correlazioni fra più variabili. Più precisi sono gli algoritmi di interrogazione che si rapportano alle banche dati, più utili saranno i dati estratti. Poiché l'estrazione dei dati avviene in maniera automatica, un importante passo avanti per avere analisi sempre più accurate, è rappresentato dalle tecniche di machine learning, ossia l'apprendimento dell'algoritmo dalle attività che lo stesso ha svolto precedentemente, al fine di migliorare le proprie performance. Le tecniche utilizzate in tale ambito sono varie, ma quelle maggiormente utilizzate sono:

a. i *clustering*, che si basano sulla similarità fra le informazioni;

b. le reti neurali, basate su elementi computazionali interconnessi in modo da variare la loro risposta agli stimoli esterni;

c. gli alberi di decisione, che forniscono diversi scenari a seconda delle possibili scelte.

Al fine di ottimizzare le performance, è necessario progettare ed implementare algoritmi di interrogazione e query più efficienti possibile, attraverso una corretta modellazione, un utilizzo attento delle risorse di sistema disponibili, e la ricerca del giusto compromesso fra complessità ed efficienza delle funzioni. Nell'implementazione delle richieste che l'utente effettua al sistema, particolare attenzione deve essere posta in fase di sviluppo al c.d. albero di esecuzione, struttura ad albero corrispondente ad un'espressione dell'algebra relazionale estesa, i cui nodi rappresentano le relazioni di input dell'interrogazione. In definitiva l'albero di esecuzione

[210] Sull'argomento Giordano A., Spezzano G., Vinci A., *Analisi e progettazione di algoritmi di data mining streaming per l'analisi online dei dati*, CNR, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR), giugno 2014, RT-ICAR-CS-14-02.

scandisce lo specifico ordine logico e sequenziale delle operazioni richieste e di quelle restituite dal sistema. Un albero di esecuzione progettato in maniera razionale e mirata, consentirà tempi di risposta più brevi e risultati maggiormente corrispondenti alle richieste. Il sistema più utilizzato si avvale, per le operazioni di join, aventi lo scopo di unire i dati richiesti a seguito di un'interrogazione, di indici e scansione sequenziale, riducendo così il numero di confronti da effettuare e di conseguenza limitando ampiamente i tempi di risposta.

2.3.4. Big data per l'emersione del conflitto di interessi

L'utilizzo sempre più esteso, nel settore pubblico, delle tecniche di big data analytics nelle attività di compliance riguardanti il conflitto di interessi, ha aperto nuovi e più ampi orizzonti nella prevenzione del rischio di fenomeni corruttivi in organizzazioni complesse, quali enti pubblici e istituzioni. Con le moderne tecnologie di analisi e l'avvento dell'intelligenza artificiale, difatti, l'accresciuta capacità di estrazione e gestione dei dati ha permesso una puntuale attività di monitoraggio per l'emersione dei conflitti di interessi, ed accurate strategie per prevenire il rischio dei reati di corruzione. In una logica di prevenzione è necessaria un'analisi e valutazione del rischio *ex an*te, che stabilisca protocolli operativi di gestione e controllo, e sanzioni nei confronti di coloro che non rispettano gli obblighi.

Tramite l'uso delle reti neurali, reti di neuroni artificiali all'interno di un sistema informatico, e degli strumenti di apprendimento automatico, ossia il c.d. machine learning, è possibile effettuare analisi sui dati a un livello talmente avanzato da poter individuare relazioni, collegamenti, anomalie e tendenze all'interno di grandi dataset. Il punto di forza dei sistemi di modellazione basati su reti neurali consiste nella loro potenza, velocità, precisione e flessibilità. Questi sistemi sono caratterizzati dalla capacità di elaborare grandi quantità di dati a diversi livelli di dettaglio, consentendo di concentrare l'attenzione e disporre di maggiori risorse per attività di approfondimento e controllo su operazioni sospette o da monitorare nel tempo. Nello specifico, nell'ambito del procurement pubblico, particolare efficacia hanno le *self-organizing maps*, fondate sul principio per cui un dato si specializza nel riconoscere uno stimolo in grado di intercettare la corruzione in ambito pubblico, basandosi sull'analisi di fattori economici e politici. A seconda dei dati statistici analizzati, è possibile stimare la probabilità di casi di corruzione emergenti prima che si verifichino, consentendo l'attuazione di misure preventive. È, perciò, possibile utilizzare i sistemi di intelligenza artificiale per identificare le vulnerabilità ed indirizzare

le azioni e i controlli in particolari aree a rischio. Gli algoritmi su set di dati complessi ed eterogenei alla ricerca di indicatori di potenziali conflitti di interessi difficili da individuare, sono stati sempre più utilizzati nel contrasto e prevenzione dei fenomeni corruttivi e contenimento della cattiva gestione della cosa pubblica.

A tal fine, particolare utilità ha l'identificazione di indicatori di anomalie (c.d. red flag) rispetto ai comportamenti ed a relazioni ordinarie, nonché la predisposizione di particolareggiati report in merito a profili anomali, fra cui si possono citare prezzi d'acquisto troppo distanti dalla media di un'area geografica, rapporti di parentela fra soggetti coinvolti nelle transazioni e terze parti, movimenti finanziari sospetti. Tutto ciò con un duplice scopo: non solo in un'ottica di contrasto ai comportamenti di rilevanza penale, ma sotto un più ampio punto di vista di identificazione di ipotesi di maladministration[211]. Ogni evento sentinella di un possibile malfunzionamento dell'attività amministrativa richiede un adeguato monitoraggio, anche per individuare le idonee misure correttive di carattere normativo, organizzativo o amministrativo.

Una corretta analisi dei dati permette il rafforzamento del sistema di *compliance* e continui adeguamenti dei protocolli di gestione del rischio, non più individuato sulla base delle tradizionali attività di indagine empirica, ma sulla base di una pervasiva analisi del patrimonio informativo, in grado di individuare profili di criticità non altrimenti identificabili. Lo sviluppo di strumenti così potenti modifica il volto dell'attuale compliance pubblica, trasferendo alla macchina molte attività di analisi ed indagine, precedentemente riservate all'uomo. Le potenzialità e le aspettative per un immediato futuro sono, al riguardo, altissime, tuttavia il trasferimento su una tecnologia informatica del ruolo di valutare il rischio ed individuare procedure per gestirlo, non è esente da controindicazioni. Mi riferisco, non solo alle problematiche riguardanti la privacy e la tutela del dato personale, ma alla vera e propria attendibilità dei dati oggetto di analisi. Ove i dati raccolti e filtrati fossero poco attendibili, di conseguenza anche gli indicatori e le analisi di prevenzione risulterebbero falsati ed irrealistici. Al fine di evitare l'utilizzo di scenari non utili al contrasto al conflitto di interessi o addirittura fuorvianti è, pertanto, necessario imporre severe policy, regolamenti e linee guida, nello sviluppo degli algoritmi utilizzati nell'Amministrazione Pubblica. Tale considerazione non può non inserirsi in una più ampia ottica di gestione efficiente dei

[211] Anche i casi di maladministration che non si trasformeranno mai in ipotesi di reato, sono comunque di grave nocumento alla società, poiché comportano uno spreco di risorse pubbliche ed inefficienze. Sul punto Vannucci A., *La sicurezza nell'integrità. Politiche anticorruzione, maladministration e tutela dei diritti*, in *SINAPPSI - Connessioni tra ricerca e politiche pubbliche*, n. 2/2020.

pubblici uffici e di buon andamento degli stessi, secondo quanto previsto ex art. 97 della Costituzione. Il rispetto di suddette regole non è, tuttavia, sempre agevole poiché richiederebbe il controllo dell'operato di soggetti esterni all'amministrazione stessa, ossia i progettisti del software di analisi dei dati.

In tale prospettiva potrebbe trovare spazio nell'immediato futuro una presa di posizione legislativa in merito all'individuazione di uno standard minimo delle tecniche di sviluppo e utilizzo dei suddetti sistemi, con particolare riguardo all'individuazione della base di dati da analizzare, della loro fonte, nonché della tipologia di analisi. Da qui la proposta in materia anticorruzione, di positivizzare le cautele da imporre all'ente pubblico, stabilendo uno standard di idoneità relativamente al modello organizzativo, in conformità con le indicazioni legislative. Tale scelta già è stata effettuata in altri ordinamenti, come quello statunitense, ove le accounting provisions del Foreign Corrupt Practices Act[212] prevedono l'implementazione di un sistema di controllo interno. Potrebbe essere, poi, utile la redazione ed il conseguente rispetto di un codice deontologico e disciplinare, nonché linee guida appositi, indirizzati a quegli sviluppatori che collaborano con l'amministrazione.

2.3.5. I big data nel procurement pubblico

Il procurement pubblico è stimato in un volume d'affari di circa il quattordici per cento del prodotto interno lordo dell'Unione europea[213]. Stante la sua importanza in termini economici in ogni Paese industrializzato, si può facilmente comprendere l'interesse dei governi all'abbattimento degli sprechi derivanti da tale settore. La centralizzazione delle procedure di acquisto insieme alle strategie di trasformazione digitale e all'utilizzo di strumenti di e-procurement, costituiscono i principali orientamenti delle politiche UE per l'innovazione[214]. La condivisione delle informazioni da parte dei soggetti pubblici è uno degli obiettivi principali del

[212] Il Foreign Corrupt Practices Act del 1977, con successive modifiche apportate nel 1988 e nel 1998, è un atto legislativo del Congresso statunitense in materia di lotta alla corruzione, recante disposizioni volte ad impedire la corruzione da parte di società americane, di pubblici ufficiali stranieri, al fine di ottenere o mantenere rapporti commerciali.

[213] Fonte: documento della Commissione Europea "Appalti pubblici efficaci in Europa e per l'Europa", Strasburgo, 3 ottobre 2017, COM(2017) 572 final.

[214] I report dei Paesi europei sugli indici DESI 2021 e sui DMI, che misurano il livello di digitalizzazione e i divari all'interno del continente, ha visto il posizionamento dell'Italia al ventesimo posto su ventisette, nel ranking dei membri dell'UE, dietro a Slovenia, Lettonia e Croazia, di poco superiore a Cipro, Slovacchia e Ungheria. Un aiuto potrà provenire dal Piano Nazionale di Ripresa e Resilienza (PNRR) che ha previsto risorse pari a 9,75 miliardi di euro per l'innovazione e gli interventi di digitalizzazione nella P.A.

processo di innovazione e digitalizzazione della Pubblica Amministrazione poiché pone in primo piano un elemento che, oggi, ha assunto un'importanza primaria in una prospettiva di efficacia ed efficienza del settore pubblico: la trasparenza. Tali determinazioni favoriscono la razionalizzazione della spesa, la collaborazione con gli stakeholder ed il controllo reciproco di soggetti pubblici e privati, innalzando conseguentemente il livello dei servizi offerti ai cittadini, la concorrenza e l'efficienza generale del sistema. Fra i fattori più incisivi al fine di una maggior trasparenza e controllo in ogni fase della procedura di affidamento spiccano, sicuramente, la creazione di una centrale unica di committenza, la condivisione e l'interoperabilità a tutti i livelli delle banche dati, la creazione di una normativa ad hoc e linee guida per il procurement pubblico digitale, la diffusione della tecnologia blockchain e l'utilizzo sempre più massiccio dei big data analytics.

Il nuovo approccio data driven è basato sui big data e incentrato sulla loro elaborazione evitando, così, quei passaggi burocratici che rappresentano il maggior limite di ogni procedimento amministrativo. La transizione che interessa oggi il procurement è volta alla creazione di regole ripensate ab origine da un punto di osservazione esclusivamente digitale, rendendo in tal modo più snelli e veloci, ma nello stesso tempo più sicuri e precisi, i controlli e le autorizzazioni. Ciò significa che non si tende più alla creazione di regole di compatibilità dei formati e delle procedure digitali nei confronti di quelle tradizionali, ma le nuove regole vengono scritte appositamente per l'e-procurement. È, anzi, la stessa digitalizzazione a stabilire le nuove regole, basate su parametri di maggiore rapidità delle operazioni, trasparenza, interoperabilità, scambio di informazioni. Le operazioni di verifica e monitoraggio sono, difatti, più semplici e rapide, poiché si avvalgono di enormi quantità di dati confrontate e processate tramite algoritmi ed intelligenza artificiale, permettendo così alle amministrazioni centrali di individuare e poter prestare maggior attenzione a comportamenti anomali nei rapporti fra le amministrazioni locali e centrali di committenza con i vari operatori economici. Ciò permette non solo di analizzare le attività di ogni singola amministrazione e la conformità con le linee strategiche generali dell'amministrazione centrale, ma soprattutto di effettuare le azioni correttive delle procedure, qualora fossero riscontrate delle devianze, ovvero la segnalazione delle situazioni di rischio di illiceità alle autorità competenti e di maladministration ove venissero riscontrate situazioni di inefficienza. Ad esempio, il confronto delle spese omologhe delle diverse Pubbliche Amministrazioni e l'analisi delle differenti condizioni di acquisto, permette di individuare le centrali di committenza virtuose nella conduzione degli acquisti, basando le nuove policy e le regole degli algoritmi sull'esperienza

acquisita da queste ultime, e di attenzionare maggiormente quelle meno virtuose e quelle ove le situazioni anomale sono più frequenti. Dalla storicizzazione dei dati di spesa delle amministrazioni più efficienti si possono, difatti, ricavare parametri minimi per tutte le altre amministrazioni, limitando in tal modo sprechi e acquisti sovradimensionati o sovrapagati.

Big data ed intelligenza artificiale permettono, poi, un controllo a 360 gradi del DGUE (documento di gara unico europeo), un formulario standard compilato e sottoscritto dall'operatore economico come autocertificazione in cui sono elencati i requisiti di partecipazione, pubblicato in relazione ad un determinato bando di gara. Il confronto operato dagli algoritmi fra i dataset consente, poi, di rilevare eventuali conflitti di interessi non dichiarati e di risolverli prima della commissione di un eventuale illecito, con l'esclusione dalla gara dell'operatore, ovvero con l'astensione da parte del pubblico dipendente. Sarebbe, a tal fine, necessario predisporre regole e conseguenze certe al verificarsi di situazioni predeterminate, evitando di lasciare una eccessiva discrezionalità al superiore gerarchico del pubblico dipendente in situazione di conflitto di interessi.

L'orientamento dell'Europa verso la realizzazione di una struttura centralizzata per le procedure di controllo, lo scambio informativo e la valutazione dei rischi, consentirà in maniera sempre più estesa l'individuazione di conflitti di interessi e correlazioni con frodi e fenomeni corruttivi, difficilmente riconoscibili con i tradizionali metodi di analisi. A tal fine, l'incrocio di informazioni dematerializzate di banche dati sugli appalti, dell'archivio delle fatture, dei dati estraibili dalle piattaforme digitali e di pagine web di organizzazioni e società che hanno ricevuto finanziamenti a seguito di un appalto, costituisce un infallibile strumento per l'individuazione ed il contrasto del conflitto di interessi.

L'obiettivo della digitalizzazione per l'UE è quello di creare un sistema di e-procurement in cui venga applicato il principio del c.d. *once only*, in cui le informazioni richieste alle imprese siano fornite una sola volta alla P.A., la quale porterà a completamento la procedura di gara basandosi sul proprio patrimonio informativo e documentale. Ciò richiede, necessariamente, un'infrastruttura basata su regole di interoperabilità dei dati e processi intimamente connessi e basati sulla correlazione e coerenza delle informazioni[215]. A tal fine è entrato in funzione il registro

[215] Cirillo A., *La sfida del procurement pubblico: stare al passo con le imprese*, in *A.D.*, procurement dell'innovazione, 18 febbraio 2019.

europeo e-Certis[216], uno strumento per facilitare lo scambio di informazione tra operatori e amministrazioni degli Stati Membri, il quale consente tramite una piattaforma on-line di identificare le certificazioni, attestazioni o altri mezzi di prova richiedibili ad un operatore economico, a fronte della verifica del possesso dei requisiti di gara. Anche tale strumento può contribuire in maniera determinante all'individuazione di eventuali anomalie o conflitti di interessi, poiché consente un continuo scambio di informazioni, anche a livello transfrontaliero. Tra gli obblighi di pubblicità e trasparenza, considerati dall'Unione europea un imprescindibile punto di partenza per un'amministrazione efficiente, è prevista la pubblicazione su Gazzetta Ufficiale europea (OJEU) di bandi ed avvisi di gara, per tramite del servizio elettronico TED (Tenders Electronic Daily)[217]. Al fine di una maggior trasparenza e controlli più stringenti, la Banca Dati Nazionale dei Contratti Pubblici (BDNCP) gestita dall'ANAC, colleziona i dati del Sistema Informativo Monitoraggio Gare (SIMOG), utilizzato dalle amministrazioni per l'ottenimento del Codice Identificativo di Gara (CIG), elemento essenziale per poter procedere alla fase di aggiudicazione. La BDNCP raccoglie le diverse informazioni che caratterizzano la storia della gara, quali i dati dell'aggiudicatario, gli importi, le date di inizio e fine contratto, utili sia ai fini di monitoraggio e di vigilanza, che di analisi e di programmazione della spesa pubblica da parte delle amministrazioni competenti.

2.4. Predictive policing

2.4.1. Tecniche di polizia predittiva

Per predictive policing o polizia predittiva si intende quell'insieme di attività che presuppongono l'utilizzo di modelli matematici atti a compiere un'analisi al fine di individuare potenziali attività criminali ovvero identificare aree geografiche o gruppi sociali nel cui ambito i soggetti sono più propensi a commettere reati. Nello specifico, essa si concretizza nell'elaborazione, da parte delle forze dell'odine e dell'autorità giudiziaria, di grandi quantità di dati associati a modelli statistici ed algoritmi, per l'identificazione di potenziali ed ipotizzabili attività delittuose. Ciò ha conferito un

[216] L'utilizzo di e-Certis è stato introdotto dalla direttiva europea 2014/24/EU ed in Italia è stato recepito dal Codice dei Contratti Pubblici, d.lgs. 50/2016 e s.m.i., citato negli articoli: 85 - Documento di gara unico europeo (DGUE); 86 - Mezzi di prova; 88 – Registro on line dei certificati (e-Certis).

[217] I bandi e gli avvisi sono pubblicati nella Gazzetta ufficiale dell'Unione europea attraverso il sito TED entro 5 giorni dal ricevimento da parte dell'Ufficio delle pubblicazioni. Gli avvisi inviati dalle istituzioni dell'UE vengono tradotti integralmente in tutte le lingue ufficiali dei Paesi membri e pubblicati entro massimo 12 giorni a norma dell'articolo 103, paragrafo 1, del regolamento finanziario.

ruolo primario all'intelligenza artificiale e alla c.d. *data driven policing*, ossia l'attività di polizia basata sulla rielaborazione di smisurate masse di dati ed in particolare l'analisi predittiva che ha il fine di valutare il rischio di connessioni illecite, difficilmente determinabile con qualsivoglia altro sistema. I software di predictive policing si avvalgono di enormi dataset da cui raccogliere le informazioni per mezzo di moderne tecniche analitiche, e sono proficuamente utilizzati nell'individuazione di presumibili situazioni di conflitti d'interesse che potrebbero sfociare in eventi corruttivi.

Le tecniche più diffuse di predictive policing permettono, attraverso sofisticati software che incrociano dati provenienti da fonti eterogenee pubbliche e private, fra cui le informazioni relative a notizie di reati precedentemente commessi ed i profili dei sospettati rintracciati nei network di relazione sociale, l'individuazione di aree territoriali a maggior rischio di attività delittuose, di ambienti lavorativi ove si compiono frequenti illeciti o probabilità di recidiva di determinati soggetti. L'utilizzo di tali strumenti, secondo recenti statistiche, ha indubbiamente determinato una riduzione dei crimini[218], ma l'analisi di un numero altissimo di informazioni può creare pregiudizi ed iniquità. Tuttavia, secondo i sostenitori delle tecniche predittive, non vi è alcun rischio per la libertà dell'individuo, poiché alcun soggetto sarà mai privato della propria libertà o incriminato soltanto in base alle analisi predittive. Queste, difatti, avranno soltanto una valenza con riguardo alla concentrazione di controlli di polizia ed indagini degli inquirenti nell'ambito di situazioni a rischio, mentre soltanto nell'ipotesi in cui venissero riscontrati effettivamente i reati, avrebbe luogo l'incriminazione ed inizio la fase processuale. In una logica a favore delle tecniche predittive, tali modelli non solo non costituiscono alcun rischio per i diritti umani ma, per converso, possono essere utilizzati come strumento di controllo per anticipare la cattiva condotta degli agenti e dei corpi di polizia in generale, proprio al fine di evitare discriminazioni ed abusi perpetrati dagli stessi nei confronti di persone di specifiche etnie o abitanti di determinati quartieri.

Per predire il momento in cui un'azione criminale può essere compiuta con elevate probabilità ci si avvale di due categorie analitiche differenti: l'analisi spazio temporale che utilizza i dati storici

[218] Il Los Angeles Police Department ha testato la nuova metodologia, riscontrando una diminuzione complessiva dei crimini del 12%. L'implementazione di un software di predictive policing a Santa Cruz in California, che elabora mappe hot spot indicanti aree ad alto rischio, ha consentito una drastica riduzione dei furti del 19%. Camden, considerata la città più pericolosa degli USA, grazie ai software di predictive policing ha visto una riduzione degli omicidi del 41% e della criminalità in generale del 26%.

dei crimini, come le c.d. *heat maps*, oppure l'elaborazione dei dati geografici associati al rischio, con la conseguente creazione di modelli predittivi geo-spaziali. I sistemi di predictive policing incrociano prevalentemente dati storici e informazioni provenienti da differenti fonti per definire trend di comportamenti criminali prevedibili, avvalendosi di analisi statistiche effettuate tramite algoritmi complessi, big data analytics e machine learning, per la creazione di heat maps, ossia mappe di calore con una rappresentazione visiva del comportamento dei soggetti analizzati divisi per area geografica o gruppo etnico. Per ciò che riguarda la classificazione dei modelli, in base al loro obiettivo viene focalizzata l'attenzione sul luogo e il momento del probabile atto criminoso, grazie alla c.d. *hot spot analysis*. La hot spot analysis è una delle categorie di tecniche maggiormente utilizzate dagli analisti nella predictive policing, poiché permette di individuare le aree a più alto rischio criminalità incrociando dati storici sui reati ed informazioni presenti nei dataset, che vengono poi visualizzati sulla mappa. La categoria della hot spot analysis si avvale dell'utilizzo della tecnica predittiva delle *grid maps*, la quale consente di suddividere, attraverso l'uso di coordinate cartesiane, le aree oggetto di analisi e misurare la quantità di reati avvenuti per ognuna di esse, individuando le zone calde presenti sulla mappa. Al fine di individuare zone sempre più precise vengono visualizzati sulla mappa dei raggruppamenti ellittici (*covering ellipses*) definiti tramite clusters che riuniscono con un'interpolazione le zone calde alle zone limitrofe ad esse. Questo approccio risulta particolarmente utile poiché segnala geograficamente i crimini previsti con maggiori probabilità[219]. La tecnica di hot spot analysis è ampiamente testata in numerosi Paesi, ed ha conseguito notevoli risultati nelle aree ad alta concentrazione di criminalità[220].

I modelli analitici basati sul *near-repeat* consentono di predire il luogo del crimine in un prossimo futuro basandosi sui big data. Essi si basano sulla teoria criminologica della multi-vittimizzazione[221], per cui coloro che hanno subito in passato dei reati hanno più probabilità di

[219] L'algoritmo maggiormente utilizzato nella categoria della hot spot analysis è il Nearest Neighbor Hierarchical Clustering (NNHC).

[220] I risultati conseguiti con l'operazione SAVVY condotta dalla polizia delle West Midlands hanno portato ad una riduzione significativa nelle aree di criminalità di livello medio e alto. Tecniche analoghe, basate su regressioni, sono state utilizzate dal dipartimento di polizia di Washington D.C. per un'analisi predittiva dei reati di rapine, con ottimi risultati.

[221] Tale teoria è basata sull'idea di omogeneità spaziale e temporale del rischio. Ad esempio alcune categorie di reati accadono con più probabilità a determinate categorie di soggetti ed in determinati luoghi ed ore del giorno. Sull'argomento si veda: Monzani M., Bertoli E., *Manuale di vittimologia. Nuovi modelli esplicativi in criminologia e vittimologia*, L.U., 2016; Curti S., *Criminologia e sociologia della devianza*, Cedam, 2020; Sette R., *Criminologia e vittimologia*, Minerva ed. Bologna, 2011.

subirne nuovamente. Allo stesso modo, i crimini possono accadere con maggiori probabilità in luoghi e condizioni temporali analoghi a quelli già avvenuti in passato, in considerazione del fatto che gli autori dei reati agiscono secondo schemi prevedibili. L'analisi spazio temporale viene, poi, effettuata in considerazione di innumerevoli variabili (c.d. modelli temporali della criminalità), fra cui l'ora e il giorno dell'avvenimento di un crimine, la stagione o le condizioni metereologiche, i fattori ambientali come l'illuminazione dell'area. La *risk terrain analysis*, il cui modello è stato sviluppato in New Jersey, utilizza un approccio statistico che caratterizza il rischio di reato di una regione in base ai suoi tratti geo-spaziali prendendo in considerazione caratteristiche di interesse quali stazioni, negozi di alcolici, bar, discoteche e locali notturni in genere. Altro strumento utilizzato per le analisi predittive è il *social network analysis* basato sulle variabili relazionali del rapporto fra soggetti, quali legami familiari, amicizie, frequentazioni, affiliazioni ad organizzazioni. Grazie al *mapping* dei rapporti interpersonali è possibile estrarre informazioni utili per prevenire crimini ed effettuare indagini più approfondite.

Uno dei più famosi software di predictive policing è il PredPol sviluppato in collaborazione tra il dipartimento di polizia di Los Angeles e l'Università della California. Esso si avvale del machine learning utilizzando per la predizione dati storici che considerano data, ora, luogo e tipologia di crimine commesso. Le predizioni vengono visualizzate tramite un'interfaccia sul modello di Google Maps che mette in evidenza gli hot spot che rappresentano le zone a più alto rischio, nelle quali viene chiesto agli agenti di pattugliare dedicandovi circa il dieci per cento del tempo del loro turno. Per individuare gli hot spot vengono utilizzati i modelli ETAS (epidemic-type aftershock sequence) che si basano su condizioni ambientali costanti nel tempo e su cambiamenti dinamici del rischio. Grazie alla previsione delle aree calde da parte del modello, ogni dodici ore vengono evidenziate le zone che necessitano di pattugliamento permettendo una migliore allocazione delle risorse di polizia. Il limite del software è costituito dalla possibilità di un'elaborazione distorta dei dati, dovuta principalmente all'utilizzo informazioni sui crimini precedenti, dai quali l'algoritmo può ricavare sempre le stesse previsioni generando un c.d. *loop*, con conseguenti predizioni errate dei medesimi hot spot e rischio di pregiudizi razziali e ghettizzazioni. Se, difatti, in una zona vengono segnalati più crimini e di conseguenza viene maggiormente pattugliata,

immancabilmente verranno individuati ancora più crimini, rendendo tale area ancora più soggetta a controllo[222].

HCR 20 è un software per il risk assessment di crimini violenti. La gestione del rischio di violenza è basata sul modello di valutazione Structured Professional Judgment (SPJ), ed ha il fine di identificare i casi in cui i soggetti rappresentano un rischio di comportamento violento e recidiva di reato, e determinare quali misure sono necessarie per proteggere la sicurezza pubblica. Il software si è dimostrato uno strumento centrale per il *decision making* nei contesti carcerari e forensi, aiutando gli esperti a definire quali azioni mettere in atto per il possibile recupero e per tutelare la sicurezza dei soggetti esposti a tale rischio, fornendo altresì informazioni utili per l'inserimento dell'individuo nel contesto detentivo, per la sua rieducazione e l'eventuale attività terapeutica, nonché per la programmazione mirata al suo reinserimento in società e la risocializzazione. La valutazione della pericolosità sociale e del rischio di recidiva criminale si basa sulla storia clinica del soggetto nel passato, condizione clinica nel presente e fattori di rischio futuro relativi alla sua condizione personale.

Particolarmente diffuso nelle attività di intelligence di tutto il mondo è lo statunitense Palantir Gotham, famoso per aver contribuito al contrasto ai cartelli del narcotraffico, ed utilizzato anche dalle forze militari nelle attività di localizzazione di terroristi internazionali. Si occupa anche di contrasto alle frodi, allo spionaggio industriale e all'immigrazione clandestina. Il software riesce ad individuare con buona approssimazione i luoghi in cui con ampia probabilità potrebbe essere commesso uno specifico crimine, grazie alla mappatura delle relazioni interpersonali tra individui, anche quelli che non sono sospettati di un crimine. Fra i maggiori successi degli ultimi anni vi è, certamente, il riconoscimento facciale dei due attentatori ceceni della maratona di Boston[223].

Il software predittivo Compas consente, avvalendosi dell'analisi di dati personali di soggetti che hanno commesso reati, un giudizio prognostico sul rischio di recidiva. L'applicativo è in grado di identificare basandosi su analisi statistiche, il rischio di recidiva sotto più aspetti: *pretrial risk*, *general recidivism*, *violent recidivism*. Accanto alla funzione predittiva il sistema elabora anche

[222] Cfr. Stroud M., *Official Police Business: Does predictive policing actually work? Crime forecasting tools are taking off, but good data is hard to find*, in *The Verge*, maggio 2016.

[223] L'attentato terroristico alla maratona annuale di Boston, compiuto da due attentatori ceceni il 15 aprile 2013 tramite due ordigni artigianali, ha cagionato la morte di tre persone, fra cui un bambino di otto anni, ed il ferimento di altre 264. Gli attentatori, Džochar e Tamerlan Carnaev, sono stati subito individuati dal software di riconoscimento facciale Palantir Gotham in dotazione all'FBI, permettendo l'uccisione di uno di essi e la cattura dell'altro.

una c.d. *need scale*, idonea a definire il profilo del soggetto e le esigenze di riabilitazione dello stesso. I dati reperiti concorrono a determinare un valore numerico di rischio di recidiva. Tuttavia la mancanza di trasparenza del procedimento attraverso cui l'algoritmo elabora tale valore è stata oggetto di critiche, soprattutto dopo il discusso caso State vs. Loomis[224].

Anche in Italia sono ormai numerose le realtà locali che fanno uso di sistemi predittivi. Uno dei primi, denominato Pelta Suite, è un software che processa grandi quantità di dati e, grazie ad un algoritmo avanzato permette la previsione di eventi dannosi per la sicurezza pubblica. Il tutto secondo una visione non riparatoria del danno ma di prevenzione dell'illecito[225] grazie all'analisi predittiva che consente di effettuare controlli non random, ma mirati per le situazioni di maggior rischio. Ciò consente un minor spreco di risorse, umane ed economiche, sia nell'eventuale fase delle indagini che del conseguente giudizio in caso di reato. Grazie alle funzioni di machine learning, poi, l'algoritmo impara dalla propria esperienza divenendo sempre più affidabile e preciso, con analisi predittive sempre più attendibili ed aderenti alla realtà. È di recente implementazione in alcune località italiane il sistema algoritmico XLAW, un'applicazione di tecniche di polizia predittiva per la sicurezza delle aree urbane basato sulla possibilità di poter prevedere con un tasso di accuratezza attribuito entro un range compreso fra l'ottantasette e il novantaquattro per cento, crimini di tipologia c.d. predatoria quali rapine e truffe. Grazie ad algoritmi di machine learning il sistema offre una soluzione probabilistica per individuare tendenze e pattern negli episodi criminali, ed è in grado di identificare potenziali sospetti di reati e hot spot, luoghi georeferenziati che con alta probabilità si trasformano in scene di possibili crimini.

Il software di polizia predittiva KeyCrime, sviluppato a Milano a partire dal 2007 con lo scopo precipuo di ridurre il numero di rapine perpetrate nei confronti di specifici esercizi commerciali, ha fatto registrare nelle località in cui è stato utilizzato, un calo con picchi dell'ottantotto per cento di tale tipologia di reato[226]. Il modello di previsione fornito dall'algoritmo si basa

[224] Vedi supra, paragrafo 2.1.1.

[225] Secondo il Prof. Di Gennaro G. dell'Università Federico II di Napoli, l'impiego di software di predictive policing "ha spostato il costrutto strategico dell'azione di controllo da una visione riparatoria del danno ad una visione probabilistica del rischio, quindi da una logica di rincorsa dei problemi e degli effetti che essi generano tipica della permanente emergenza, ad una che lavora sugli schemi della prevenzione".

[226] Risultati riportati sul sito ufficiale di KeyCrime relativi al periodo 2009-2017, fonte Questura di Milano: per le rapine in banca la riduzione è dell'88,8%, mentre i dati aggregati delle rapine a Milano con l'utilizzo del software hanno visto una diminuzione di tali reati del 58%. Secondo le analisi basate sui dati ufficiali Ossif la riduzione di tali reati nelle località che si avvalgono del KeyCrime raggiunge agevolmente il 50%.

sull'abitualità dei comportamenti criminali e conseguente prevedibilità di aree e situazioni di rischio, compresi i tratti distintivi delle vittime. Dai dati raccolti vengono estratte informazioni sulle rapine, sugli autori, sulle armi e sui veicoli utilizzati dai criminali, infine sulle stesse vittime. Ciò consente di stabilire dei collegamenti fra le rapine ed individuare comportamenti ricorsivi, le cosiddette serie criminali, permettendo la predizione di nuovi episodi con un'accuratezza sorprendente. L'approccio metodologico del software è completamente differente dallo statunitense PredPol, poiché non prevede una mappatura della città e una ricerca delle zone ad alto rischio di criminalità su cui indirizzare più pattugliamenti a scopo deterrente e preventivo, ma si concentra sulla ricerca di informazioni utili a ricostruire le serie criminali tramite un *crime linking*[227], per anticipare un'azione criminosa sulla base degli eventi precedenti. I risultati di KeyCrime sono stati analizzati dalla Essex University, i cui studi hanno evidenziato il suo maggior punto di forza, nella sua peculiarità di non lavorare su base puramente statistica, come avviene in quasi tutti gli altri applicativi di polizia predittiva, ma di definire anche le modalità dei crimini previsti, grazie ad un'analisi comportamentale dell'autore e dei suoi tratti psicologici. Il maggior limite del KeyCrime[228] è rappresentato, invece, dalle ingenti risorse investigative impiegate durante la delicata fase di collezione dei dati.

Gianos è un software di predictive policing utilizzato dal novanta per cento delle banche italiane per individuare eventuali indici di anomalia che individuano la probabilità di riciclaggio di denaro. Le anomalie sono elaborate da innumerevoli regole prefissate, decise sulla base di minuziose sperimentazioni, messe a punto da un comitato interbancario di esperti sulla base di istruzioni operative emanate della Banca d'Italia.

È invece rimasto a livello sperimentale il progetto S.O.Cr.A.Te.S. la cui finalità è di attuare una matrice statistico-criminologica di criminal profiling, rappresentativa del modello comportamentale di soggetti che si sono macchiati di crimini violenti a sfondo sessuale, nonché le variabili sintomatiche che li legano alla scena di un delitto. Anche in questo caso l'attività predittiva è basata prevalentemente su dati storici riguardanti i delitti avvenuti in tempi relativamente recenti, in maniera analoga al sistema Compas statunitense.

[227] Sulle moderne tecniche di crime linking e criminal profiling, Russo F., *Manuale di criminal profiling. Teorie e tecniche per tracciare il profilo psicologico degli autori di crimini violenti*, Celid Editore, aprile 2018, p.181 ss.
[228] Cfr . Venturi M., *KeyCrime. La chiave del crimine*, in *Profiling*, 14/01/2010, p. 3 ss.

Nel nostro Paese non vi è una regolamentazione legislativa in materia di polizia predittiva. Tuttavia una recente pronuncia del Consiglio di Stato, la sentenza n. 2270 del 08.04.2019, per la prima volta si è espressa in materia di giustizia predittiva ed utilizzo di algoritmi completamente automatizzati, gettando le basi per la futura disciplina. Il caso riguarda la nomina e il trasferimento di docenti avvenuti tramite algoritmi informatici. In virtù delle disfunzioni evidenti emerse, il Consiglio di Stato, dopo aver statuito la liceità dell'utilizzo di operazioni algoritmiche automatizzate, ha colto l'occasione per definire alcuni punti chiave della materia, ritenendo che gli algoritmi dovessero operare in coerenza con i principi di imparzialità, trasparenza, ragionevolezza, proporzionalità, e pubblicità, oltre a dover essere oggettivi e privi di discrezionalità. L'algoritmo deve, poi, essere sottoposto ad aggiornamenti e controlli frequenti che permettano di monitorarne la trasparenza, quest'ultima intesa sia riguardo le modalità operative del sistema, sia la conoscibilità dei soggetti che hanno materialmente elaborato gli algoritmi, i quali devono peraltro predisporre tutte le misure utili per correggere eventuali errori al fine di impedire effetti discriminatori nei confronti delle persone[229].

[229] Secondo il Consiglio di Stato "l'assenza di intervento umano in un'attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica", tuttavia "il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico. […] In secondo luogo, la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo".

Capitolo 3. I rischi connessi alle nuove tecnologie e la tutela dei dati

3.1. Rischi connessi ai big data e alle attività di predictive policing

3.1.1. Violazioni dei diritti umani e discriminazioni

Negli ultimi anni si è riscontrato un incremento esponenziale dell'utilizzo delle moderne tecnologie data driven, dovuto ai benefici che esse possono apportare alla ricerca e alla scienza in innumerevoli settori, con particolare riguardo alle analisi predittive. È necessario, tuttavia, tenere sempre in considerazione i rischi che tali strumenti innovativi possono rappresentare nei confronti di diritti costituzionalmente tutelati, ed in particolare del diritto di eguaglianza e quello della tutela della privacy. La raccolta di dati genetici dei pazienti ha, ad esempio, aiutato in maniera significativa l'individuazione, la prevenzione e la cura di gravi malattie, ma nei casi in cui non sono state predisposte sufficienti precauzioni a tutela dei diritti umani, si è verificata la divulgazione di informazioni personali sensibili. Ove l'utilizzo di tali dati non venga regolato da precisi dettami giuridici e deontologici, il rischio maggiore è quello della c.d. discriminazione genetica, per cui dall'analisi delle informazioni le assicurazioni potrebbero decidere l'entità del premio basandosi sul rischio genetico, oppure le imprese potrebbero decidere politiche di assunzione discriminando alcune fasce di popolazione geneticamente più fragile e maggiormente predisposta alle malattie[230].

L'immagazzinamento e l'analisi di masse di dati eterogenei raccolti dalla rete, ed in particolare l'utilizzo dei big data e le attività di predictive policing si sono rivelati di grande aiuto per l'individuazione di situazioni ad alto rischio di commissione di reati. La concentrazione di risorse umane ed economiche nelle aree a maggior rischio ha sortito il duplice effetto di deterrente con riguardo alla commissione di nuovi crimini e minor spreco di risorse dovuto a controlli mirati e non generalizzati. Nonostante i notevoli risultati ottenuti per merito delle predette tecnologie, numerose sono state le critiche in riferimento al loro utilizzo. Una delle maggiori problematiche riguardanti big data e attività di predictive policing attiene al concreto rischio di alimentare pregiudizi e diseguaglianze, con conseguente violazione di diritti costituzionalmente tutelati[231].

[230] Sulla discriminazione genetica, cfr., Bianchi Clerici G., *Le grandi sfide: open data, genomica, intelligenza artificiale*, in *Garante per la protezione dei dati personali, Big data e Privacy. La nuova geografia dei poteri*, Atti del convegno, 30 gennaio 2017, p.85.

[231] Antonello Soro, Presidente del Garante per la protezione dei dati personali fino al 2020, nell'intervento del gennaio 2017 al Convegno "Big Data e Privacy. La nuova geografia dei poteri", affermava "L'attenzione ai Big Data non può

L'utilizzo dell'intelligenza artificiale e di algoritmi avanzati per la predizione di eventi illeciti deve, difatti, sempre essere dosato con sapienza e moderazione evitando usi scorretti e sproporzionati, e con limiti precisi determinati dalla legge, proprio per non incorrere in problematiche riguardanti il rispetto dei diritti umani, che renderebbero qualsivoglia rimedio tecnologico peggiore del male, con la proposizione di scelte eticamente e giuridicamente inappropriate.

Si pensi al costante pattugliamento delle forze dell'ordine esclusivamente in determinati quartieri identificati dagli algoritmi come luoghi ad alto rischio criminalità o probabilità di reato, oppure al pedinamento di soggetti considerati a rischio di recidiva, o all'inserimento di soggetti nelle *black list* anti terrorismo sulla base dei contatti telefonici e delle relazioni interpersonali. In particolare, l'affidamento ad algoritmi predittivi che processino gigantesche quantità di dati per l'individuazione di aree ad alto rischio di conflitto d'interessi, corruzione, e crimini in genere, può in taluni casi violare diritti costituzionalmente garantiti, pertanto dovrebbe prevedere ampie tutele alla persona e limiti ben determinati[232]. Nello specifico ambito del procurement potrebbe, difatti, verificarsi un controllo continuo ed approfondito soltanto di determinate imprese concorrenti considerate a rischio, o addirittura l'esclusione di un candidato da una gara d'appalto, perché individuato preventivamente dall'algoritmo in potenziale conflitto d'interessi con un membro del personale della stazione appaltante. Il pericolo di discriminazioni ed ingiustizie è, pertanto, concreto, tanto che commissioni ed organizzazioni sovranazionali hanno negli ultimi anni cercato di affrontare la problematica. Al fine di evitare pericolose derive in tal senso, è stata redatta la "Carta etica europea sull'utilizzo dell'intelligenza artificiale"[233], la quale ha identificato cinque princìpi etici fondamentali, prioritari nei confronti della tecnologia:

a. rispetto dei diritti fondamentali;
b. non discriminazione;

riguardare soltanto le sue implicazioni scientifiche e tecniche o gli sconvolgenti effetti delle innovazioni sull'economia. Ci deve preoccupare anche il potenziale discriminatorio che dal loro utilizzo, anche rispetto a dati non identificativi o aggregati, può nascere per effetto di profilazioni sempre più puntuali ed analitiche: in un gioco che finisce per annullare l'unicità della persona, il suo valore, la sua eccezionalità".

[232] In tal senso la Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), per cui "l'apprendimento automatico offre enormi vantaggi economici e innovativi per la società migliorando notevolmente le capacità di analisi dei dati, sebbene ponga nel contempo alcune sfide legate alla necessità di garantire la non discriminazione, il giusto processo, la trasparenza e la comprensibilità dei processi decisionali".

[233] Adottata dalla CEPEJ (Council of Europe, European commission for the efficiency of justice) nel corso della sua trentunesima riunione plenaria, "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment" (Strasburgo, 3-4 dicembre 2018).

c. principio di qualità e sicurezza, con l'utilizzo di fonti certificate e dati non modificabili, in un ambiente tecnologico sicuro;
d. trasparenza, imparzialità ed equità, al fine di rendere i metodi di trattamento dei dati accessibili e comprensibili, autorizzando audit esterni;
e. controllo da parte dell'utilizzatore (il c.d. *under user control*), al fine di prevenire un approccio prescrittivo ed assicurare che gli utenti siano attori informati e nel pieno controllo delle loro scelte.

La Carta vuole fornire un quadro di princìpi destinati ai policy maker, legislatori e professionisti della giustizia con riguardo al rapido sviluppo dell'I.A. soprattutto nei procedimenti giudiziari nazionali. Come si evince dalla Carta, il CEPEJ ritiene che l'introduzione dell'I.A. possa contribuire al miglioramento dell'efficienza e della qualità nel campo della giustizia, a patto che avvenga in modo responsabile e conforme ai diritti fondamentali garantiti, in particolare della Convenzione Europea dei Diritti dell'Uomo (CEDU) e della Convenzione del Consiglio d'Europa sulla protezione dei dati personali. Per il CEPEJ, è essenziale garantire che l'intelligenza artificiale rimanga uno strumento al servizio dell'interesse generale e che rispetti al contempo i diritti individuali. Nel maggio del 2019, il Commissariato per i diritti umani del Consiglio d'Europa[234] ha adottato una raccomandazione indirizzata alle autorità nazionali finalizzata a prevenire l'impatto negativo dell'intelligenza artificiale sui diritti umani, attraverso informazione accurata, trasparenza, e una supervisione indipendente ed efficace sulla conformità delle tecnologie nell'ottica del rispetto dei principi di non discriminazione, uguaglianza e protezione dei dati personali. Allo scopo di predisporre un quadro giuridico per la progettazione e l'applicazione dell'I.A. basata sugli standard del Consiglio d'Europa, è stato istituito nel 2019 il Comitato ad hoc per l'Intelligenza Artificiale (CAHAI), il cui obiettivo è quello di valutare l'impatto delle applicazioni dell'I.A. su individuo e società, in considerazione delle norme vigenti e degli strumenti di soft law. Su tali basi, l'European Union Agency for Fundamental Rights si è fatta carico, in un report del dicembre 2020[235], di esporre la necessità di una valutazione d'impatto più ampia, distinguendo macroaree nelle quali la valutazione deve essere più incisiva: servizi sociali, polizia predittiva, servizi sanitari,

[234] Council of Europe, Unboxing artificial intelligence: 10 steps to protect human rights, maggio 2019.
[235] European Union Agency for Fundamental Rights, Report *Getting the future right artificial intelligence and fundamental rights*, 14 dicembre 2020.

pubblicità mirata. Sono considerate applicazioni rischiose che necessitano particolari garanzie la profilazione, il tracing sanitario, le attività di polizia predittiva.

Un punto fondamentale vagliato dalla dottrina più critica nei confronti delle tecniche predittive è l'affidabilità ed integrità dei dati processati e la distorta interpretazione degli stessi. L'analisi delle informazioni per prevedere i punti caldi del crimine si basa su dati storici, e sul principio che determinate aree necessitino di maggiori controlli. Tali controlli nei confronti dell'area attenzionata, faranno aumentare l'individuazione di illeciti, innalzando ulteriormente l'indice di rischio, creando così un circolo vizioso. Nelle aree maggiormente a rischio, pertanto, gli individui hanno maggior probabilità degli abitanti di altre aree, di essere controllati, individuati, sottoposti a procedimento e condannati. L'idea che le tecnologie predittive data driven giustifichino l'aumento delle misure di sorveglianza in relazione a gruppi e individui presumibilmente ad alto rischio, può apparire discriminatoria. Le statistiche raccolte sulla base di una politica intollerante contro etnie determinate creeranno previsioni a loro volta discriminatorie, traducendosi in un eccesso di sorveglianza che continuerà a generare dati fuorvianti e previsioni razziste. Anche a livello individuale e non solo di gruppi sociali l'asimmetria dei sistemi evidenzia la miopia delle analisi predittive, esacerbando tendenze basate unicamente sulla traduzione numerica dei tassi di criminalità rilevati, piuttosto che su quella effettiva. Senza limiti giuridici e correttivi l'utilizzo dei sistemi predittivi avrebbe fattori negativi di gran lunga maggiori nei confronti dei benefici.

Prima fra tutte, l'American Civil Liberties Union (ACLU) ha criticato la pratica del profiling razziale, affermando che, ove alimentato con dati distorti, l'algoritmo amplifica i pregiudizi che emergono dai processi convenzionali, intensificando ulteriormente le discrepanze ingiustificate nell'applicazione concreta. A livello sistemico, poi, metodologie di policing predittive possono minare la fiducia della comunità nei confronti delle forze dell'ordine e della giustizia, esasperando altresì lo scontro etnico e sociale ed incentivando l'intolleranza. L'automatizzazione dell'analisi dei dati, unita alla complessità e segretezza degli algoritmi, deresponsabilizza gli organi deputati al controllo, minando la capacità di giustificare decisioni e modalità di valutazione dei rischi, che potrebbero essere basate su dati distorti o sistemi di previsione difettosi. Soltanto un quadro giuridico completo applicato a queste tecnologie potrà limitare i rischi di distorsioni e comportamenti sproporzionati che possono trasformare un utile strumento di supporto alla giustizia e alle operazioni di polizia, in un vessillo autoritario e discriminatorio, motivo di dissapori, recriminazioni e ribellioni.

La trasparenza è un altro punto nodale della questione *de qua*. Di norma, difatti, gli algoritmi non vengono resi pubblici, per la tutela della proprietà intellettuale, non potendo, così, essere verificati dalle parti danneggiate a causa del loro utilizzo. Ciò costituisce non solo un nocumento al principio della trasparenza, ma altresì una negazione del diritto di difesa, costituzionalmente garantito all'articolo 24[236]. Un processo decisionale algoritmico trasparente potrebbe essere un primo passo per affrontare giuridicamente il pericolo innanzi sollevato.

Oltre all'affidabilità ed integrità dei dati, ed alla trasparenza, un altro punto centrale è la capacità degli analisti di decifrarli. Al fine di tutelare i diritti umani è, pertanto, di primaria importanza una raccolta e lettura dei dati acritica e senza aspettative da parte dell'analista. Nelle tecnologie predittive guidate dai dati, appare prioritariamente discutibile l'idea che l'estrazione di informazioni riguardanti specifici gruppi o individui per valutare la probabilità che possano commettere un crimine, giustifichi l'intensificazione delle misure di sorveglianza. Ove i controlli si concentrino in relazione a gruppi ed individui presumibilmente ad alto rischio, si corre il pericolo di sovvertire le basi su cui si fondano i concetti di misura specialpreventiva e generalpreventiva, ma anche le stesse basi su cui è stato edificato il moderno pensiero di diritto penale dei Paesi democratici e dei sistemi accusatori, ossia la presunzione di innocenza.

Bisogna, difatti, considerare che l'utilizzo dei dati personali per prevedere le inclinazioni di un individuo alla commissione di crimini, può rappresentare una seria minaccia al principio di rango costituzionale e sovranazionale della presunzione di non colpevolezza[237], secondo il quale tutti devono essere considerati e trattati come innocenti fino a prova contraria, e soprattutto fino alla sentenza di condanna definitiva. Riguardo tale problematica, più volte sollevata dalla dottrina[238], lo scrivente ritiene che alcun rischio di discriminazione possa sorgere in riferimento a semplici controlli, ovvero alla concentrazione di sorveglianza in determinate aree. Ovviamente i controlli non devono mai sconfinare in operazioni di polizia invasive e limitative della libertà, quali

[236] Secondo il comma 1 dell'art. 24 Cost. "Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi". Nel caso in cui gli algoritmi restassero segreti, verrebbe a mancare l'effettività del diritto di difesa, con la sopravvivenza del solo diritto formale, esteriore e svuotato di significato.

[237] Art. 27 comma 2 della Costituzione, secondo cui "l'imputato non è considerato colpevole sino alla condanna definitiva". Tale regola è precisata all'art. 6, co. 2, della Convenzione Europea dei Diritti dell'Uomo, in base alla quale "ogni persona accusata di un reato è presunta innocente sino a quando la sua colpevolezza non sia stata legalmente accertata".

[238] Kremer J., *The end of freedom in public places? Privacy problems arising from surveillance of the European public space*, Univ. Helsinki, 2017, p. 269 ss.; Polidoro D., *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio Penale*, n. 3/2020, p. 6 ss.

perquisizioni, arresti, ovvero decisioni giudiziarie basate sull'utilizzo dei big data e sulle attività di predictive policing.

È dunque opportuno che l'analisi predittiva data driven sia condotta con "greater algorithmic accountability and transparency"[239] tramite la predisposizione di misure che assicurino la trasparenza impedendo, altresì, la violazione dei diritti umani in tema di discriminazione, violazione del diritto alla privacy e presunzione di innocenza, evitando ogni decisione vincolante automatizzata. Solo il rispetto di garanzie minime può ridurre i profili di incompatibilità dell'utilizzo dei big data e della predictive policing con la tutela dei diritti fondamentali, legittimando il ricorso da parte delle forze dell'ordine a pratiche che offrono potenzialità elevate nel contrasto al crimine ed alla corruzione[240].

Il momento più delicato nell'ambito delle funzioni predittive data driven è certamente l'estrazione massiva di informazioni dai dataset e la conseguente organizzazione dei dati, nonché la profilazione di determinate categorie di soggetti al fine di segmentarli in gruppi a seconda del comportamento rilevato. Tuttavia nei casi in cui venga in rilievo la funzione di prevenzione e non sanzionatoria di fenomeni corruttivi, la conoscenza dell'identità della persona risulta generalmente marginale, acquisendo rilievo il dato aggregato al fine di poter compiere delle tipizzazioni, ossia il riconoscimento di individui modello in grado di rappresentare gruppi di persone che rientrano in un determinato profilo e che realizzeranno con alta probabilità le scelte effettuate dal c.d. tipo ideale. In tali casi il problema della tutela dei dati risulta marginale nei confronti del rispetto di altri diritti dell'individuo quali l'eguaglianza e la presunzione di non colpevolezza.

Con riguardo all'utilizzo della tecnologia predittiva si è visto che problema principale è quello della qualità e dell'affidabilità dei dati oggetto dell'analisi informatica. È, difatti, assente uno standard tecnologico minimo, pertanto è il creatore del software a stabilire le istruzioni da impartire all'algoritmo e l'analisi e confronto dei dati raccolti. Ciò in quanto manca una regolamentazione in materia, cosicché ogni organizzazione ha assoluta libertà nello strutturare i suddetti sistemi. Sarebbe, in prima analisi, necessario sopperire all'assenza di tali regolamentazioni, con precetti

[239] European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, par. 8.
[240] In tal senso anche Babuta A., *Pseudomysation is likely to be the only way to perform big data analytics on personal datasets while complying with data protection law*.

precisi che stabiliscano dei livelli minimi di affidabilità e linee guida che infondano uniformità alle procedure[241]. Solo partendo da tale presupposto i fattori di rischio identificati dai big data possono risultare affidabili e credibili. La principale causa di risultati distorti e predizioni inesatte deriva essenzialmente dall'inaffidabilità dei dati presenti nella rete, col rischio di risultati parziali e fuorvianti. Le amministrazioni pubbliche, tuttavia, possono contare su un patrimonio informativo affidabile composto da atti pubblici e banche dati come quella degli appalti pubblici, i cui contenuti si rivelano attendibili per individuare red flag nella prevenzione della corruzione. Soltanto se i dati di origine sono attendibili e se l'analisi viene compiuta avvalendosi di algoritmi neutrali, i software possono individuare anomalie ed elaborare report di gestione del rischio e scenari differenziati, precisi ed attendibili. L'impiego di tecnologie e software che filtrino i dati, conservando ed utilizzando tutti quelli affidabili reperiti dalle banche dati dell'amministrazione, e trattando con maggior selettività tutti quei dati inaffidabili provenienti dal web, permetterebbe una maggior efficienza nella gestione del rischio, coerentemente con uno sviluppo e perfezionamento dei piani triennali anticorruzione[242].

Un altro rilevante problema riguarda l'affidamento ad aziende private dell'*information technology*, del compito di raccolta, estrazione e selezione dei dati. Non si può, invero, lasciare al privato un compito tipicamente pubblicistico come quello di prevenire reati e fenomeni illeciti senza fornirgli adeguati strumenti normativi che gli consentano di svolgere tale ruolo, limitandone nel contempo i poteri decisionali. L'utilizzo degli algoritmi in chiave di prevenzione della criminalità pone l'esigenza di approntare, sulla scia di una regolamentazione del fenomeno nell'ambito pubblico, una disciplina nel settore privato soprattutto improntata sulla trasparenza e sul rispetto dei diritti fondamentali, nonché sulla limitazione del potere di coloro che raccolgono, analizzano e processano i dati[243].

A fronte dei vantaggi dei big data, delle funzioni predittive degli algoritmi nel rafforzamento dei sistemi di *compliance* anticorruzione e di innovative metodologie di gestione del rischio, l'utilizzo dei relativi software richiede un deciso intervento legislativo che bilanci equamente i diversi interessi in gioco. Guardare con fiducia all'utilizzo dell'intelligenza artificiale, dei big data analytics

[241] Si tratta di procedure polimorfe, in grado cioè di assumere rilievo, a seconda delle tecniche con cui sono costruite e implementate, sia nell'ambito del risk assessment, che nell'ambito del risk management.
[242] Cfr. Birritteri E., *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Diritto penale contemporaneo*, 2/2019, p. 289 e ss.
[243] Della Morte G., *Big data e protezione internazionale dei diritti umani*. *Regole e conflitti*, Editoriale Scientifica, Napoli 2018, p. 145 ss.

e delle tecniche predittive nell'ambito delle attività di controllo e sorveglianza, delle indagini e perfino della funzione giurisdizionale, è un atteggiamento pienamente condivisibile, a patto che vi siano regole precise che pongano specifici limiti alle scelte operate in base ai risultati estrapolati dai dati. Tali limiti possono essere indubitabilmente assimilati con i cinque princìpi etici fondamentali enucleati nella Carta etica europea sull'utilizzo dell'intelligenza artificiale, ossia rispetto dei diritti fondamentali, non discriminazione, sicurezza, trasparenza ed equità, controllo umano.

3.1.2. I c.d. bias e le distorsioni nell'analisi dei dati

I big data sono uno strumento innovativo utilissimo sia nelle aziende che in ogni organizzazione ed istituzione, tuttavia possono contenere insidie e rischi. Quello maggiore è costituito dalla poca attendibilità della maggior parte dei dati provenienti dalla rete. Ove non si riuscisse a raggiungere un sufficiente livello di affidabilità, anche le scelte determinate in base a tali informazioni, la gestione dei rischi, nonché le analisi predittive risulterebbero imprecise o erronee. I rischi, tuttavia, non derivano unicamente dalla qualità dei dati originari. Sarà, difatti, compito di algoritmi dotati di intelligenza artificiale riuscire ad organizzare, selezionare e confrontare le informazioni raccolte per renderle affidabili ed utili agli scopi cui sono destinate. I pericoli di attendibilità dei risultati derivano prevalentemente dalla struttura dell'algoritmo stesso, che potrebbe operare una distorsione delle informazioni analizzate, rischiando di rendere il dato inaffidabile, limitato e potenzialmente pericoloso, con particolare riguardo al rischio di discriminazioni sociali. In tali ipotesi si parla di "bias", pregiudizi insiti nello sviluppo e gestione degli algoritmi, e dalla cui individuazione dipenderà l'accuratezza delle informazioni oppure una distorsione dei dati.

Per bias cognitivi si intendono quelle scorciatoie mentali che inducono ad analizzare le informazioni per blocchi, creando delle routine che una volta acquisite non vengono più messe in discussione anche se potenzialmente errate e fuorvianti. Allo stesso modo anche gli algoritmi, nel processare gruppi di informazioni, possono generare dei bias. Gli algoritmi, difatti, analizzano con approccio statistico un'enorme quantità di dati per trovare elementi comuni da cui ottenere previsioni comportamentali sempre più precise. Un presupposto errato può essere la base per un dilatamento dell'errore da parte dell'algoritmo che lo processa. Ciò può creare evidenti problematiche di affidabilità delle previsioni e dei modelli, e soprattutto distorsioni e pericolo di

discriminazioni. È, pertanto, necessario il rapido sviluppo di un'etica dei dati, e di normative di ampia visuale, dirette specificamente ai programmatori degli algoritmi ed ai responsabili dei team di sviluppo. Da tale punto di vista l'Europa ha già posto le basi per la diffusione di regole universali per definirne con certezza i limiti e le opportunità, e per sollevare una coscienza collettiva in materia di intelligenza artificiale.

Norme e linee guida possono fissare dei limiti ex post riguardo lo sviluppo e diffusione dell'algoritmo, tuttavia, le maggiori difficoltà non sono giuridiche o etiche, bensì attengono strettamente al settore tecnico-informatico. Più elevate sono le quantità dei dati processati, più il bias potrà nascondersi e mimetizzarsi, soprattutto nei casi in cui il codice dell'algoritmo sia tenuto segreto e non possa essere controllato da soggetti esterni all'organizzazione che lo ha progettato o che lo utilizza. Il rischio maggiore è che la distorsione venga standardizzata. Ciò avviene qualora le moderne tecnologie di machine learning, che permettono ai sistemi di apprendere sulle esperienze trascorse, vanno ad interessare anche altri sistemi, i quali ereditano i pregiudizi dall'algoritmo che li conteneva originariamente.

Un famoso esempio riguarda il software di reclutamento del personale di Amazon, il quale per una serie di distorsioni storiche e bias, ha privilegiato per lungo tempo le assunzioni maschili rispetto a quelle femminili. L'apprendimento automatico del sistema, abituato a ricevere molti più curriculum di candidati di sesso maschile, si era autoistruito prediligendo profili maschili nei confronti di quelli femminili. Un problema simile si è presentato con il c.d. gender bias di LinkedIn che produceva risultati distorti privilegiando candidati uomini rispetto alle donne. Ciò in quanto nelle posizioni disponibili gli uomini erano maggiormente presenti risultando, erroneamente, più propensi a cercare nuove opportunità lavorative rispetto alle donne. Oggi LinkedIn utilizza algoritmi che escludono il nome, l'età, il sesso e la razza di una persona, in quanto tali caratteristiche possono contribuire a distorsioni nei processi automatizzati. Nel Regno Unito i sistemi automatizzati per la prevenzione dei crimini sono stati oggetto di aspre critiche da parte degli studiosi[244], i quali hanno mostrato come i dati raccolti, già discriminatori in origine, siano stati analizzati da algoritmi che hanno consolidato i pregiudizi mettendo in pericolo i diritti umani, ed in particolare discriminando le minoranze ed etnie.

[244] Il Royal United Service Institute ha condotto nel 2019 uno studio sulla difesa e la sicurezza del Regno Unito, che evidenzia i pregiudizi nei confronti della popolazione di pelle nera da parte dei sistemi di giustizia predittiva basati sui rapporti delle forze dell'ordine, considerati più inclini a commettere reati.

Un caso di algoritmo ritenuto discriminatorio che in Italia ha avuto particolare risonanza ha riguardato la vicenda giudiziaria CGIL contro Deliveroo, poiché è stata la prima causa del nostro Paese avente ad oggetto un bias causato dal machine learning di un software. Il sindacato nazionale adiva il giudice del lavoro, per tutelare un interesse collettivo della categoria dei c.d. riders, lamentando un comportamento discriminatorio dell'azienda dovuto ad un bias dell'algoritmo chiamato "Frank", utilizzato dalla stessa per assegnare le consegne ai lavoratori. Secondo CGIL l'azienda escludeva da ulteriori impieghi i lavoratori che per motivi costituzionalmente tutelati, come malattia e sciopero, non si rendevano continuativamente disponibili al lavoro. In tale contesto i riders che non si adeguavano al meccanismo su cui era basato l'algoritmo, venivano declassati ingiustamente dal ciclo produttivo aziendale e gradualmente esclusi da ogni possibilità di impiego nell'azienda stessa. Il bias era generato dalla mancata distinzione fra assenze giustificate da reali esigenze ed assenze ingiustificate e non tutelate costituzionalmente. In pratica venivano penalizzati anche i lavoratori assenti per malattia, che venivano trattati alla stessa stregua di coloro che risultavano assenti ingiustificati. Il Tribunale di Bologna ha stabilito, così, con ordinanza del 31 dicembre 2020 che l'algoritmo fosse discriminatorio, condannando la Deliveroo[245]. Il pregiudizio dell'algoritmo è, in quest'ultimo caso, generato non da un errore di programmazione o dati analizzati in maniera scorretta, ma da una semplice omissione nel referenziare i dati, tuttavia l'intelligenza artificiale ha amplificato il bias generando dati distorti e lesivi nei confronti dei diritti dei lavoratori. Conseguentemente alla sentenza di condanna, la Deliveroo ha sostituito la piattaforma con una più moderna, dotata di un algoritmo più sofisticato e non discriminatorio[246].

La vicenda giudiziaria riguardante i riders riporta in primo piano un problema già precedentemente affrontato: in un contesto di contenzioso è indispensabile lasciare alle parti la possibilità di analizzare il codice sorgente e rilevare altre informazioni tecniche circa il processo di generazione del dato al fine di effettuare una verifica dei risultati dell'elaborazione di un software e contestarne l'affidabilità, per poter correttamente esercitare il diritto di difesa costituzionalmente garantito[247]. Senza la c.d. trasparenza algoritmica, ossia l'accesso al codice di

[245] Tribunale di Bologna, Sezione Lavoro, CGIL contro Deliveroo, Causa iscritta al RG n. 2949/2019.

[246] Secondo le dichiarazioni del General manager di Deliveroo Italy, Matteo Sarzana la decisione del giudice "fa riferimento a un sistema di prenotazione delle sessioni dei rider che non è più in uso […] perché dal mese di novembre questa tecnologia è stata sostituita da un'altra, più moderna, che non prevede l'uso di statistiche, pertanto questa decisione non ha alcun impatto sul nostro modello di business".

[247] Cfr. Quattrocolo S., *Artificial intelligence, Computational Modelling and Criminal Proceedings*, Springer 2020, p. 12 ss.

programmazione dell'algoritmo ed altre informazioni tecniche circa il processo di generazione del dato, risulta difatti impossibile contestare l'attendibilità dell'informazione analizzata automaticamente, inibendo qualsivoglia possibilità di agire in giudizio per far valere le proprie ragioni[248]. Ove venisse negato l'accesso al codice sorgente, generalmente con la giustificazione basata su motivazioni riguardanti la proprietà intellettuale, una soluzione ragionevole che non mortifica il diritto di difesa di entrambe le parti, potrebbe essere la presunzione di discriminazione in casi non manifestamente infondati, ossia l'inversione dell'onere della prova, per cui dovrebbe essere il produttore del software a dimostrare la veridicità e la correttezza dei risultati dell'algoritmo, e non viceversa.

3.1.3. Le minacce dell'I.A. ai diritti umani nel panorama extracontinentale

Big data, machine learning e predictive policing sono ampiamente utilizzati negli Stati Uniti, ove le strategie di prevenzione del crimine per l'identificazione di aree e quartieri a rischio, incidono fortemente sulla riduzione dei reati violenti. Notevoli sono, tuttavia, le perplessità sollevate con riguardo al pericolo di compressione dei diritti umani ed in particolare di diseguaglianze e discriminazioni, nonché invasione nella sfera privata delle persone. Con il programma PRISM[249], prima gli Stati Uniti, poi anche Francia e Gran Bretagna, hanno utilizzato un piano di sorveglianza di massa indifferenziato, per conservare ed analizzare dati sensibili di cittadini statunitensi ed europei[250]. Grande clamore internazionale ha sollevato il caso "datagate" che ha svelato una rete di intercettazioni e controllo del traffico informatico e telefonico, organizzata dalla National Security Agency (NSA) statunitense nei confronti di cittadini e uomini politici europei. Anche le maggiori multinazionali dell'informatica come Google e Facebook e i colossi della telefonia e informatica come Apple, lamentano di dover sottostare costantemente alle richieste di accesso da parte del governo statunitense ai profili personali degli utenti, con grave violazione del diritto alla privacy[251]. Ma il problema della privacy non è l'unico nel nuovo continente a creare un conflitto fra nuove tecnologie e diritti umani. Difatti in America gli algoritmi predittivi vengono utilizzati nelle aule di tribunale (c.d. giustizia predittiva) nella fase preliminare al giudizio per la

[248] Cfr. Palmiotto F., *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in *Algotirhmic Governance and Governance of Algorithms*, Ebers M., Cantero Gamito M. (a cura di), 2020.

[249] Nino M., *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, 2013, 440 ss.

[250] Della Morte G., *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli 2018, 178 ss.

[251] Apple nel rapporto sulla trasparenza pubblicato il 25 maggio 2018 rivela che nella sola prima parte dell'anno ha ricevuto dal governo statunitense 16.249 richieste di accesso a dati personali di utenti per fini di sicurezza nazionale.

determinazione della cauzione[252], ed anche nella fase dibattimentale per valutare l'eventuale messa alla prova o il pericolo di recidiva dell'imputato. Emblematico è, al riguardo, il caso Suprema Corte del Wisconsin vs./Eric L. Loomis, divenuto famoso in quanto la Corte fondò alcune scelte riguardanti la recidiva, sugli esiti degli algoritmi di giustizia predittiva del software Compas[253]. Da un'analisi di organizzazioni indipendenti, fra cui ProPublica, il funzionamento di tale software ha evidenziato non soltanto una palese carenza di trasparenza, ma anche risultati discriminatori, con il calcolo di una probabilità di recidiva di crimini violenti dei soggetti di pelle nera maggiore del settantasette per cento rispetto ai bianchi. La vicenda, seppur strumentalizzata, ha avuto il merito di focalizzare l'attenzione dell'opinione pubblica sulle criticità dei sistemi di giustizia che si avvalgono di algoritmi predittivi.

In tema di polizia predittiva e I.A., la privacy e soprattutto il diritto a non essere discriminati sono ancor meno tutelati in Asia. Il Police Cloud System cinese consente alle forze dell'ordine un capillare controllo sui cittadini, creando un'immensa rete di sorveglianza comprendente conversazioni telefoniche, espressioni del volto, ed un costante controllo degli spostamenti grazie a un potente sistema di tecnologie integrate gestite da applicazioni con intelligenza artificiale[254]. Un'altra piattaforma cinese, la Integrated Joint Operations Platform si concentra, invece, sull'analisi dei dati di determinate minoranze religiose di specifiche aree[255]. Tramite il software gli appartenenti alla minoranza etnica analizzata vengono sorvegliati e profilati grazie ai sensori presenti nelle videocamere dotate di riconoscimento facciale, spyware installati nei telefonini e wi-fi sniffer. Vengono perfino analizzati i consumi domestici di energia delle famiglie per estrarne dati comportamentali individuali e condividerne poi le informazioni. Nel caso appena rappresentato, oltre alla violazione della privacy, sorgono evidenti problematiche riguardanti la discriminazione di minoranze ed etnie a dispetto del principio di eguaglianza. Sempre in Cina è sorto nell'ultimo decennio un vero e proprio sistema di controllo sociale, noto come Chinese

[252] Il più diffuso software utilizzato nella fase pre-trial è il Public Safety Assessment (PSA), col compito di supportare i giudici nelle decisioni riguardanti il rilascio su cauzione o la carcerazione preventiva.
[253] Cfr., sul caso Loomis, Yong E., *A che servono gli algoritmi nei tribunali statunitensi*, in *The Atlantic*, U.S.A., febbraio 2018; Celella R., *L'algoritmo che condanna: i limiti della giustizia predittiva*, in *Data Protection Law*, maggio 2019; V. Vescio di Martirano, *Algoritmo e giustizia predittiva in campo penale*, in *Altalex*, giugno 2019.
[254] Lo studio dello Human Rights Watch, *China: Police 'Big Data' Systems Violate Privacy, Target Dissent Automated Systems Track People Authorities Claim 'Threatening'*, 19 novembre 2017, afferma che il Police Cloud System cinese incrocia "data routinely gathered by China's police, such as residential addresses, family relations, birth control methods, and religious affiliations" e "hotel, flight and train records, biometrics, CCTV footage, and information from other government departments and even private companies".
[255] Nello specifico la minoranza musulmana degli Uliguri stanziata nello Xinjiang, a ovest della Cina.

Social Credit System, che attribuisce un rating ai cittadini a seconda dei pagamenti effettuati on line di multe e debiti, del rispetto delle norme, e della coerenza delle idee politiche nei confronti della linea del Governo. Tale rating influisce su rilevanti questioni, quali la possibilità di ottenere un visto per andare all'estero, ottenere prestiti, trovare alloggio, iscrivere i figli nelle migliori scuole. Se il rating, calcolato da un algoritmo di machine learning, scende oltre un determinato livello, verranno conseguentemente compressi i diritti della persona, che non potrà più avvalersi di sgravi fiscali o ottenere mutui, mandare i figli nelle scuole desiderate, e sarà perfino inibito l'acquisto di biglietti aerei o treni veloci. Ma la peculiarità più pericolosa in termini di controllo sociale, in quanto crea l'isolamento delle famiglie inserite nella black list, si concretizza nell'abbassamento del rating in base a quello di amici e conoscenti. Ciò non solo discrimina frange di popolazione, ma emargina tutti coloro che hanno un basso rating, isolandoli da parenti ed amici. Un utilizzo così estremo delle tecnologie di machine learning ed intelligenza artificiale può sembrare lontano dalle democrazie occidentali, ma così non è. Vari sistemi, seppur differenti nell'applicazione ma con peculiarità analoghe, hanno avuto recentemente diffusione nei Paesi anglosassoni. Ne è un esempio il software PatronScan, che permette di rilevare le generalità di persone che hanno creato problemi nei locali preposti alla ristorazione. Agli avventori segnalati potrà essere impedito l'accesso nei locali che vorranno frequentare in futuro, qualora il gestore lo riterrà opportuno. A ben vedere anche in quest'ultimo caso, il controllo dell'individuo è finalizzato esclusivamente ad una valutazione dei suoi comportamenti, ed a una conseguente eventuale compressione dei suoi diritti.

Anche in Europa vi sono Paesi che si avvalgono in maniera massiccia dei big data e dell'intelligenza artificiale per la raccolta di informazioni, nonché dell'analisi predittiva: in Danimarca attraverso una normativa che amplifica le possibilità di intrusione dei corpi di polizia nei dati personali, e l'ausilio della piattaforma POL-INTEL, che incrocia ed analizza banche dati delle forze dell'ordine, Internet e videosorveglianza, la tutela della privacy dei cittadini ha subìto una grave limitazione[256]. Si aggiunga che la gestione della piattaforma e l'analisi dei dati sono affidate a società private, che potrebbero utilizzare le informazioni per interessi personali o per discriminare determinate classi sociali o settori professionali. La segretezza degli algoritmi e dei software rappresentano, poi, un limite al principio di trasparenza. A tal fine sarebbe necessario imporre, per tali tipi di

[256] Con riguarda all'attività di polizia predittiva in Danimarca, si veda *New Legal Framework for Predictive Policing in Denmark*, in *EDRi*, 22 febbraio 2017.

algoritmi, soprattutto se utilizzati da istituzioni pubbliche, l'impiego di tecnologie open source, con la possibilità da parte di chiunque di poter esaminare il codice sorgente e le routine di programmazione degli stessi.

L'Olanda è stata recentemente oggetto di un rapporto di Amnesty International, che critica aspramente l'utilizzo di sistemi di algoritmi generanti una sorveglianza di massa indiscriminata e profilazione etnica. Il rapporto documenta i pericoli generati da nuovi progetti, definiti "laboratori viventi", di controllo predittivo delle forze di polizia olandese. I modelli matematici utilizzati per valutare il rischio di perpetrazione di un reato sono considerati da Amnesty International altamente discriminatori. Nello specifico è stato esaminato un progetto di sorveglianza predittiva nella città di Roermond, chiamato "Progetto di rilevamento". Esso rischia di rendere le persone di Roermond delle vere e proprie cavie della sorveglianza di massa, ma è soprattutto discriminatorio nei confronti di soggetti di nazionalità dell'Europa dell'Est[257]. Attraverso l'utilizzo di telecamere e di altri sensori, la polizia monitora in maniera sistematica gli spostamenti nei pressi della città, raccogliendo informazioni in merito a veicoli e modalità di spostamento. I dati raccolti sono poi elaborati utilizzando un modello algoritmico che calcola un "punteggio di rischio" in merito alla probabilità di commissione di un reato contro il patrimonio. Fra gli indicatori utilizzati ai fini di questa valutazione vi è la provenienza di un veicolo dall'Europa orientale. Qualora venga classificato un veicolo ad alto rischio, la polizia effettuerà approfonditi controlli. La mancanza nelle normative olandesi di adeguate garanzie giuridiche riguardo fermi e perquisizioni arbitrari rende il rischio discriminatorio nei confronti di soggetti provenienti dall'Est europeo, ancora più alto.

Dal 2014 l'Italia ricorre ad un programma di predictive policing, il software Key-Crime, che si avvale di algoritmi complessi per l'individuazione di potenziali profili criminali. L'algoritmo matematico, creato da Mario Venturi, "elabora e incrocia tutti i dati: corporatura, abbigliamento, modus operandi, orari, luoghi e dà un risultato, proponendo al poliziotto una serie di eventi che sono potenzialmente collegabili con quello appena inserito. Questa procedura permette di

[257] Amnesty International ha pubblicamente condannato il "Progetto di rilevamento" dell'Olanda, considerandolo pregiudizievole e discriminatorio. Secondo Merel Koning, responsabile del programma tecnologia e diritti umani della famosa organizzazione non governativa "Il problematico esperimento di Roermond, che profila e discrimina le persone dell'Europa dell'est, mette in luce la natura pregiudizievole, e non predittiva, dei sistemi di polizia di tipo algoritmico. Questo genere di progetti si stanno moltiplicando rapidamente in tutto il paese, mentre sono carenti le garanzie necessarie per affrontare le numerose minacce che pongono nei confronti dei diritti umani".

collegare tra loro dei reati che altrimenti potrebbero rimanere fatti singoli"[258]. L'invasione nella sfera privata dell'individuo viene giustificata con esigenze di sicurezza pubblica, che consentono la sorveglianza sulle persone, ed hanno origine, almeno nel nostro Paese, nella lotta al terrorismo, per estendersi, poi, a tuti gli altri reati di alto allarme sociale, ed infine anche ai reati corruttivi e recentemente a quelli comuni. Non vi è dubbio, tuttavia, che l'analisi di dati personali e sensibili di individui che abbiano già avuto problemi con la giustizia, sia un elemento di discriminazione oltre che di invasione della privacy. La profilazione dei dati sull'etnia, poi, lascia perplesse molte associazioni non governative che da anni si battono contro la discriminazione[259].

L'applicativo Serpico[260], già in uso in Italia da alcuni anni, permette ad Agenzia delle Entrate e alla Guardia di Finanza di accedere a tutte le transazioni bancarie dei residenti in Italia, alle utenze, alle banche dati di Inps, Inail e motorizzazione, consente il controllo di patrimoni immobiliari, eventuali investimenti finanziari, la stipulazione di polizze assicurative e tutto ciò che può rivelarsi utile per rilevare anomalie e contrastare l'evasione fiscale. La mole di informazioni personali che Serpico può processare ogni secondo è impressionante[261]. Ciò costituisce una evidente violazione del diritto alla privacy, basti pensare che il sistema ha un accesso completo agli oltre quaranta milioni di conti correnti presenti nel nostro Paese. Quanto detto è aggravato dal fatto che il software sia progettato, aggiornato e gestito da una società privata, che potrebbe in linea di principio sfruttare informazioni private e sensibili a proprio vantaggio.

Oltre al rischio delle raccolte governative di dati e delle analisi predittive effettuate da ministeri ed enti pubblici, si corre in ogni Paese il rischio della crescita di un sistema di controllo parallelo a quello istituzionale, con effetti ancora più problematici, come l'affievolimento della privacy o l'assenza della presunzione di innocenza, attuato da privati senza alcuna sorta di controllo. A questo si aggiunga l'attività di profiling, riconoscimento facciale ed analisi predittiva effettuata da organizzazioni militari e paramilitari, che spesso agiscono senza alcun riconoscimento istituzionale. Non esiste nessuna garanzia che le regole vengano applicate in maniera corretta e controllata, e non arbitraria ed immotivata, e nella maggior parte dei casi non vi è alcuna possibilità di difendersi poiché manca una regolamentazione sulla trasparenza degli algoritmi.

[258] Morabito C., *La chiave del crimine*, in *Polizia Moderna*, luglio 2015.
[259] È lo stesso ideatore di KeyCrime, Mario Venturi, ad affermare che "A livello di indagine, le informazioni sull'etnia di chi ha compiuto i crimini sono fondamentali".
[260] Vedi supra, par. 2.2.3.
[261] Ha il potenziale per processare 22.000 operazioni al secondo.

Soltanto colmando il gap fra progresso tecnologico e legislativo si possono creare precetti che rendano i big data e l'analisi predittiva una risorsa, e non un problema sociale globalizzato del terzo millennio.

3.1.4. Violazione della privacy e tutela dei dati personali

La tecnologia è entrata in maniera sempre più pervasiva nel settore della giustizia sia nella fase delle indagini che durante il dibattimento, momento centrale dell'attuale sistema processuale penale tendenzialmente accusatorio approdato in Italia nel 1988. Un utilizzo altrettanto importante delle moderne tecnologie si ha nella fase di prevenzione dei reati e di individuazione di situazioni di conflitto di interessi che possano far prevedere eventi corruttivi. Le tecnologie informatiche più moderne, ossia i big data, le reti neurali e l'intelligenza artificiale in primis, possono tuttavia favorire diseguaglianze e discriminazioni, nonché limitare la libertà dell'individuo, ostacolando peraltro il legittimo diritto a potersi difendere adeguatamente. Con tali affermazioni non si vuole certo demonizzare l'utilizzo di tecnologie che si avvalgono dei big data, ma è necessario porre sempre in primo piano la protezione dei diritti dell'individuo e le libertà personali.

Il conflitto fra le tecnologie e i diritti umani si manifesta in un modo differente nei confronti del passato anche recente, e richiede una corrispondente riconsiderazione della sfera valoriale. La rilevanza dei molteplici diritti messi a rischio dall'utilizzo delle reti informatiche e dell'intelligenza artificiale è, difatti, mutata rispetto a qualche anno addietro, stante la progressiva ed inesorabile valorizzazione del diritto alla privacy, rilevata specialmente nell'ambito delle istituzioni sovranazionali europee. Il diritto alla riservatezza e la tutela dei dati hanno assunto sempre più importanza nel novero dei diritti umani proprio perché le informazioni possono, oggi, viaggiare da una parte all'altra del pianeta in tempo reale e senza controllo alcuno, influenzando sistemi economici, politici e sociali. L'evoluzione di Internet e l'espansione del processo tecnologico hanno contribuito a spostare il baricentro dello stesso diritto alla privacy, ricomprendendo al suo interno anche la protezione dei dati personali, venendo così a configurarsi prevalentemente come un diritto ad esercitare un controllo sulle proprie informazioni, e ponendo quale paradigma centrale il consenso informato. Tuttavia secondo il parere dello scrivente, nel rapporto dualistico fra tecnologie e diritti umani sarebbe necessario seguire una strategia olistica, che consideri questi ultimi come un *unicum*, e non distinti e frammentati. I diritti dell'uomo, dalla privacy

all'eguaglianza, dalla libertà di pensiero al principio di non colpevolezza, dovrebbero essere, difatti, considerati sulla base dell'interrelazione degli uni con gli altri, e non singolarmente, per poterne stimare appieno l'effettivo impatto sociale, culturale e politico nel complesso. Una valutazione d'insieme dei diritti violati, permetterebbe di stabilire con maggior equilibrio i casi in cui alcuni di essi possano essere sacrificati in ossequio a diritti di maggiore impatto sulle libertà individuali, in considerazione di un controbilanciamento fra contrapposti interessi. Ciò consentirebbe di individuare un limite oltre il quale nessuna tecnologia possa spingersi, poiché sarebbe in ogni caso intollerabile la limitazione dei diritti individuali. Per contro, l'utilizzo della tecnologia potrebbe continuare a vivere ed espandersi, nelle ipotesi in cui la compressione dei diritti possa essere tollerata a fronte di risultati positivi nella lotta a fenomeni comunque limitanti la libertà del singolo e il buon andamento della Pubblica Amministrazione, quali la corruzione ed il conflitto di interessi.

Per poter effettuare analisi predittive utilizzando i dati ed elaborare scenari credibili è necessaria la raccolta di altissime quantità di informazioni, sia pubbliche che private, ed in alcuni casi anche di dati personali sensibili. Nonostante le norme sul consenso informato e sull'anonimato dei dati, sussistono evidenti profili di incompatibilità fra utilizzo dei big data e tutela della privacy, poiché vi è in ogni caso il rischio di una violazione dei diritti individuali connesso alla potenziale identificazione a posteriori dei loro titolari. La morfologia dell'ambiente digitale e la facile reperibilità di dati personali in rete, rende ancor più concreta questa preoccupazione[262]. In particolare l'utilizzo massificato dei social media ha, indubbiamente, amplificato i rischi riguardanti il diritto alla riservatezza ed al trattamento dei dati. Il pericolo di essere tracciati in ogni attività quotidiana, non è più così remoto se si pensa che l'internet banking, i social network, gli acquisti tramite e-commerce e la tracciabilità delle attività in rete permettono a terzi di poter sorvegliare ogni azione del singolo individuo. Se, poi, consideriamo che anche le nostre attività quotidiane al di fuori della rete vengono sempre più monitorate da telecamere di videosorveglianza e i nostri spostamenti tracciati dai sistemi di localizzazione dei telefoni cellulari, può apparire arduo immaginare che il diritto alla privacy possa sopravvivere alla tecnologia. L'estrazione, l'analisi ed il riutilizzo di informazioni pubblicamente disponibili su Internet e di

[262] Sul rapporto nuove tecnologie e privacy si veda: Tosi E., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019, p. 36 ss; per ciò che riguarda lo specifico rapporto fra big data e trattamento dei dati personali: Orefice M., *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, 2018.

filmati delle telecamere a circuito chiuso pongono, difatti, seri rischi alla privacy di ogni individuo ed al suo diritto alla riservatezza. In considerazione della natura sensibile di tali informazioni e della possibilità di intercettazioni ed utilizzi impropri di dati, il fenomeno appare, oggi, particolarmente allarmante con effetti potenzialmente dannosi sulla vita privata e professionale delle persone e violazione dei diritti riguardanti la tutela dei dati[263].

Pur non potendo arrestare il progresso tecnologico, è necessario trovare un punto di equilibrio fra esso ed il diritto alla riservatezza relativo alla sfera privata, ancorato al concetto originario di matrice statunitense "*the right to be let alone*". L'aumento della vulnerabilità degli individui cagionato dai rischi delle nuove tecnologie, può essere contrastato soltanto in parte attraverso la regolamentazione giuridica delle attività degli operatori tecnologici. A tal fine non si può prescindere dall'individuazione, fra i problemi principali, della detenzione del possesso di ampia parte dei dati solo da parte di poche aziende private, e dalle conseguenze di un vero e proprio oligopolio riguardo il potere di raccolta delle informazioni. Alcune multinazionali possiedono, difatti, un immenso patrimonio informativo, in grado di influenzare le scelte delle persone e condizionare trend, comportamenti, opzioni finanziarie, ma anche decisioni politiche e sociali[264]. Sarebbe, pertanto, necessario un obbligo di trasparenza da parte dei detentori dei dati ed il conseguente divieto di raccolta e trattamento degli stessi, se effettuato tramite algoritmi segreti e non basati sulle tecnologie open source[265]. Senza, poi, dimenticare che la raccolta e il riutilizzo continuo delle informazioni contenute nei dataset, nonché la profilazione ed il trattamento di dati personali, ledono il diritto all'oblio, inteso quale diritto al c.d. *de-listing*, ossia alla cancellazione dei propri dati e "ad essere dimenticati" per vicende che nel passato sono state oggetto di cronaca[266]. È necessario, pertanto, che le norme giuridiche e le regolamentazioni vengano

[263] Secondo Soro A., *Big Data e Privacy. La nuova geografia dei poteri*, in *Atti del Convegno - 30 gennaio 2017*, p. 10, "La libertà di ciascuno è insidiata da forme sottili e pervasive di controllo, che noi stessi, più o meno consapevolmente, alimentiamo per l'incontenibile desiderio di continua connessione e condivisione. Da un lato le imprese tecnologiche hanno dilatato la raccolta e la disponibilità dei nostri dati, dall'altro le esigenze di sicurezza, di fronte alla minaccia criminale e terroristica, hanno spinto progressivamente i governi ad estendere il controllo delle attività svolte in rete per finalità investigative in modo sempre più massivo. Il combinarsi di questi processi ha prodotto una straordinaria intrusione nella vita di tutti, una vera e propria sorveglianza, con effetti importanti sui comportamenti individuali e collettivi, sugli stessi caratteri delle nostre democrazie".

[264] Si pensi ai patrimoni di dati personali in possesso di aziende quali Apple, Google, Facebook.

[265] Cfr. audizione del Prof. Mantelero A. (21 novembre 2017), p. 6, secondo il quale vi sarebbe "l'impossibilità di applicare logiche meramente proprietarie ai dati personali o di seguire modelli d'oltreoceano favorevoli all'assimilazione delle informazioni personali all'ambito della proprietà intellettuale".

[266] La Corte di giustizia (Grande Sezione, sentenza del 13 maggio 2014, causa C-131/12, Google Spain), ha affermato (par. 97), che il diritto alla protezione dei dati personali e il cd. diritto all'oblio prevalgono "in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona".

supportate da un approccio etico selettivo, responsabile e senza pregiudizi, basato sulla trasparenza, sul consenso informato, sulla tutela dei dati sensibili, ed infine su un diritto di cronaca che trova il suo naturale limite nel diritto all'oblio[267].

Ove manchi una piena partecipazione informata delle persone interessate al trattamento con i big data analytics, aumentano vertiginosamente i rischi di violazione della tutela dei dati personali. Sono questi i casi sui quali si sono maggiormente concentrati i regolamenti sovranazionali e le autorità garanti dei Paesi democratici. Il Regolamento europeo sulla protezione dei dati[268] introduce importanti garanzie riguardo il trattamento dei dati personali utilizzati senza un pieno consenso informato, quali l'anonimizzazione e la pseudonimizzazione, al fine di eliminare o quanto meno ridurre i rischi di reidentificazione della persona. Tuttavia l'anonimizzazione dei dati raccomandata dal GDPR costituisce una mera illusione, poiché anche nelle raccolte ritenute anonime i dati possono essere successivamente, nuovamente associati ad una specifica persona. È, comunque, da rilevare che, anche nei casi in cui il consenso informato sia liberamente manifestato, sussiste pur sempre un rischio riguardo l'utilizzo che viene fatto delle informazioni, e la possibilità di cessione di dati personali a soggetti terzi, alla stregua di una comune merce di scambio. Non a caso i dati sono stati unanimemente definiti da studiosi e media "l'oro del nuovo millennio", e i sociologi statunitensi hanno già definito il nostro periodo storico qualificandolo con la locuzione "the age of data".

Un valido aiuto può pervenire dalla stessa tecnologia. Le problematiche sorte con la raccolta, l'elaborazione e la manipolazione di enormi masse di dati, ed in particolare quelle riguardanti l'utilizzo e il trattamento di informazioni ed il relativo diritto di privacy, possono essere, difatti, se non risolte almeno limitate con la diffusione, nei casi in cui sia possibile il suo utilizzo, della tecnologia blockchain. Quest'ultima unisce il controllo peer-to-peer alla crittografia, permettendo la verifica di ogni nodo di una rete, consentendo tracciabilità ed immodificabilità dei dati. Ciò rende, innegabilmente, più sicura l'attività di tracciamento e raccolta delle informazioni. Una struttura con tali caratteristiche rende, altresì, superflua l'opera di intermediari nella tenuta di registri, estromettendo i colossi dell'informatica e delle comunicazioni, e favorisce la trasparenza

[267] Soro A., id, p. 6: "Le Autorità europee di protezione dati avvertono il bisogno di accompagnare questi fenomeni attraverso un più rigoroso approccio etico e di generale responsabilità. E prima di tutto abbiamo bisogno di promuovere garanzie di trasparenza dei processi, anche per la progressiva difficoltà a mantenere un effettivo controllo sui dati: per l'opacità delle modalità di raccolta, dei luoghi di conservazione, dei criteri di selezione e di analisi".

[268] GDPR (General Data Protection Regulation), Regolamento 679/2016, art. 32.

giacché tutti gli interessati hanno accesso ai propri dati, con il diritto di cancellarli o renderli visibili solo a determinati utenti o gruppi di utenza.

Grandi passi avanti, nel conflittuale rapporto fra big data e privacy, sono stati fatti negli ultimi anni in Europa, proprio grazie al GDPR e all'interlocuzione dei legislatori e delle istituzioni nazionali governative con autorità indipendenti di settore, ed in particolare, in Italia, con il Garante per la protezione dei dati personali. Nei Paesi industrializzati e nelle democrazie occidentali le problematiche inerenti la privacy sono al centro di normative, regolamenti e convenzioni. Tuttavia è necessario rimarcare che ad oggi nel panorama mondiale, il 42% dei Paesi non ha una legislazione sulla protezione dei dati[269]. Alcune nazioni come il Venezuela, l'Egitto e la Libia non hanno in alcun modo imposto una regolamentazione, né tantomeno hanno iniziato alcun processo normativo o predisposto disegni di legge in tal senso.

3.2. Diritti costituzionalmente garantiti e tutela dei dati

3.2.1. Il diritto alla protezione dei dati personali

La tutela dei dati personali è un diritto fondamentale dell'individuo ai sensi della Dichiarazione Universale dei Diritti dell'Uomo e della Carta dei diritti fondamentali dell'Unione europea. Per la Dichiarazione Universale è riconosciuto il diritto, negativo, alla riservatezza, consistente nell'obbligo di astensione da parte di chiunque dall'interferire in modo arbitrario nella vita privata della persona, nonché nel diritto a mantenere il controllo sulle proprie informazioni. L'art. 12 della Dichiarazione Universale stabilisce, infatti, che "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni". A ben vedere l'art. 12 della Dichiarazione dell'Assemblea dell'ONU del 1948, fa riferimento ad un più generale diritto alla privacy[270], a tutela della sfera intima del singolo, comprendente un insieme di diritti fra cui anche quello alla riservatezza delle informazioni personali. In maniera ancor più specifica l'art. 8 della Carta dei diritti fondamentali dell'Unione europea (protezione dei dati di carattere personale) statuisce che "Ogni persona ha diritto alla protezione dei dati di carattere personale che la

[269] I dati sono stati raccolti nel 2019 dal Global Cyberlaw Tracker, per l'elaborazione di una mappa pubblicata dall'UNCTAD (Conferenza delle Nazioni Unite per il Commercio e lo Sviluppo).
[270] Definito "the right to be let alone", per la prima volta da Warren S. e Brandeis L.D., *The Right to Privacy*, in *Harvard Law Review*, n. 5, 1890.

riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica".

La diffusione globale delle reti pubbliche e l'utilizzo massivo di Internet in ogni attività quotidiana, sia essa lavorativa che di svago, ha richiesto norme sempre più stringenti, precise e soprattutto al passo con i tempi, nell'ambito della tutela dei dati personali. Le normative nazionali dei Paesi membri dell'UE si sono, oggi, uniformate alle disposizioni previste dal Regolamento UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione. Il GDPR ha abrogato la, ormai inattuale, Direttiva 95/46/CE (regolamento generale sulla protezione dei dati), ponendosi quale principale fonte europea riguardante la protezione dei dati personali.

L'odierna regolamentazione prevede, innanzi tutto, che l'interessato ha il diritto di chiedere al titolare del trattamento, sia esso un soggetto pubblico che privato, se sia in corso un trattamento di dati personali che lo riguarda e, in tal caso, essere informato sulle finalità del trattamento, i destinatari dei dati, l'origine dei dati personali trattati, l'esistenza di un processo decisionale automatizzato, compresa la profilazione. Il titolare dei dati ha, poi, diritto alla rettifica degli stessi, alla cancellazione, alla limitazione del trattamento. Per quanto riguarda la richiesta di cancellazione, non vi è, tuttavia, alcuna modalità di accertamento o controllo da parte di autorità terze, che possa comprovare l'effettiva eliminazione delle informazioni riguardanti il titolare dai database. Una novità assoluta dell'attuale regolamentazione è il c.d. diritto alla portabilità dei dati personali, ossia il diritto di trasferirli ad un altro titolare, se il trattamento si basa sul consenso o su un contratto stipulato con l'interessato, da effettuarsi con mezzi automatizzati.

I princìpi su cui si basa il diritto alla tutela dei dati personali sono la liceità, correttezza e trasparenza del trattamento, limitazione della finalità e della conservazione, minimizzazione dei dati, accuratezza, esattezza, integrità e confidenzialità. Per ciò che riguarda la liceità e correttezza, bisogna rimarcare che i dati devono essere trattati in modo lecito e le modalità di raccolta e utilizzo devono essere corrette, mantenendo l'impegno assunto con l'interessato al momento della ricezione del consenso, secondo princìpi di lealtà. La trasparenza ha, invece, lo scopo di alimentare la fiducia dell'individuo nei confronti della società digitale, e consiste nel rendere

conoscibili e comprensibili le modalità di raccolta dei dati, favorendo accessibilità e informazione. La limitazione della finalità vincola la legittimità del trattamento, che può avvenire solo se i dati sono raccolti per scopi predeterminati, espliciti e legittimi. I dati devono, poi, essere conservati per il solo tempo necessario rispetto alle finalità stabilite (limitazione della conservazione), dopodiché devono essere cancellati o quanto meno resi anonimi senza più possibilità di risalire al titolare (anonimizzazione). Essi devono essere anche rilevanti e necessari rispetto alle finalità per le quali sono trattati (minimizzazione dei dati)[271]. I dati devono essere accuratamente raccolti, esatti, ma soprattutto aggiornati ed eventualmente corretti, su richiesta dell'interessato. Infine le informazioni personali devono essere trattate in maniera confidenziale secondo un principio di riservatezza, in modo sicuro e con precauzioni che le preservino da alterazioni o accessi non autorizzati[272].

3.2.2. La posizione dell'Europa sulla tutela dei dati

Non sussiste alcun dubbio circa l'insostituibilità dei big data e dell'intelligenza artificiale nella prevenzione di reati e nell'individuazione di aree e situazioni a rischio di conflitto di interessi, in particolare nel procurement pubblico. Si è rilevato, tuttavia, che l'utilizzo dei big data può avere un impatto notevole sui diritti della persona, specialmente in termini di tutela della privacy[273], in considerazione dell'odierna diffusione delle reti informatiche e di Internet. Sempre più numerose sono le associazioni internazionali ed i comitati scientifici che sollevano forti preoccupazioni etico-giuridiche sull'utilizzo crescente ed incontrollato dei big data allo scopo di prevenire i crimini ed in generale di raccogliere grandi quantità di informazioni e profilare le persone fisiche. Per tale motivo norme sovranazionali e nazionali, nonché autorità indipendenti si sono focalizzate sul rischio connesso all'uso massivo dei dati. Le istituzioni europee hanno sempre mostrato un particolare impegno ed interesse nella tutela della privacy, considerando la protezione dei dati un diritto fondamentale, favorendo un'armonizzazione delle tutele non solo degli Stati membri ma anche con gli Stati extra europei, e sostenendo la trasparenza ed il controllo in materia di dati

[271] L'art. 5, par. 1 lett. C) del GDPR prevede che i dati debbano essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

[272] L'art. 5, par. 1 lett. f) del GDPR stabilisce che i dati devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

[273] Nel saggio di F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale e uomo*, pp. 10 ss., condivisibile è la preoccupazione dell'autore con riguardo alla privacy e alle applicazioni fornite di intelligenza artificiale, ove si legge: "in considerazione della gran mole di dati che queste applicazioni (fornite, ad esempio, di sensori e telecamere avanzate) possono acquisire in relazione alla vita, anche privata, dei cittadini: dati che, peraltro, potrebbero essere manipolati abusivamente, sottratti, deformati, con grave pregiudizio per le persone cui essi si riferiscono".

personali. L'orientamento dell'Unione europea è, oggi, indirizzato verso una maggior libertà di circolazione dei dati, affiancata però da controlli più stringenti secondo il principio della sicurezza adeguata al rischio, al fine di infondere una maggior fiducia dei cittadini nei confronti della c.d. società digitale. Per ciò che riguarda specificamente la protezione dei dati personali nell'ambito delle attività di raccolta dati a fini di prevenzione, indagine ed accertamento dei reati, è proprio dalla normativa europea che derivano le principali disposizioni nazionali a tutela dei diritti della persona.

A livello europeo[274] già nel 1981 la Convenzione 108 del Consiglio d'Europa[275] ha redatto delle linee guida che prevedono una regolamentazione in materia di trattamento automatizzato di grandi quantità di dati gestite da algoritmi. Si tiene in considerazione l'impatto del trattamento di masse di dati, evitando che esso possa confliggere con i diritti umani, le libertà fondamentali e i valori etici e sociali delle comunità. La normativa mira a tutelare la persona da abusi relativi alla privacy, nonché il diritto alla vita privata in relazione all'elaborazione automatica dei dati, ed a regolamentare i flussi transnazionali di informazioni. La Convenzione limita il trattamento e la raccolta dei dati al rispetto dei principi di correttezza, liceità e finalità del trattamento, nonché qualità dei dati stessi. Su di essa si è basata la Direttiva 1995/46 sulla tutela dei dati personali adottata nell'ambito della Comunità europea e del Mercato unico. Nel maggio 2018 il Consiglio ha adottato un protocollo di modifica, la c.d. Convenzione 108+[276], teso a modernizzare il previgente testo per fornire un quadro giuridico più attuale ed incisivo in un mutato ambito tecnologico, nel quale le violazioni del diritto alla protezione dei dati sono diventate un pericolo maggiore e coinvolgente un numero di persone di gran lunga più ampio che nel passato. Nel Protocollo di modifica viene definito in maniera più specifica il principio di liceità del trattamento, con particolare riferimento ai requisiti relativi al consenso, e viene rafforzata la protezione delle categorie speciali di dati. Viene, inoltre, ampliata la categoria dei dati sensibili, rafforzata la responsabilità degli addetti al controllo dei dati, consolidati i poteri e l'indipendenza delle autorità preposte alla protezione dei dati e delle basi giuridiche necessarie per la cooperazione internazionale. La convenzione aggiornata prevede ulteriori garanzie per le persone fisiche alle quali si riferiscono i dati personali trattati, soprattutto in materia di trasparenza ed accesso ai dati.

[274] Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016, p. 62 ss.
[275] "Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", Strasburgo, 28 gennaio 1981.
[276] Trattato n. 223, "Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", Strasburgo, 10 ottobre 2018.

Sono stati introdotti, poi, nuovi diritti degli interessati. Fra quelli di maggior importanza ed attualità, è da rilevare il diritto di non essere sottoposti ad una decisione basata unicamente su un trattamento automatizzato che arrechi un pregiudizio alle persone, e di potersi opporre con un ricorso al trattamento, in caso di violazione dei diritti. La convenzione prevede la designazione ad una o più autorità indipendenti del compito di garantire il rispetto delle disposizioni, con potere di imporre sanzioni amministrative.

In sintonia con tale orientamento, la Direttiva europea 2016/680[277] e la Direttiva 2016/1148, in uno con il regolamento europeo in materia di protezione dei dati personali (General Data Protection Regulation) o GDPR[278], introducono un complesso di disposizioni a tutela dei diritti della persona e regolamentazione del trattamento dei dati. La direttiva e il regolamento pongono limiti alla raccolta e utilizzo dei dati personali, ma escludono dall'ambito di regolamentazione i dati anonimizzati, non soggetti alle protezioni previste per il trattamento dei dati personali, ossia (Considerando 26 GDPR) quelle "informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi e tali da impedire o da non consentire più l'identificazione dell'interessato". Il GDPR[279] non definisce, tuttavia, le specificità del dato anonimo e non prescrive alcun metodo per l'anonimizzazione lasciandone l'onere ai singoli responsabili del trattamento. Per l'art. 32 del regolamento il titolare del trattamento dei dati deve mettere in atto misure idonee a proteggere efficacemente i dati personali evitando rischi per i diritti e le libertà dell'interessato. Fattore di principale rilevanza, a tutela dei dati personali, è la pseudonimizzazione, ossia il trattamento dei dati che non permetta più la loro attribuzione "a un interessato specifico senza l'utilizzo di informazioni aggiuntive". Le informazioni pseudonimizzate devono essere "conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile"[280]. L'assenza di una chiara distinzione fra anonimizzazione e

[277] Direttiva europea 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 o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, Parlamento europeo e Consiglio, 27 aprile 2016, in *OJ L 119*, 4 maggio 2016.

[278] Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[279] Molto ampia è la letteratura descrittiva e critica avente ad oggetto il GDPR. A puro titolo esemplificativo si cita: AA.VV., Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, Giappichelli, 2019; Alongi A., Pompei F., *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Tab Edizioni, 2021; Fabiano N., *GDPR e privacy. Consapevolezza e opportunità*, goWare, 2020; Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.

[280] Art. 4 GDPR.

pseudonimizzazione ha, tuttavia, reso complessa l'applicazione di univoche regole, sottovalutando la possibile reidentificazione dei soggetti pseudonimizzati. Ad esempio la crittografia è un metodo di pseudonimizzazione ma non di anonimizzazione, poiché le informazioni in chiaro sono reversibili con la decrittazione, permettendo così la successiva reidentificazione della persona. È d'uopo, poi, aggiungere che sussiste un rischio residuo di reidentificazione anche con dati anonimizzati, poiché la combinazione di informazioni non considerate personali può permettere, grazie ai moderni algoritmi, l'identificazione di una specifica persona fisica. La reidentificazione rende, pertanto, inutile l'anonimizzazione dei dati, permettendo l'identificazione dell'interessato tramite tecniche c.d. di *data matching*, ossia confrontando elementi identificativi indiretti, quali la posizione geografica, un software utilizzato o un'opinione, con altri frammenti di informazioni che nel complesso (c.d. effetto mosaico) possono essere decisivi per il riconoscimento della persona fisica[281]. L'anonimizzazione non può, pertanto, considerarsi un processo definitivo poiché vi è un rischio reidentificazione da monitorare e gestire nel tempo. I processi di anonimizzazione devono, dunque, essere adattati, in un contesto di accettabilità del rischio, alla natura dei dati per consentire di mantenerne l'utilità, nonché alle finalità del trattamento, ma soprattutto al rispetto dei diritti e delle libertà della persona.

Con riguardo alla pseudonimizzazione e alla possibilità di identificazione e reidentificazione, la posizione della Corte di giustizia dell'U.E. è chiarita dalla sentenza Breyer, nella quale i giudici stabiliscono che gli indirizzi IP dinamici pur non rivelando direttamente l'identità della persona proprietaria del computer, possono essere un "mezzo che può essere ragionevolmente utilizzato per identificare la persona interessata"[282]. Di conseguenza non possono in alcun modo essere considerati dati anonimi. Il regolamento presenta, pertanto, profili di rischio per la tutela dei diritti individuali, poiché nonostante le suesposte limitazioni, una raccolta generalizzata di dati potrebbe sempre condurre all'utilizzo illegittimo e non consentito degli stessi, ovvero all'identificazione di persone fisiche che non abbiano prestato il consenso, con conseguenti ingiustificate ingerenze

[281] Cfr. Boccaccini P., *Anonimizzazione e pseudonimizzazione: potenzialità, rischi e punti di attenzione*, in *Cybersecurity 360*, novembre 2021. Numerosi sono stati i casi di reidentificazione conseguenti all'anonimizzazione. Fra i più famosi, il caso Netflix risalente al 2006 e quello della "New York City Taxi and Limousine Commission", che nel 2013 rese pubblico un elenco di corse, teoricamente anonimizzate ma che in concreto erano riconducibili al titolare della licenza.

[282] CGUE, C-582/14, Patrick Breyer c. Bundesrepublik Deutschland (2016).

nel diritto alla privacy e trattamento dei dati personali, o alla stigmatizzazione di determinati profili o categorie di persone.

Sulla base delle suesposte premesse si fondano le cautele dalla direttiva 2016/680 in materia di profilazione, ovvero di trattamento automatizzato di dati personali. Con riguardo alla legittimità del trattamento dei dati dei soggetti coinvolti nelle indagini informatiche l'art. 22 del Regolamento europeo sulla protezione dei dati personali, nonché l'art. 11 della Direttiva 2016/680/UE sulla protezione dei dati personali nell'attività di prevenzione, indagine, accertamento e perseguimento di reati, vietano le decisioni basate unicamente su trattamenti automatizzati e stabiliscono il diritto dell'interessato di ottenere l'intervento umano nel procedimento di formazione della volontà da parte del titolare del trattamento. Nello specifico, l'art. 22 comma 1 del GDPR stabilisce che "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Sono, pertanto, necessarie adeguate garanzie, fra cui il diritto di intervento da parte del titolare del trattamento, mentre è del tutto illegittima una profilazione da cui possa derivare una qualsivoglia "discriminazione di persone fisiche sulla base di categorie particolari di dati personali"[283].

Coerentemente con tale orientamento, il Parlamento Europeo ha, in più occasioni, palesato la consapevolezza che l'utilizzo dei big data analytics possa costituire un pericolo per i diritti individuali e un rischio di discriminazione nei confronti di gruppi composti da soggetti con caratteristiche comuni. Secondo il Parlamento Europeo, difatti "the risk of data being used for discriminatory or fraudulent purposes and the marginalisation of the role of humans in these processes, leading to flawed decision-making procedures that have a detrimental impact on the lives and opportunities of citizen"[284]. Le tutele previste da GDPR e Direttiva 2016/680 per contrastare tali rischi sono nette, precise e ben delineate. Per l'art. 10 della Direttiva "Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato

[283] Direttiva 2016/680, art. 11 par. 3 e Considerando 38.
[284] European Parliament, Report on fundamental rights implications of big data, cit., par. M.

solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato".

Le problematiche del trattamento automatizzato presentano le stesse criticità dell'utilizzo di algoritmi intelligenti nelle c.d. attività di *sentencing* da parte del giudice, sollevandosi in tal caso il tema dell'assenza di possibilità concrete di difesa da parte del condannato rispetto alla contestazione di una valutazione compiuta interamente da una macchina, senza alcun intervento di mediazione da parte dell'uomo. Una situazione, quest'ultima, che potrebbe a ben vedere verificarsi anche con riferimento all'utilizzo dei predetti sistemi di data analytics nell'ambito delle attività di compliance. Infatti, l'output prodotto dai software in parola non soltanto potrebbe basarsi su un trattamento di dati personali integralmente automatizzato e senza alcun intervento umano di c.d. mediazione valutativa del risultato dell'analisi, ma potrebbe determinare, con tutto ciò che ovviamente ne consegue, la scoperta di elementi fattuali indizianti a carico o l'assunzione di decisioni disciplinari su soggetti coinvolti nell'analisi informatica. Peraltro, la possibilità concreta che attraverso l'uso della big data analytics possano individuarsi elementi indizianti a carico di persone fisiche solleva l'ulteriore problematica della difficoltà del diritto di difesa nella fase investigativa, proprio per l'impossibilità da parte del difensore di poter analizzare i dataset senza una strumentazione idonea. Senza considerare, poi, come si anticipava, le difficoltà connesse alle limitate possibilità di contestare il risultato cui il sistema informatizzato sia pervenuto, stante la complessità di comprendere le modalità attraverso cui la macchina possa aver optato per una determinata soluzione valutativa. La Corte Europea dei Diritti dell'Uomo, nella sentenza S. and Marper vs. The United Kingdom ravvisa un'ingerenza ai sensi dell'art. 8 CEDU nella memorizzazione dei dati concernenti la vita privata di un individuo, con un alto rischio per la libertà individuale qualora soggetti "che non sono stati condannati per alcun reato e hanno diritto alla presunzione di innocenza, sono trattati allo stesso modo dei condannati". La Corte EDU giunge alla conclusione che la percezione che tutte le persone siano trattate come potenziali sospetti è dovuta principalmente alla conservazione dei loro dati a tempo indeterminato, al pari di coloro che hanno subìto condanne definitive[285].

[285] Corte EDU, S. and Marper v. the United Kingdom, ric. 30562/04 e 30566/04 (2008), par. 67 e par. 122.

La Convenzione Europea dei Diritti dell'Uomo, così come il GDPR, oltre a tutelare il diritto al rispetto della propria vita privata e familiare (art. 8 par. 1), legittima le limitazioni al diritto di privacy e protezione dei dati personali soltanto per esigenze di sicurezza pubblica. L'art. 8 par. 2 CEDU prevede l'illegittimità dell'ingerenza delle autorità pubbliche nel diritto alla privacy salvo che essa "sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Lo scrivente rileva che, seppur pienamente condivisibili, tali deroghe siano tuttavia così ampie e generiche da richiedere un'attenta valutazione relativamente al singolo caso concreto. Secondo lo stesso orientamento il GDPR autorizza gli Stati membri ad adottare misure limitative del diritto al trattamento e protezione dei dati personali soltanto "al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui"[286], il tutto nel rispetto, ex art. 23 GDPR, delle libertà fondamentali, sempre che sia una misura necessaria e proporzionata in una società democratica.

3.2.3. Tutela della privacy e conservazione del traffico telefonico e telematico

Le modalità e i tempi di conservazione del traffico telefonico e telematico sono, con la diffusione globale delle tecnologie ICT ed in particolare di Internet e della telefonia cellulare, divenuti un argomento centrale in materia di protezione dei dati personali. Con specifico riguardo ai tempi di conservazione dei dati, la c.d. data retention, è richiesto un costante bilanciamento fra contrapposte, ma parimenti importanti, esigenze di sicurezza e giustizia da un lato e di tutela della privacy dall'altro[287]. La normativa italiana del 2008[288] in attuazione di una direttiva europea del 2006[289] prevede il sequestro di dati presso il fornitore di servizi informatici: in tal modo vengono attribuiti oneri di conservazione e custodia di dati a soggetti privati terzi, che potrebbero peraltro

[286] GDPR art. 13.
[287] Formici G., *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Giappichelli Editore, 2021.
[288] Legge n. 109 del 2008 "di attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce", la quale ha novellato l'art. 132 Cod. privacy, proprio al fine di attuare la disciplina europea.
[289] D.lgs. n. 109 del 30 maggio 2008, in attuazione della Direttiva n. 2006/24/CE, c.d. Direttiva Frattini.

essere essi stessi coinvolti ovvero avere interessi nell'inchiesta. Le disposizioni della direttiva europea del 2006 sono state, in Italia, applicate estensivamente, suscitando critiche e dubbi circa una presunta, ma quanto mai concreta, violazione della sfera privata dell'individuo. Il traffico telefonico deve essere conservato per 24 mesi, quello telematico per 12 mesi, mentre le chiamate senza risposta 6 mesi. In particolare dal 2017 i dati relativi al traffico telefonico e telematico utili per indagini di specifici reati, esclusi i contenuti delle comunicazioni, devono essere conservati per 72 mesi, tempistiche eccessive anche secondo il parere della Corte di Giustizia UE[290] e del Garante per la protezione dei dati personali[291]. Ciò conferma il concreto ed attuale rischio di ingerenza nella sfera privata dell'individuo e violazione dei diritti inerenti alla privacy. Il GDPR si limita a chiarire che i dati "debbano essere conservati in una forma tale che permetta l'identificazione del soggetto interessato per un periodo di tempo che non superi quello che serve agli scopi per il quale essi sono stati raccolti e trattati, anche se l'interessato non richiede la loro cancellazione".

L'obiettivo originario della Direttiva 2006/24/CE era di armonizzare le disposizioni degli Stati membri concernenti gli obblighi dei fornitori di servizi di comunicazione "relativi alla conservazione di determinati dati da essi generati e trattati, allo scopo di garantirne la disponibilità ai fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale", cercando un difficile punto di equilibrio con la tutela della privacy, non prevedendo, peraltro, la conservazione del contenuto della comunicazione e delle informazioni consultate. Le maggiori problematiche sono sorte dalla necessità di conciliare l'interesse all'acquisizione di elementi utili per la prosecuzione delle indagini con la tutela dei dati personali, evitando perciò un'acquisizione indiscriminata di tutte le informazioni. Generalmente, nell'ordinamento italiano, non è ammissibile il sequestro per finalità esplorative[292], come strumento di ricerca della *notitia criminis*, in particolare nel caso di sequestro presso terzi, al fine di evitare intrusioni illegittime nella sfera personale del soggetto. La normativa

[290] Sentenza Digital Rights Ireland (cause riunite CGUE C-293/12 e C-594/12).

[291] Nel Provvedimento del 14 maggio 2020 [9442587] l'Ufficio del Garante mostrava il proprio disappunto nella scelta di conservare i dati per tempi così lunghi. Nel Convegno del 24 ottobre 2019 "Privacy digitale e protezione dei dati personali tra persona e mercato" il Garante A. Soro aveva affermato "diventa ancora più incomprensibile la decisione di aumentare fino a 6 anni la Data Retention, ignorando, non solo le sentenze della Corte di giustizia europea, ma anche il buon senso".

[292] La recente sentenza della Suprema Corte n. 13486 del 2021 ha ribadito il divieto di disposizione del sequestro in base alle sole finalità esplorative di un'ipotesi criminosa statuendo che "deve escludersi che la misura sia illegittima, perché sorretta da finalità meramente esplorative, solo ove si sia in presenza di una notizia di reato sufficientemente delineata e suscettibile di approfondimenti istruttori".

del 2008 prevede, comunque, il sequestro presso il fornitore di servizi informatici con conseguente dovere di conservazione dei dati.

La sentenza Digital Rights Ireland della Corte di giustizia dell'UE (CGUE C-293/12), in applicazione ai principi della Carta europea dei diritti fondamentali dell'UE riguardanti il contrasto all'eccessiva ingerenza nei diritti individuali della persona, invalida la direttiva 2006/24, che obbligava i *service provider* a conservare per lungo tempo i dati relativi agli utenti, e prevedeva altresì un accesso da parte delle autorità nazionali senza la previsione di limitazioni. La sentenza, infatti, afferma che i dati "idonei a fornire precise indicazioni sulla vita privata e sulle abitudini degli individui, costituiscono una ingerenza nella privacy dei soggetti, in contrasto con quanto previsto agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea". Essa pur riconoscendo l'utilità della conservazione dei dati di traffico prevista dalla Direttiva per permettere alle autorità di poter perseguire i reati e contrastare la criminalità, afferma tuttavia che tale obiettivo non possa giustificare una conservazione indiscriminata e con tempi eccessivi degli stessi[293]. La genericità che caratterizza le disposizioni della Direttiva medesima, (si pensi alla generica definizione di "gravi reati, quali definiti da ciascuno Stato" ex art. 1 della Direttiva) si pone in contrasto col principio di proporzionalità di cui all'art. 52 par. 1 della Carta dei diritti Fondamentali dell'Unione. La Corte ha rilevato poi la completa mancanza, nella Direttiva, di presupposti sia materiali che procedurali sulla base dei quali le autorità competenti possono ottenere l'accesso ai dati di traffico per farne uso in un momento successivo. Infine, la Direttiva, nello specificare all'art. 6 che la conservazione dei dati non avrebbe dovuto avere una durata inferiore a 6 mesi, non ha chiarito un limite massimo, oltre il quale i suddetti dati avrebbero dovuto essere cancellati da parte dei service provider, non stabilendo neanche che l'accesso ai dati debba essere subordinato ad un previo controllo da parte di un organo giudicante o un'autorità indipendente. Sono pertanto necessarie regole chiare e precise che impediscano accessi generalizzati e senza limiti di tempo e impongano garanzie sufficienti contro il rischio di abusi che limitino i diritti fondamentali della persona. In conclusione, la Corte, alla luce delle criticità esposte poc'anzi ed

[293] Secondo la Corte "anche se l'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine, un siffatto obiettivo di interesse generale, per quanto fondamentale esso sia, non vale di per sé solo a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta".

in ossequio ai principi stabiliti nella Carta dei diritti fondamentali dell'Unione ha ritenuto di dover invalidare la Direttiva 2006/24/CE.

Dello stesso tenore è la sentenza Tele2 Sverige AB c. Postoch telestyrelsen[294], nella quale la Corte di giustizia censura la normativa nazionale svedese di recepimento della Direttiva del 2006, che obbliga i provider a conservare in maniera generalizzata i dati degli abbonati. Secondo la Corte i Paesi membri sono legittimati ad emanare normative che consentano la conservazione a titolo preventivo, non generalizzata dei dati, ma soltanto qualora tale conservazione sia mirata alla lotta alla criminalità e per il solo tempo strettamente necessario[295], in modo da fornire "garanzie sufficienti tali da permettere di proteggere efficacemente i loro dati personali contro i rischi di abuso".

Nell'ordinamento italiano la Legge Europea del 2017, senza alcuna considerazione nei confronti delle decisioni della Corte di giustizia, prevede un periodo di conservazione dei dati di 72 mesi per un cospicuo numero di reati che non si riduce alle sole ipotesi di delitti tentati e consumati di terrorismo, ma che comprende anche i delitti contemplati all'art. 407 comma 2 lett. a) c.p.p.[296]. Il decreto legislativo n. 101/2018, di modifica dell'articolo 132 del Codice per la protezione dei dati personali conferma il periodo di conservazione dei dati telefonici e telematici in sei anni. La sentenza della Suprema Corte di Cassazione del 13 febbraio 2020, n. 5741, ha affermato che "non può ritenersi che la disciplina italiana di conservazione dei dati di traffico (c.d. data retention) sia in contrasto con le pronunce della Corte di giustizia datate 8 aprile 2014 e 21 dicembre 2016 poiché la suddetta normativa prevede la conservazione dei dati per un periodo limitato pari a 24 mesi, subordina la possibilità di acquisizione degli stessi soltanto per finalità di accertamento e repressione dei reati, prevede che l'utilizzazione degli stessi dati sia sottoposta al provvedimento di acquisizione emesso da parte del Pubblico Ministero e cioè di un organo giurisdizionale che

[294] CGUE, C-203/15, Tele2 Sverige AB c. Postoch telestyrelsen, 21/12/2016.
[295] Ibid., par. 108.
[296] All'art. 24 la Legge Europea sancisce che "per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta […] è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali". L'art. 407 comma 2 lettera a) comprende, oltre al reato di associazione mafiosa, anche altri delitti di alto allarme sociale, quali: devastazione, saccheggio e strage; guerra civile; omicidio; ipotesi aggravate dei delitti di rapina, estorsione e contrabbando; sequestro di persona a scopo di estorsione; associazione sovversiva o con finalità di terrorismo; banda armata; fabbricazione e detenzione di armi da guerra; spaccio di sostanze stupefacenti, limitatamente alle ipotesi aggravate; associazione per delinquere nei casi in cui è obbligatorio l'arresto in flagranza; reati sessuali, in particolare contro i minori.

procede nell'ambito di una attività di indagine preliminare. Ne deriva quindi che la legislazione italiana non prevede la facoltà delle autorità pubbliche di accesso indiscriminato ai dati sensibili bensì la limita ai soli casi di indagini per fatti di reato svolte entro un determinato arco temporale di 24 mesi (elevati a 72 solo per fatti di reato di particolare allarme sociale) e la subordina alla autorizzazione proveniente da un organo giurisdizionale. […] Va pertanto ribadita la legittimità della normativa nazionale di riferimento costituita dall'art. 132 Codice della privacy, poiché la deroga al diritto alla riservatezza delle comunicazioni è prevista per un periodo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati, è subordinato alla emissione di un provvedimento da parte di un'autorità giurisdizionale".

La Corte di giustizia dell'Unione europea, con sentenza del 2 marzo 2021 (causa C-746/18, H.K. c./ Prokuratuur), ha contestato l'argomento utilizzato dalla Cassazione. Ad avviso della Corte di giustizia, difatti, l'acquisibilità processuale dei dati di traffico va limitata ai soli procedimenti per gravi reati o gravi minacce per la sicurezza pubblica e subordinata all'autorizzazione di un'autorità terza rispetto all'autorità pubblica richiedente[297]. In piena sintonia con le osservazioni della Corte di giustizia, il Garante per la protezione dei dati personali ha inviato il 22 luglio 2021 una segnalazione al Parlamento e al Governo circa l'opportunità di una riforma della disciplina della conservazione dei dati di traffico telefonico e telematico a fini di giustizia, maggiormente rispettosa del diritto alla privacy. Nello specifico l'Autorità Garante ha auspicato una riforma della disciplina della data retention, tale da differenziare limiti e termini di conservazione dei dati di traffico telefonico e telematico in base alla particolare gravità del reato per cui si procede, e comunque entro termini massimi compatibili con il principio di proporzionalità[298], come stabilito dalla Corte di giustizia dell'Unione europea. Secondo il Garante, infine, l'acquisizione dei dati di traffico telefonico e telematico dovrebbe essere subordinata all'autorizzazione di un organo giudicante, ossia il GIP, ferma restando, nei casi di urgenza, la possibilità per il pubblico ministero di provvedere con proprio decreto, che comunque deve essere soggetto a convalida.

[297] Per la Corte "L'accesso, per fini penali, ad un insieme di dati di comunicazioni elettroniche relativi al traffico o all'ubicazione, che permettano di trarre precise conclusioni sulla vita privata, è autorizzato soltanto allo scopo di lottare contro gravi forme di criminalità o di prevenire gravi minacce alla sicurezza pubblica", e tale autorizzazione deve essere subordinata ad un'autorità che "da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale".

[298] Secondo il Garante per la protezione dei dati personali è necessaria una nuova regolamentazione che preveda "condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in ragione della particolare gravità del reato per cui si proceda, comunque entro periodi massimi compatibili con il […] principio di proporzionalità".

Con decreto legge n. 132 del 30 settembre 2021[299] il Governo è intervenuto a disciplinare in materia di acquisizione di dati relativi al traffico telefonico e telematico per fini di indagine penale, decretando il coinvolgimento del giudice nel procedimento di acquisizione dei dati. Ove ricorrano ragioni di urgenza il pubblico ministero, difatti, dispone l'acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati[300]. Tuttavia il decreto legge in parola non ha ridotto i tempi di conservazione dei dati, corrispondenti a 72 mesi, confermando di fatto una violazione del principio di proporzionalità. La giustificazione addotta dalla sentenza della Cassazione del 2020, per cui l'elevazione a 72 mesi implica solo fatti riguardanti reati di particolare allarme sociale è facilmente confutabile, poiché i service provider non possono conoscere e distinguere a priori i dati che riguardano determinati reati, trovandosi di fatto a doverli conservare tutti indistintamente ed indiscriminatamente per il lasso di tempo, oggettivamente sproporzionato e lesivo di ogni diritto alla privacy, di sei anni.

3.2.4. La tutela dei dati personali in Italia

Nel nostro Paese la prima elaborazione del diritto alla privacy è di natura giurisprudenziale. Il caso giudiziario avente ad oggetto la protezione dei dati personali, risale agli anni cinquanta e riguarda il procedimento avviato dagli eredi del grande tenore Enrico Caruso, i quali chiedevano al giudice di bloccare la proiezione di un film sulla sua vita ritenuto lesivo della riservatezza del tenore napoletano. Nel 1953 il giudizio di primo grado affermava per la prima volta in Italia l'esistenza di un diritto alla riservatezza tutelabile tramite il diritto all'immagine, poiché non vi era ancora una disciplina specifica riguardante il divieto di ingerenze nella sfera della vita privata. Tuttavia la Suprema Corte[301] ribalta le precedenti decisioni delle corti di merito sostenendo che il semplice desiderio di riserbo non fosse, fino a quel momento, ritenuto un interesse tutelabile dal legislatore, o socialmente apprezzabile per i terzi. Secondo la Cassazione, difatti, "nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto

[299] Convertito in legge n. 178 del 23 novembre 2021.
[300] Lo schema per l'acquisizione dei dati è sovrapponibile a quello già previsto per l'intercettazione del flusso di comunicazioni telefoniche o relativo a sistemi informatici o telematici, come disciplinato dagli artt. 266, 266-bis e 267 c.p.p.
[301] Corte di Cassazione, sentenza n. 4487 del 1956.

assoluto all'intimità della vita privata e tanto meno come limite alla libertà dell'arte. Sono soltanto riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona. Gli artt. 96 e 97 della legge di autore riguardano esclusivamente il ritratto della persona e la riproduzione dell'immagine nella persona ritrattata, ma non offrono argomento per ravvisare in essi l'applicazione di un principio generale a tutela dei diritti della personalità e tanto meno di un preteso diritto all'intimità". Soltanto nel 1975 il Supremo Collegio italiano, in seguito alla controversia sorta per alcuni scatti effettuati alla principessa Soraya Esfandiari a sua insaputa nelle proprie mura domestiche, in atteggiamenti intimi con un uomo, riconosce per la prima volta l'esistenza di un diritto alla riservatezza.

Con la legge 675 del 1996, si ha la prima normativa in materia di tutela dei dati personali, conseguenza degli obblighi derivanti dal trattato di Schengen in materia di libertà di circolazione e per dare attuazione alla Direttiva 95/46/CE. Con la stessa legge si istituisce un'autorità di garanzia chiamata a sovraintendere l'applicazione della regolamentazione. Il Decreto legislativo n. 196 del 30 giugno 2003, Codice in materia di protezione dei dati personali, sostituisce la previgente normativa del 1996 riunendo in un unico corpo tutta la disciplina in materia di privacy. Esso prevede il diritto a non vedere trattati i propri dati personali in assenza di consenso, nonché l'adozione di cautele tecniche ed organizzative per procedere in maniera corretta al trattamento dei dati. Lo scopo del Testo Unico del 2003 è di evitare che il trattamento dei dati avvenga senza il consenso dell'avente diritto, o in modo da recare pregiudizio al suo diritto alla riservatezza. A tal fine il Titolo II riguarda i diritti degli interessati, ed in particolare gli articoli da 7 a 10 disciplinano il diritto di accesso, la modalità di raccolta e i requisiti dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali, mentre il Titolo III disciplina la cessazione del trattamento (art. 16) e le responsabilità e sanzioni in caso di danni (art. 15), nonché le regole ulteriori riguardanti i dati sensibili e giudiziari previste agli articoli 20-22. Oltre al diritto di accesso ai dati, conoscenza, modifica e aggiornamento, ed opposizione al trattamento, il codice prevede anche il diritto all'oblio[302], oggi regolato anche dall'art. 17 del GDPR.

[302] Definito dalla Suprema Corte (Cass. sent. n. 3679 del 1998) il "giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata".

Il Codice del 2003, ormai obsoleto per la diffusione di Internet, viene novellato con decreto legislativo n. 101 approvato l'8 agosto 2018[303], in modo da adeguare la normativa italiana al Regolamento europeo in materia di tutela dei dati personali del 2016 (GDPR). Fra le modifiche più rilevanti del decreto di adeguamento del 2018, i nuovi poteri conferiti all'Autorità garante, la previsione giuridica del danno di immagine, il consenso alla fornitura dei servizi delle società di informazione fissato ad un minimo di 14 anni, la semplificazione del trattamento dei dati sanitari, biometrici e genetici, prevedendo misure specifiche per una loro maggiore tutela, fissate periodicamente dal Garante, e l'estensione delle tutele previste dal GDPR anche al trattamento dei dati delle persone non più in vita. Il decreto legislativo n. 101 del 2018 amplia le tutele previste dal decreto legislativo n. 51 del 2018, con cui l'ordinamento italiano ha attuato la direttiva 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, completando il recepimento del c.d. pacchetto protezione dati dell'Unione europea.

La figura centrale di vigilanza e controllo in materia di trattamento dei dati è, senza dubbio alcuno, il Garante per la protezione dei dati personali che, con i decreti di attuazione del 2018, ha acquisito maggiori prerogative e poteri più ampi. Il GDPR ed il Regolamento UE 2018/1725, istituiscono la figura del garante europeo per la protezione dei dati (European Data Protection Supervisor). Tra i compiti principali del garante, previsti oggi anche dagli articoli 57 e 58 del GDPR, vi sono: il controllo sul rispetto delle normative europee e nazionali in materia di trattamento dei dati personali; la formulazione di pareri su proposte di atti normativi e amministrativi e le segnalazioni alle istituzioni dell'esigenza di innovazioni normative; l'esame dei reclami da parte di cittadini ed enti; le consulenze alle istituzioni riguardo alle normative vigenti in tema di privacy. Peculiarità essenziale del Garante europeo per la protezione dei dati e di quelli nazionali è l'indipendenza, così come previsto ex art. 55 Regolamento UE 2018/1725. Il Garante, difatti, deve poter agire "in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri[304] […] non subisce pressioni esterne, né dirette né indirette, e non sollecita né accetta

[303] Decreto legislativo n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679".
[304] Art. 55 par. 1, Regolamento UE 2018/1725.

istruzioni da alcuno[305]". Per tutta la durata del mandato, poi, egli si astiene da qualunque azione incompatibile con i suoi doveri e non può esercitare alcuna attività professionale.

La riforma sulla protezione dei dati personali che ha nel GDPR uno dei pilastri fondamentali, predispone un rafforzamento dei poteri delle autorità nazionali deputate a far rispettare le disposizioni europee, e responsabilità ben delineate e distinte. Al titolare del trattamento sono attribuite maggiori responsabilità rispetto al passato, per ciò che riguarda il rispetto e la tutela dei dati personali. Alle autorità di controllo, ed in particolare al Garante per la protezione dei dati personali, sono oggi attribuiti i poteri necessari per garantire il rispetto del Regolamento europeo e dei diritti delle persone fisiche. Nello specifico, il Regolamento inasprisce significativamente le sanzioni a carico di chi viola il dettato normativo europeo, portandole, a seconda della gravità della violazione, fino ad un massimo di € 20.000.000 o al 4% del fatturato mondiale annuo del gruppo riferito all'anno precedente. È previsto, inoltre, che gli Stati membri possano stabilire disposizioni relative a sanzioni penali in caso di violazioni del Regolamento. Si tende in tal modo ad incentivare una cooperazione di tutte le figure professionali aziendali con il titolare dei dati, affinché sia garantito il rispetto delle disposizioni del Regolamento e dei diritti e libertà riconosciuti all'interessato, alla luce dell'innovato contesto normativo.

Conformemente al Regolamento[306] è previsto, poi, l'obbligo in capo al titolare del trattamento di eseguire, al ricorrere di determinate condizioni, una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment), la c.d. DPIA. Essa è richiesta nei casi di valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato. Sulla suddetta valutazione si fondano decisioni che hanno effetti giuridici o incidono significativamente su di esse, trattamento su larga scala di dati sensibili o dati giudiziari, sorveglianza sistematica di zone accessibili al pubblico. La valutazione d'impatto sulla protezione dei dati personali risponde al principio di accountability, poiché permette al titolare del trattamento di adottare misure idonee a garantire il rispetto delle prescrizioni dettate dal Regolamento, nonché valutare la probabilità e la gravità dei rischi connessi a un'attività di trattamento per i diritti e le libertà degli interessati, individuando le misure tecniche e

[305] Art. 55 par. 2, Regolamento UE 2018/1725.

[306] Ai sensi dell'art. 35 del Regolamento europeo n. 679/2016, il titolare del trattamento ha l'onere di procedere ad una valutazione d'impatto sulla protezione dei dati personali "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

organizzative necessarie a garantire un livello di sicurezza adeguato al rischio identificato, assicurando così la protezione dei dati personali trattati. Essa ha una funzione preventiva, pertanto deve essere effettuata prima di procedere al trattamento. Il Regolamento riconosce, tuttavia, la possibilità per il titolare di svolgere una singola valutazione al fine di esaminare un insieme di trattamenti simili. Qualora dall'esito del processo di DPIA risultasse, nonostante le contromisure, un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrà consultare l'Autorità di controllo che provvederà a fornire un proprio parere nel merito. L'inosservanza delle disposizioni in materia di DPIA comporta cospicue sanzioni amministrative pecuniarie.

Di particolare rilevanza è l'obbligo in capo ai titolari ed ai responsabili del trattamento di tenere un registro delle attività riguardanti i dati personali svolte sotto la loro responsabilità, ove sono indicate le finalità del trattamento, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali, la descrizione generale delle misure di sicurezza tecniche ed organizzative adottate. I registri devono essere tenuti in forma scritta, anche in formato elettronico[307] e su richiesta, devono essere messi a disposizione dell'autorità di controllo.

3.2.5. Trasparenza delle informazioni

La trasparenza consiste nella pubblicità di informazioni sul trattamento dei dati allo scopo di favorire forme di controllo sul loro utilizzo, sulla provenienza e sulle modalità con le quali essi vengono raccolti. In particolare i dati personali necessitano di ampie tutele, nel rispetto del diritto alla privacy che negli ultimi anni ha acquisito sempre maggior importanza per la diffusione delle reti, della connessione condivisa e dei social network. Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile direttamente o anche indirettamente. Ogni persona soggetta a trattamento dei dati personali deve essere informata dei rischi, norme, e garanzie riguardanti il trattamento stesso, nonché dei diritti relativi e delle modalità di esercizio. Le finalità specifiche del trattamento dei dati devono, inoltre, essere chiare e legittime, precisate in maniera esplicita al momento della raccolta.

[307] Il registro viene generalmente redatto nella forma di fogli di calcolo Excel nei quali ad ogni riga corrisponde un'attività di trattamento e ad ogni colonna corrisponde una delle informazioni richieste a norma del Regolamento europeo.

Le recenti normative hanno imposto ed ottenuto dalla Pubblica Amministrazione un'ampia trasparenza degli atti, introducendo il concetto di accessibilità a tutte le informazioni allo scopo di promuovere forme diffuse di controllo sulla realizzazione delle funzioni istituzionali. Questa forma di trasparenza amministrativa ha presentato inevitabili punti di contrasto con il diritto alla tutela dei dati personali, richiedendo un bilanciamento fra contrapposti interessi. Al fine del riequilibrio di tali interessi, oltre a richiedere la non intelligibilità dei dati personali non pertinenti o non indispensabili[308], le norme a tutela del trattamento dei dati personali hanno imposto alle amministrazioni di prestare una particolare attenzione alle informazioni erogate in materia di consenso al trattamento[309].

Molti nodi restano, però, da sciogliere con riguardo alle informazioni raccolte da aziende private per la profilazione degli utenti. In questi casi le concrete difficoltà che gli organi preposti incontrano nel controllo della legittimità delle modalità di trattamento dei dati, non consentono il rispetto effettivo del principio di trasparenza. Di primaria importanza è l'obbligo in capo a chi raccoglie i dati di dare all'interessato tutte le informazioni relative al trattamento cui saranno soggetti i dati stessi[310]. A tal riguardo non si può non rilevare che nella pratica il consenso informato ha sempre rappresentato una sorta di formalità, per cui il titolare dei dati si trova a dover sottoscrivere informative di numerose pagine senza neanche riuscire a leggerle o comprenderle, per la loro lunghezza e complessità. Una soluzione a tale problematica, seppur non ancora diffusa, è costituita dalle informazioni stratificate (c.d. formati multistrato), ossia la divisione di un insieme di dati e del relativo consenso in diversi sottogruppi, più facilmente gestibili e consultabili dall'interessato, nel rispetto della normativa attuale che, basata sul GDPR del 2016, prevede informative chiare e di facile comprensione e leggibilità.

Le tutele del titolare dei dati e le stringenti regole riguardanti il loro trattamento sono alla base della fiducia di ogni individuo nei confronti della c.d. *data economy*. Solo tramite tale fiducia si

[308] In varie occasioni l'Autorità Garante ha richiesto la non ostensibilità di dati personali nelle graduatorie pubbliche, vietando la diffusione dei nominativi in grauatorie che di per sé possano contengano dati sensibili, come ad esempio quelle riguardanti persone invalide, o che hanno usufruito di esenzioni poiché in condizione economiche disagiate.
[309] Sul punto Cucumile P., *Il trattamento dei dati sensibili alla luce del principio di trasparenza, del C.A.D. e del GDPR. Il necessario bilanciamento degli interessi nel rapporto tra la normativa sulla trasparenza amministrativa e quella posta a tutela dei dati personali. Le modifiche normative e gli interventi dell'Autorità Garante*, in *Cammino Diritto* n. 11/2018.
[310] Più precisamente l'informativa è una comunicazione che ha lo scopo di informare ogni soggetto, anche prima che diventi interessato, sulle finalità e le modalità dei trattamenti, al fine di assicurare la trasparenza e correttezza di essi fin dalla fase di progettazione, e di essere in grado di comprovarli in qualunque momento venga richiesto.

potrà raggiungere una più corretta e libera circolazione delle informazioni. Un obiettivo essenziale del GDPR (art. 1) è infatti rendere più ampia e robusta la tutela dei dati personali non solo per attuare un diritto fondamentale previsto dalla Carta dei diritti dell'Unione europea (art. 8), ma anche per incentivare la libera circolazione dei dati personali. Tutela e libera circolazione dei dati potrebbero sembrare due obiettivi contrapposti, tuttavia possono coesistere, se non addirittura fondersi, se le informazioni vengono raccolte e trattate in un'ottica di trasparenza. L'ampliamento delle basi di legittimità dei trattamenti operato dall'art. 6 GDPR insieme alla responsabilizzazione del titolare del trattamento stesso consente, difatti, una libera circolazione dei dati rafforzando, altresì, i diritti degli interessati e della collettività nel suo complesso, grazie all'obbligo imposto dall'art. 24 al titolare delle informazioni di essere in grado di dimostrare in ogni momento la conformità del trattamento al GDPR[311].

Nel Regolamento 679/2016 il principio di trasparenza è inteso come obbligo di rendere conoscibili "le modalità con cui i dati sono raccolti, utilizzati e consultati grazie ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro"[312]. Per l'art. 5 paragrafo 1 lettera a) "i dati personali devono essere trattati in modo lecito, corretto e trasparente". Il GDPR, nel rispetto del principio di trasparenza, all'art. 12 stabilisce che le informazioni destinate al pubblico o all'interessato debbano essere facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. In particolare lo stesso articolo, al paragrafo 1, impone al titolare del trattamento l'adozione di misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice, specialmente nel caso di informazioni destinate prevalentemente ai minori. L'informativa deve, poi, essere resa per iscritto o con altri mezzi che siano comunque idonei a comprovarne l'esistenza, come ad esempio la posta elettronica, e a consentire alle autorità di vigilanza di verificarne completezza e correttezza[313]. Può essere fornita in forma orale solo se richiesto dall'interessato e nel rispetto delle garanzie previste dall'art. 12 GDPR.

[311] GDPR, art. 24 par. 1: "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento".
[312] Regolamento 679/2016, Considerando 39.
[313] Art. 12 paragrafo 1 GDPR e Considerando 58.

Le ulteriori informazioni che il titolare dovrà fornire all'interessato per garantire un trattamento equo e trasparente riguardano:

a. il periodo di conservazione dei dati personali oppure i criteri utilizzati per determinare tale periodo;
b. il diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la revoca del consenso in qualsiasi momento;
c. il diritto di proporre reclamo ad un'autorità di controllo;
d. l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Il GDPR prevede, poi, nell'ottica della trasparenza, l'istituzione di meccanismi di certificazione che consentano agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi. Le persone fisiche devono, difatti, essere "sensibilizzate ai rischi" che i trattamenti dei dati possono comportare. Come specifica il Considerando 39 del Regolamento, è opportuno che, sulla base del principio di trasparenza, il titolare sia in qualunque momento in grado di informare l'interessato anche rispetto al livello di rischio che i trattamenti presentano.

3.2.6. Protezione e conservazione dei dati personali

Il concetto di protezione dei dati personali attiene alla loro integrità ed alla capacità di chi ne detiene il trattamento di garantirne la sicurezza e la segretezza da attacchi esterni finalizzati ad appropriazioni o manipolazioni non autorizzate. Conformemente a questo principio il responsabile del trattamento deve adottare tutte le misure tecniche ed organizzative per proteggere i dati fin dalle prime fasi, ossia dalla loro raccolta, per tutto il periodo di conservazione degli stessi, ovvero fino alla loro cancellazione o anonimizzazione. Per l'art. 5 par. 1 lett. f) del GDPR il trattamento deve, difatti, avvenire in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, secondo un principio di integrità e riservatezza degli stessi. Sicurezza e riservatezza richiedono misure che impediscano l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento[314]. L'art. 32 par. 1 GDPR esplicita in maniera ancor più specifica la necessità da parte del titolare del trattamento di proteggere i dati personali,

[314] Cfr. GDPR Considerando 39, ultimo periodo.

statuendo che "il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Le contromisure ritenute più efficaci, ma non obbligatorie, ai fini della sicurezza delle informazioni sono, secondo il GDPR, sia la pseudonimizzazione che la cifratura, ossia la crittografia[315]. Per pseudonimizzazione si intende il trattamento dei dati personali in maniera tale che questi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Essa si concretizza in una destrutturazione dei dati, che opera attraverso l'uso di codici e pseudonimi, ed è generalmente interamente automatizzata. Nel testo del Regolamento, l'idea di pseudonimizzazione viene affiancata alle nozioni di "*privacy by design*" e di "*privacy by default*", ossia ad un sistema di protezione dei dati fin dalla progettazione e per impostazione predefinita[316]. La cifratura, o crittografia, è un sistema più performante della pseudonimizzazione in termini di protezione e sicurezza dei dati, poiché impedisce la leggibilità in chiaro di tutte le informazioni a chi non abbia il sistema di cifratura e la chiave per decifrare il dato stesso. La segretezza della chiave rappresenta il sigillo di sicurezza di ogni sistema crittografico[317]. Le moderne tecnologie hardware e software hanno reso enormemente complessa la decrittazione di dati cifrati da parte di soggetti non autorizzati, soprattutto se protetti con chiave asimmetrica. La crittografia con chiave asimmetrica è molto più sicura di quella simmetrica, ed è particolarmente indicata per i dati cifrati che viaggiano sulla rete poiché non richiede lo scambio

[315] A differenza del Codice della Privacy il GDPR non prevede un elenco tassativo e specifico di misure minime riguardo la sicurezza delle informazioni, ma considera la cifratura dei dati e degli archivi e la pseudonimizzazione delle informazioni come tecniche ideali per aumentare la protezione dei dati, soprattutto di quelli sensibili.

[316] Per l'art. 25 GDPR "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".

[317] Stallings W., *Crittografia*, De Paola A., Lo Re G. (a cura di), Mylab ediz., 2022; Sgarro A., *Crittografia. Tecniche di protezione dei dati riservati*, Muzzio Editore.

fisico della chiave privata, necessaria alla decrittazione, che a differenza di quella pubblica deve essere mantenuta segreta. Gli algoritmi asimmetrici sono, difatti, studiati in modo tale che la conoscenza della sola chiave pubblica e dell'algoritmo stesso non siano sufficienti per risalire alla chiave privata. La coppia di chiavi pubblica/privata viene generata attraverso un algoritmo a partire da sequenze *random*. Il livello di sicurezza della crittografia con chiave asimmetrica è oggi considerato fra i più alti, tanto che sia la posta elettronica certificata che la firma digitale si avvalgono di tale tecnologia. Altro importante vantaggio della crittografia è l'integrità dei dati, poiché li protegge da modifiche, cancellazioni ed alterazioni non autorizzate[318].

In caso di violazione dei dati personali, poi, l'art. 34 prevede un diritto dell'interessato di immediata comunicazione: "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo". Non è, tuttavia, richiesta la comunicazione nel caso in cui il titolare del trattamento abbia "messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura".

In conformità a quanto previsto dall'art. 12 del GDPR il titolare che riceva una richiesta dall'interessato deve fornire informazioni senza ingiustificato ritardo, e comunque non più tardi di un mese dal ricevimento della richiesta stessa. Tale arco temporale può essere prorogato fino a due mesi. Qualora il titolare non possa ottemperare alla richiesta dell'interessato deve dargliene comunicazione, spiegando i motivi della impossibilità di dar seguito alla sua richiesta e informando l'interessato della possibilità di proporre un reclamo all'autorità di controllo. Le suddette richieste sono gratuite, ed il titolare potrà legittimamente rifiutarsi di soddisfarle nella sola ipotesi in cui esse siano palesemente infondate. Qualora il titolare, senza giustificato motivo, non dia seguito all'esercizio del diritto dell'interessato, effettuerà una violazione che prevede sanzioni pecuniarie.

Alla protezione è strettamente connesso il concetto di conservazione. Riguardo tale aspetto, il GDPR stabilisce che, al fine di garantire un trattamento corretto e trasparente i dati sono conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi

[318] Cfr. Ziccardi G., *Crittografia e pseudonimizzazione nel GDPR*, ipsoa.it, 17 marzo 2018.

sono stati raccolti o successivamente trattati, conformemente a quanto previsto dagli obblighi di legge (art. 13 Regolamento 679/2016). L'art. 5 del GDPR al par. 1 prevede l'obbligo di assicurare un periodo di conservazione dei dati personali limitato al minimo necessario. Con riguardo alle sanzioni in caso di mancato adeguamento al GDPR in materia di conservazione dei dati, l'organo generalmente deputato ad irrogarle è il Garante della Privacy. Contro tali sanzioni amministrative è sempre possibile ricorrere all'autorità giudiziaria. Oltre alla tutela inibitoria e ripristinatoria, le sanzioni comminate sono di ordine economico e possono raggiungere cifre rilevanti. In una recente ordinanza del Garante per la Protezione dei Dati Personali emessa per la violazione delle regole sulla conservazione dei dati previste dal GDPR, all'azienda Foodinho s.r.l. è stata applicata una sanzione amministrativa pecuniaria di due milioni e seicentomila euro[319], per aver conservato la documentazione sui dati personali dei dipendenti (nello specifico i c.d. riders) per tempi prolungati, anche dopo la cessazione del rapporto di lavoro.

3.2.7. Tutela della privacy e open data

Nell'epoca attuale della c.d. *digital economy* le esigenze della persona sono profondamente mutate rispetto al passato, poiché la diffusione globale delle reti pubbliche ha reso sempre più necessario un bilanciamento fra la libera circolazione delle informazioni e la tutela dei dati personali. In ambito pubblico l'utilizzo dei big data analytics è strettamente legato agli open data, dati raccolti dalla pubblica amministrazione, messi a disposizione dei cittadini e liberamente utilizzabili e riutilizzabili come bene comune in un'ottica di trasparenza e partecipazione alla cosa pubblica. È necessario, da un punto di osservazione di libera condivisione responsabile e controllata dei documenti, bilanciare l'accesso, la disponibilità e il riutilizzo dei dati senza restrizioni, con il diritto alla privacy di ogni individuo, creando un equilibrio nel difficile rapporto tra diritto alla riservatezza e diritto alla trasparenza degli *open government data*. Con riguardo ai dati in formato aperto messi a disposizione dalla pubblica amministrazione, il Garante è intervenuto già nel 2015 con un provvedimento[320] avente ad oggetto le misure di sicurezza nello scambio dei dati personali tra amministrazioni. Il predetto documento del Garante della privacy oltre a ribadire l'obbligo per le amministrazioni di comunicare al Garante stesso "tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali

[319] Ordinanza ingiunzione nei confronti di Foodinho s.r.l. del 10 giugno 2021, Registro dei provvedimenti n. 234, Garante per la Protezione dei Dati Personali.

[320] Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche, Garante per la protezione dati personali, 2 luglio 2015, documento web n. 4129029.

contenuti nelle proprie banche dati"[321], prescrive alle pubbliche amministrazioni l´adozione delle misure necessarie per mettere a disposizione gli accessi alle proprie banche dati alle altre amministrazioni, nell'ambito della cooperazione applicativa di cui all´articolo 72, comma 1, lettera e) del Codice dell'Amministrazione Digitale[322].

In ambito europeo l'European Interoperability Framework ha fornito importanti istruzioni in ordine all'impostazione dei servizi pubblici digitali, finalizzate a migliorare le practices in materia di open data. In Italia Il CAD (Codice dell'Amministrazione Digitale) riprende il concetto di formato aperto, di accessibilità attraverso le tecnologie dell'informazione e della comunicazione, di reti telematiche in formati aperti adatti all'utilizzo automatico da parte di programmi per elaboratori. Gli open data devono essere aperti dalle pubbliche amministrazioni in formati tali da assicurare a tutti la fruizione, l'utilizzo e il riutilizzo, tanto più se si considera che i dati aperti possono essere impiegati per lo sviluppo di servizi di pubblica utilità che facilitano il godimento dei diritti fondamentali, nel rispetto dell'uguaglianza giuridica, che deve essere garantita anche in rete. Il principio di uguaglianza si traduce anche e soprattutto, nel diritto dei cittadini di controllare e gestire i propri dati personali. Risulta di tutta evidenza, pertanto, l'orientamento del legislatore a favore dei dati aperti al fine di razionalizzare il processo di valorizzazione del patrimonio informativo pubblico nazionale, preservando tuttavia la fiducia del cittadino nella e-government con un apparato di tutele volto al trattamento dei dati personali[323].

Definiti gli indubbi vantaggi di una pubblica amministrazione aperta, la stessa è, difatti, tenuta a garantire il riconoscimento dei diritti fondamentali e della privacy al cittadino. L'attuale disposto normativo in materia di trasparenza (d.lgs. 97/2016), con l'introduzione dell'accesso civico generalizzato, espone a probabili rischi di tensione tra diritto alla privacy e trasparenza. Gli stessi obblighi di trasparenza della Pubblica Amministrazione in riferimento ai propri dipendenti creano rilevanti problematiche di non agevole soluzione, riguardo la tutela dei dati personali degli stessi. A tale riguardo si è espressa la Corte costituzionale con sentenza n. 20 del 23 gennaio 2019. Il caso riguarda una pretesa violazione della normativa europea sulla privacy concernente l'obbligo a carico dell'amministrazione di pubblicare la documentazione attestante i compensi ricevuti dai

[321] Provvedimento del Garante della privacy del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche", par. 1.
[322] Id, par. 2.
[323] De Robbio A., *Dati aperti nella pubblica amministrazione tra crescita e trasparenza*, in *DigitaliaWeb, Rivista del digitale nei beni culturali*, 2013, p.38 ss.

dirigenti pubblici per l'espletamento dei loro incarichi nonché le dichiarazioni relative ai dati reddituali e patrimoniali degli stessi e dei loro congiunti. La Corte ha applicato il principio di proporzionalità per bilanciare, in tema di obblighi di pubblicazione, le contrapposte esigenze di trasparenza e riservatezza. Il giudice delle leggi, con la sentenza indicata, ha dichiarato l'illegittimità costituzionale dell'art. 14, comma 1-bis, lett. f) del d.lgs. n. 33 del 2013 nella parte in cui tale disposizione obbligava le pubbliche amministrazioni a pubblicare on line i dati personali sul reddito e sul patrimonio dei dirigenti pubblici diversi da quelli che ricoprono incarichi apicali[324].

Profili di incompatibilità possono sorgere, altresì, fra il già citato d.lgs. n. 33 del 2013 ed il Regolamento UE 2016/679. Il c.d. decreto Trasparenza del 2013 prevede che tutte le informazioni oggetto degli obblighi della trasparenza debbano essere pubblicate in formato aperto e siano riutilizzabili da chiunque, anche per scopi diversi da quelli per i quali esse sono state originariamente raccolte. Al riguardo è intervenuto il Garante per la protezione dei dati personali chiarendo che nel processo di apertura del patrimonio informativo pubblico non debba, tuttavia, essere pregiudicata la tutela della riservatezza, nel rispetto del principio di finalità[325]. Ciò sta a significare che la trasparenza non deve costituire un fine a sé, ma è necessaria una valutazione di bilanciamento degli interessi fra obiettivi dei soggetti pubblici e tutela della riservatezza[326]. Tale bilanciamento è, peraltro, un punto centrale anche nel GDPR, ove il Considerando 4 stabilisce che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità". Come non può sussistere un diritto assoluto ed incontrollato alla trasparenza che preveda la pubblicazione indiscriminata di informazioni private

[324] La Corte Costituzionale, con sentenza 23 gennaio - 21 febbraio 2019 n. 20 ha dichiarato "l'illegittimità costituzionale dell'art. 14, comma 1-bis, del decreto legislativo 14 marzo 2013, n. 33 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni), nella parte in cui prevede che le pubbliche amministrazioni pubblicano i dati di cui all'art. 14, comma 1, lettera f), dello stesso decreto legislativo anche per tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione, anziché solo per i titolari degli incarichi dirigenziali previsti dall'art. 19, commi 3 e 4, del decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche)".

[325] Cfr. Parere del Garante per la protezione dei dati personali n. 239 del 23 aprile 2015, doc. web n. 3959470, Provvedimento n. 92 del 3 marzo 2016, doc. web n. 4772830. Nello specifico il Garante afferma che "una P.A. può effettuare un trattamento di dati personali ulteriore – come la comunicazione di dati personali a terzi a seguito di una richiesta di «accesso civico» – solo se la finalità dell'ulteriore trattamento è compatibile con gli scopi originari del trattamento stesso".

[326] Orientamento seguito in più occasioni anche la Corte di Giustizia europea Corte di giustizia. Cfr. cause riunite C-203/15 e C-698/15, Tele2 Sverige AB c. Post-och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a., sentenza del 21 dicembre 2016.

senza alcun fine, allo stesso modo la tutela dei dati personali non può essere utilizzata dalla Pubblica Amministrazione allo scopo di ostacolare l'accesso alle informazioni, quale mera forma dell'esercizio della propria autorità. Solo un bilanciamento effettuato tramite organismi indipendenti di controllo, quali il Garante della privacy, può preservare il rapporto fra trasparenza della P.A. e tutela dei dati, da effetti distorsivi ed utilizzi strumentali dei relativi diritti[327].

Elemento essenziale del rapporto fra big data ed open data è l'integrazione delle informazioni fra le amministrazioni pubbliche. L'Agenzia per l'Italia Digitale nel 2017 ha presentato il progetto Data e Analytics Framework, volto alla semplificazione, interoperabilità e scambio dei dati pubblici tra amministrazioni per ampliare i benefici offerti da moderne piattaforme che siano in grado di valorizzare le informazioni, ottimizzandone lo scambio in ottica data driven, consentendo l'offerta di servizi più moderni a cittadini e imprese, e valorizzando il proprio ruolo nella transizione digitale nel rispetto della tutela dei dati personali. In un rinnovato quadro di interoperabilità nello scambio dei dati fra le amministrazioni emerge la nuova figura del *data scientist*, con il compito di contribuire a trasformare i dati in informazioni rilevanti nell'attività di erogazione dei servizi offerti dalle pubbliche amministrazioni. Tale figura professionale ha, oggi, acquisito particolare rilevanza proprio perché nell'organizzazione dei dati e durante il processo di analisi e strutturazione delle informazioni, ha il delicato compito di assicurare che il trattamento in corso non leda il diritto alla privacy tutelato dal GDPR[328].

3.2.8. Piattaforma di accesso alle banche dati della P.A. e rispetto della privacy

Le logiche di semplificazione e modernizzazione digitale della Pubblica Amministrazione hanno, fino a qualche anno fa, sacrificato alcuni diritti e valori dei cittadini del nostro Paese, quali il diritto alla privacy, e nello specifico il diritto alla tutela dei dati personali. Soltanto con l'attuazione del GDPR si è avuta un'inversione di tendenza. Grazie al ruolo attivo dell'ufficio del Garante per la protezione dei dati personali, poi, è ormai opinione comune che la privacy non sia un ostacolo alla semplificazione, ma un valore aggiunto[329]. Tale rinnovata visione ha condotto alla simbiosi fra

[327] Cfr. *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, Gazzetta Ufficiale n. 134 del 12 giugno 2014.

[328] Cfr. Loré F., *Il trattamento dei dati personali nella pubblica amministrazione tra Open data, Big Data e privacy*, in Ratio Iuris, 07/2019, p. 11 ss.

[329] In tal senso il Vice presidente dell'Autorità Garante per la protezione dei dati personali, Ginevra Cerrini Feroni, ha ribadito in un'intervista del 13 ottobre 2020 (intervistatore Di Paolo A., consultabile nelle pagine web del Garante per la privacy all'indirizzo: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9466550), che "La privacy è un valore, non un ostacolo alla semplificazione della PA e allo sviluppo della competitività", e più

semplificazione e privacy, con la progettazione di una piattaforma digitale di accesso telematico alle banche dati della Pubblica Amministrazione.

La predetta piattaforma, nel pieno rispetto del nuovo comma 2 bis dell'art. 60 del CAD[330], funge da centro di raccolta di tutti i dati delle amministrazioni, in un'ottica di semplificazione e sviluppo digitale, ma anche in ossequio di una nuova strategia pubblica di rispetto della tutela dei dati, tutti rigorosamente aggregati ed anonimizzati. I princìpi in materia di privacy sui quali la piattaforma è stata sviluppata riguardano la liceità dei trattamenti, nell'ambito dell'esecuzione di compiti di interesse pubblico e nel rispetto di tutte le garanzie previste dall'art. 6 par. 3 lett. b) del GDPR. Con specifico riguardo alla determinatezza, le finalità del trattamento devono essere predeterminate, mentre se i dati sono trattati per finalità diversa da quella per la quale sono stati originariamente raccolti (artt. 5, par.1, lett. b) e 6, par. 4), il principio di riferimento è quello della compatibilità. Altri punti fondamentali nella progettazione della piattaforma riguardano l'esattezza e minimizzazione, per cui il trattamento dei dati deve essere limitato a quanto necessario rispetto alle finalità per le quali sono trattati, evitando la duplicazione di archivi pubblici. L'integrità e la sicurezza dalla piattaforma sono rispettate tramite la previsione di adeguate misure di controllo e prevenzione riguardo possibili usi fraudolenti della stessa. Le misure vengono poste in essere anche rispetto alla fruibilità delle banche dati da parte di altre Pubbliche Amministrazioni, nell'ambito della c.d. cooperazione applicativa, nel pieno rispetto del CAD[331]. A tal fine vengono stabilite idonee policy di sicurezza dei sistemi informativi, che prevedano la presenza di una figura apicale a garanzia del rispetto dei presupposti per l'accesso, anche attraverso verifiche periodiche e aggiornamenti riguardanti misure tecniche di sicurezza, gestione delle utenze e profili di autorizzazione degli utenti. In caso di violazioni delle banche dati

specificamente "si rende necessario che le più condivisibili logiche di semplificazione e modernizzazione digitale del Paese si accompagnino all'effettivo rispetto dei limiti previsti dal regolatore nazionale ed europeo in materia di diritti fondamentali dell'individuo".

[330] L'art. 60 del CAD afferma al comma 2 "Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. Tali sistemi informativi possiedono le caratteristiche minime di sicurezza, accessibilità e interoperabilità e sono realizzati e aggiornati secondo le regole tecniche di cui all'articolo 71 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni". Per il nuovo comma 2 bis dell'art. 60 "Le pubbliche amministrazioni responsabili delle basi dati di interesse nazionale consentono il pieno utilizzo delle informazioni ai soggetti di cui all'articolo 2, comma 2, secondo standard e criteri di sicurezza e di gestione definiti nelle Linee guida".

[331] Il C.A.D. all'articolo 76 precisa che "Lo scambio di documenti informatici tra le pubbliche amministrazioni nell'ambito dell'SPC realizzati attraverso la cooperazione applicativa e nel rispetto delle relative regole tecniche di sicurezza, costituiscono invio documentale sufficiente per ciascun procedimento amministrativo ad ogni effetto di legge".

o incidenti informatici che possano avere un impatto significativo sui dati personali (c.d. *data breach*), questi devono essere comunicati dalle amministrazioni al Garante entro quarantotto ore. La mancata comunicazione al Garante dei c.d. data breach, nonché la mancata adozione delle misure necessarie[332], configurano un illecito amministrativo sanzionato ai sensi dell´art. 162, comma 2-ter del Codice della privacy[333].

Le modalità di accesso alle banche dati devono essere configurate offrendo un livello minimo di accesso ai dati, limitando i risultati delle richieste a valori di tipo booleano, mentre livelli di accesso gradualmente più ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore. Per ogni fruitore possono essere individuate più modalità di accesso ad una medesima banca dati in relazione alle diverse funzioni da lui svolte, modulando così il livello di accesso ai dati. Deve, infatti, essere prevista dalle amministrazioni la segmentazione dei dati visualizzabili al fine di rendere consultabili dall´utente, in base al profilo e funzione del fruitore, esclusivamente quelli necessari rispetto alle finalità in concreto perseguite. L'accesso può, così, essere consentito alle sole informazioni pertinenti e non eccedenti rispetto alla finalità perseguita. Gli accessi codificati alle banche dati devono consentire all'erogatore del servizio il tracciamento delle operazioni compiute sui dati personali e l'identificazione dei soggetti che le hanno effettuate, tramite un identificativo dell´utenza che ha posto in essere l'operazione, tuttavia le utenze codificate devono essere prive di elementi che rendano il fruitore direttamente identificabile. L'accesso a dati sensibili o giudiziari deve essere sempre codificato e i dati devono essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati al contesto, ai sensi dell´art. 22, comma 6, del Codice dell'Amministrazione Digitale. L'accesso alla banca dati in forma di web application sulla rete pubblica Internet, deve avvenire utilizzando protocolli di sicurezza tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014, emessi da una *Certification Authority* e riconosciuti dai browser e sistemi operativi. Di particolare rilevanza è, poi, la verifica di accessi anomali attraverso strumenti di *business intelligence* per monitorare ogni attività svolta sulla piattaforma tramite *report di log*, ovvero attraverso specifiche procedure di *audit*.

[332] Si consulti: *Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach)*, 30 luglio 2019, doc. n. 9126951.

[333] Art. 162 comma 2-ter Codice della privacy "In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro".

Dal 2020 è disponibile in Italia una piattaforma di accesso a banche dati e servizi della Pubblica Amministrazione direttamente da smartphone. La piattaforma, denominata "IO" è stata progettata, in un'ottica di semplificazione, per consentire un unico punto di accesso telematico[334] ai servizi, alle informazioni e alle comunicazioni della Pubblica Amministrazione. Ciò è stato possibile grazie all'integrazione con banche dati e piattaforme di ogni singola amministrazione, secondo un concetto di interoperabilità. Tramite delle open API (Application Programming Interface) programmate appositamente per la piattaforma, sono possibili l'invio di notifiche e messaggi ai cittadini da parte delle amministrazioni, transazioni economiche, invio, richiesta e ricezione di documenti da parte dell'utente. Con specifico riferimento alla tutela dei dati personali, l'app IO ha ricevuto un parere favorevole da parte dell'Autorità Garante, per ciò che riguarda le linee guida AgID disciplinanti l'accesso telematico ai servizi pubblici[335]. In considerazione delle indicazioni fornite dall'Ufficio del Garante sono difatti, state assicurate opportune garanzie a tutela della privacy, che hanno riguardato principalmente i ruoli assunti dai soggetti erogatori e le modalità di adesione al punto di accesso telematico. Particolare attenzione è stata posta alle misure e garanzie adottate per realizzare il punto di accesso, nel rispetto dei principi di privacy by design e privacy by default, con specifico riguardo al trattamento di dati relativi alla salute e dati personali relativi a condanne penali e reati, nonché alle modalità di integrazione del punto di accesso telematico con altre piattaforme digitali. Alcune criticità, che hanno richiesto il rinvio a successive interlocuzioni con AgID sono state riscontrate su determinati aspetti tecnici riguardanti l'utilizzo di sessioni di lunga durata dell'App IO e l'accesso ai servizi di altre amministrazioni con meccanismi di *federated identity*. Inoltre PagoPA ha effettuato per la nuova release dell'App IO innumerevoli misure tecniche a tutela della privacy degli utenti, evitando il trasferimento di informazioni sull'utente a società terze ove non necessario e disattivato alcune funzioni che consentivano di risalire all'ubicazione dell'utente attraverso il suo IP address. Sono state superate con riserva le perplessità del Garante, anche per ciò che riguarda

[334] L'art. 64 bis del nuovo CAD prevede un unico punto di accesso telematico per l'erogazione e la fruizione dei servizi delle Pubbliche Amministrazioni. La trasformazione digitale della P.A. rappresenta anche uno dei pilastri del d.l. n. 76 del 2020, il c.d. Decreto Semplificazioni, convertito in legge con modifiche l'11 settembre 2020. L'art. 24 del decreto interviene sull'art. 64 bis del CAD, identificando nell'app IO il punto unico di accesso telematico, in ottica mobile-first, ai servizi della PA.

[335] Garante per la protezione dei dati personali, "Parere all'AgID sullo schema di Linee guida per l'accesso telematico ai servizi della pubblica amministrazione, ai sensi dell'art. 64-bis del d.lgs. 82/2005", 1 novembre 2021, doc. n. 9714315.

il servizio di certificazione verde Covid-19, a condizione che i dati siano conservati per un periodo non superiore a dieci giorni dalla raccolta[336].

Nell'ambito del procurement pubblico, ad oggi non abbiamo in Italia una piattaforma unica di accesso alle gare ed alla relativa documentazione, tuttavia gli applicativi forniscono ai partecipanti sufficienti garanzie di semplicità di utilizzo, trasparenza e tutela dei dati personali. Oltre ad essere, le piattaforme, connotate da accessibilità e navigabilità, con la possibilità di accedere da qualunque dispositivo elettronico, l'orientamento attuale prevede nella maggioranza dei casi una distribuzione in Saas (*Software as a Service*), ossia senza necessità di installazioni e fruibile tramite i più comuni web browser. La modularità di ogni piattaforma, suddivisa in singoli moduli interdipendenti tra di loro, le conferisce una maggiore sicurezza da attacchi esterni e nei confronti di furti o perdite accidentali di dati. L'architettura multi livello[337] la rende, poi, maggiormente affidabile anche sul piano della navigabilità. La trasparenza, principio base nell'ambito dell'e-procurement, è garantita dalla tracciabilità dei dati e della documentazione, nonché dall'accesso in condizioni paritarie, da parte di tutti i partecipanti alla gara. L'intelligenza artificiale consente, infine, un approfondito controllo sui dati dei partecipanti alle gare d'appalto, fornendo alle amministrazioni c.d. red flag ed analisi rischi, utili per individuare conflitti di interessi e situazioni meritevoli di approfondimento, al fine di prevenire irregolarità nelle procedure.

3.3. La tutela dei dati nel procurement pubblico

3.3.1. Big data nel procurement pubblico e tutela dei dati personali

Secondo le stime del 2021 della Commissione europea, nell'UE viene spesa dalle autorità pubbliche per appalti di servizi e forniture, una cifra pari al 14 per cento del prodotto interno lordo dell'Unione[338]. Ciò a dimostrazione della rilevanza a livello continentale, in termini economici, acquisita dal procurement pubblico, nel cui ambito viene generata una vasta mole di dati relativi ai partecipanti alle gare ad evidenza pubblica, ed alle modalità e destinazioni di spesa delle Pubbliche Amministrazioni. Modelli avanzati di aggregazione ed interpretazione dei dati possono ingenerare una maggior efficienza dei processi di acquisto, nonché un incremento della

[336] Garante per la protezione dei dati personali, "Provvedimento recante garanzie per l'utilizzo dell'App IO per recuperare le certificazioni verdi Covid-19", 17 giugno 2021, doc. n. 9670670.
[337] Sul tema, Cabibbo L., *Architettura del software. Strutture e qualità*, Edizioni Efesto, febbraio 2021.
[338] Relazione del 28/10/2021 sulla revisione del regolamento finanziario in vista dell'entrata in vigore del quadro finanziario pluriennale 2021-2027.

trasparenza e della concorrenza nel mercato. L'utilizzo di strumenti evoluti di e-procurement, è uno dei principali driver delle politiche UE per l'innovazione ed è al centro delle strategie di trasformazione digitale della P.A., ivi compresi gli appalti pubblici. I sistemi di e-procurement sono oggi considerati delle leve strategiche per la crescita dell'economia dei Paesi, per la modernizzazione e per una maggiore efficienza dei processi amministrativi nell'ambito degli acquisti della P.A., tramite il controllo e la riduzione della spesa pubblica. L'estrazione di informazioni sul contesto in cui viene condotta un'analisi dati permette alle Pubbliche Amministrazioni di orientarsi verso un procurement strategico, con una tipologia di approvvigionamento che non si limita al solo impatto della spesa nel breve termine ma si concentra sul medio-lungo periodo, consentendo altresì l'introduzione dell'innovazione nel mercato. La digitalizzazione del procurement pubblico è uno strumento potente e di notevole rilevanza nelle strategie economiche dell'amministrazione, tuttavia per esprimere appieno le proprie potenzialità e la sua utilità deve essere integrata in ogni fase del processo di acquisizione, a partire già dalla programmazione delle gare di appalto.

Con tali finalità, il decreto ministeriale n. 148 del 12 agosto 2021[339], preannunciato dall'articolo 44 del Codice dei contratti pubblici (D.lgs. n. 50/2016), costituisce lo strumento attuativo per la definizione dei requisiti funzionali e tecnologici dei sistemi telematici del procurement pubblico e definisce le modalità di digitalizzazione delle procedure di affidamento, anche attraverso l'interconnessione per l'interoperabilità dei dati delle pubbliche amministrazioni[340]. Il provvedimento, composto da 29 articoli, individua i principi generali per la digitalizzazione dei processi di approvvigionamento delle pubbliche amministrazioni, in particolare delle fasi di acquisto e negoziazione, e indica le caratteristiche tecniche generali dei sistemi che ne costituiscono il supporto telematico. Le regole tecniche, comprensive della descrizione dei flussi,

[339] Decreto ministeriale 12 agosto 2021, n. 148 del Ministero per la pubblica amministrazione, di concerto con i Ministeri delle Infrastrutture e dell'Economia, pubblicato nella Gazzetta Ufficiale Serie generale n. 256 del 26 ottobre, "Regolamento recante modalità di digitalizzazione delle procedure dei contratti pubblici, da adottare ai sensi dell'articolo 44 del decreto legislativo 18 aprile 2016, n. 50".

[340] Per l'art. 44 del Codice dei contratti pubblici (Digitalizzazione delle procedure) "Entro un anno dalla data di entrata in vigore del presente codice, con decreto del Ministro per la semplificazione e la pubblica amministrazione, di concerto con il Ministro delle infrastrutture e dei trasporti (e il Ministro dell'economia e delle finanze), sentita l'Agenzia per l'Italia Digitale (AGID) nonché dell'Autorità garante della privacy per i profili di competenza, sono definite le modalità di digitalizzazione delle procedure di tutti i contratti pubblici, anche attraverso l'interconnessione per interoperabilità dei dati delle pubbliche amministrazioni. Sono, altresì, definite le migliori pratiche riguardanti metodologie organizzative e di lavoro, metodologie di programmazione e pianificazione, riferite anche all'individuazione dei dati rilevanti, alla loro raccolta, gestione ed elaborazione, soluzioni informatiche, telematiche e tecnologiche di supporto".

degli schemi dei dati e degli standard europei di interoperabilità tra i sistemi telematici, sono dettate dall'Agenzia per l'Italia digitale con apposite linee guida. Obiettivo del decreto è uniformare le procedure telematiche alle migliori pratiche nazionali ed europee. Particolare impegno viene dedicato all'ottimizzazione delle procedure telematiche ad evidenza pubblica, poiché gli appalti elettronici contribuiscono a migliorare l'efficienza amministrativa complessiva diminuendo i costi di gestione delle procedure di gara, riducendo la durata del ciclo dell'appalto e gli oneri amministrativi a carico delle imprese, facilitando e rendendo più efficaci i controlli, stimolando altresì la concorrenza, favorendo la partecipazione e l'informazione delle piccole e medie imprese.

In tale contesto si è diffuso, negli ultimi anni, l'utilizzo da parte delle amministrazioni dei big data analytics, non solo per quanto riguarda le scelte strategiche di mercato, ma anche per la possibilità che essi offrono di individuare potenziali episodi di conflitto di interessi e fattori di rischio riguardanti la corruzione negli appalti pubblici, con un potenziale risparmio di cifre rilevanti, corrispondenti a numerosi miliardi di euro. È, difatti, possibile realizzare una valutazione del rischio in tempo reale, sviluppando specifici segnali di allarme che si manifestano durante i processi di gara, le c.d. red flag riferite a situazioni a rischio collegate a potenziali episodi corruttivi o di conflitto di interessi nel procurement pubblico, ed integrare gli stessi nei sistemi nazionali di e-procurement. Lo sviluppo di tecniche basate sui big data per rilevare e prevenire in tempo reale comportamenti impropri negli appalti pubblici, avviene tramite l'analisi di un ingente volume di dati che permette di fare una valutazione del rischio approfondita. In questo contesto la prevenzione della corruzione e dei casi di conflitto di interesse viene facilitata da uno strumento che valuti, in modalità automatizzata ed in tempo reale, i rischi relativi agli appalti pubblici in un determinato territorio, amministrazione o comparto.

In ambito europeo una delle analisi più valide è stata effettuata con la piattaforma SceMaps[341], considerando ben diciassette segnali d'allarme di potenziali irregolarità. Una concentrazione di segnali in riferimento ad una particolare azienda, amministrazione, settore o Paese corrisponde ad un indice di comportamenti sospetti nei processi di appalto. La valutazione del rischio basata sull'analisi dei big data ha evidenziato un notevole squilibrio fra i Paesi membri, con enormi

[341] L'analisi è stata effettuata da SceMaps (State Capture Estimation and Monitoring of Anticorruption Policies at the Sectoral level) in tre settori in cui le autorità pubbliche sono i principali acquirenti e che sono considerati tra i più rischiosi in termini di possibili abusi e cattiva gestione della spesa pubblica: edilizia, commercio all'ingrosso di combustibili e commercio all'ingrosso di prodotti farmaceutici.

vulnerabilità a comportamenti sospetti in particolare negli appalti pubblici in Bulgaria e Romania. Uno dei segnali d'allarme è l'indice di concentrazione dell'acquirente, il c.d. *buyer concentration index*, comprovante che un fornitore ha ricevuto l'intero ammontare delle entrate da appalti pubblici da una sola amministrazione. Esso costituisce un indizio relativo alla possibile dipendenza di una società da un particolare ente pubblico[342]. Viene anche considerata come red flag la vittoria, da parte delle società, di gare d'appalto nello stesso anno della loro costituzione. Tale segnale rappresenta il rischio potenziale che persone giuridiche possano essere costituite appositamente per vincere una particolare gara d'appalto. Maggiore è la percentuale di società costituite nell'anno di aggiudicazione, più alto è il rischio che i processi di appalto siano influenzati da mezzi non competitivi e potenzialmente illeciti. Questi indicatori evidenziano segnali d'allarme con riferimento sia alle autorità pubbliche che alle aziende. Queste ultime potrebbero essere ulteriormente indagate sia attraverso le informazioni e i dati dei profili di ciascuna persona giuridica, sia attraverso l'analisi incrociata di ulteriori segnali d'allarme. Una valutazione del rischio basata su questi indicatori offre possibilità di valutazione finalizzata all'elaborazione di misure preventive alla segnalazione di irregolarità negli appalti pubblici, ed è rivolta ad istituzioni di vigilanza e anticorruzione, organismi di regolamentazione e controllo, autorità di contrasto, ma anche stampa e società civile. I profili tratti dall'incrocio dei dati possono facilitare le investigazioni fornendo informazioni dettagliate sulle attività di approvvigionamento, sulle aziende e sulle gare d'appalto. Un altro importante segnale d'allarme è il rapporto tra esposizione nell'appalto e numero di dipendenti, il *procurement exposure per employee ratio*, indicatore che rappresenta il valore medio degli appalti vinti da una determinata azienda in uno specifico periodo in rapporto al numero di dipendenti della stessa. Tale segnale d'allarme si manifesta quando aziende con un numero insufficiente di dipendenti vincono gare d'appalto che richiederebbero una forza lavoro maggiore, circostanza solitamente associata ad un uso illecito di subappaltatori. Anche un valore sproporzionato del rapporto tra fatturato e numero di dipendenti ("*revenue per employee ratio*") può essere un segnale di possibili comportamenti illeciti. Un altro segnale d'allarme è il rapporto fra esposizione in appalti pubblici e ricavi ("*procurement exposure to revenue ratio*"), ossia l'indicatore che calcola la quota di entrate derivanti da appalti pubblici rispetto al totale delle entrate di un'azienda. Ove la società dipenda dagli appalti pubblici, difatti, aumenta la probabilità

[342] In Bulgaria la quota di autorità pubbliche che concentrano oltre il 60% delle somme assegnate a un determinato fornitore è di gran lunga superiore agli altri Paesi, e si concentra anche il gruppo più numeroso di acquirenti che ha assegnato ad un solo fornitore più del 90% degli appalti.

di ricorrere a strumenti illeciti per aggiudicarsi le gare, ovvero alla sussistenza di un conflitto di interessi fra soggetti coinvolti nel processo di acquisizione. L'indicatore consente anche l'identificazione di aziende che non possono dimostrare la propria redditività senza il sostegno del denaro pubblico, raffigurando così un fattore di rischio circa l'emersione di conflitti di interesse fra soggetti facenti parte dell'amministrazione ed impresa appaltatrice[343].

La valutazione del rischio negli appalti pubblici basata sulle analisi dei big data si è, pertanto, mostrata uno strumento di particolare utilità nel contrasto al conflitto di interessi e alle attività illecite nel procurement. I big data analytics possono essere, difatti, utilizzati sia nelle analisi dei casi esistenti relativi a comportamenti sospetti, sia nella programmazione di misure preventive e di sistemi di controllo in tempo reale dei processi di gara. A tal fine è necessario l'intervento della società civile e dei mezzi di informazione, ma soprattutto delle autorità pubbliche di controllo e della magistratura. Nonostante la crescente rilevanza e l'utilizzo sempre più diffuso dei big data nel procurement pubblico per le suesposte ragioni, è tuttavia sempre necessario considerare quale presupposto fondamentale la tutela dei dati personali in ogni fase del loro trattamento, dalla raccolta all'elaborazione ed analisi, durante tutto il periodo di conservazione degli stessi fino alla loro cancellazione. Con riguardo ai dati delle aziende, quali ragione sociale, numero di dipendenti, fatturati, dislocazione dei mercati delle transazioni, non sorgono particolari problematiche relative alla tutela dei dati, soprattutto nei casi in cui l'analisi delle informazioni sia aggregata e non individuale, ossia si limiti a produrre una variabile numerica determinata da un conteggio inerente un gruppo di soggetti. Le analisi del rischio effettuate sui big data riguardanti le red flag basate sugli indicatori aziendali, come quelle della piattaforma SceMaps, non sollevano, difatti, problemi attinenti alla tutela dei dati, poiché si avvalgono di dati aziendali, nella maggior parte dei casi utilizzati in forma aggregata. Per rendere attendibili specifiche tipologie di analisi è, tuttavia, spesso necessario trattare ed elaborare informazioni personali, oggi protette dalle normative sulla privacy ed in particolare dal GDPR. Per quanto riguarda i dati nel procurement pubblico, bisogna considerare che il diritto alla privacy confligge, almeno in parte, con il dovere di pubblicità delle amministrazioni. In tali casi è necessario bilanciare il dovere di pubblicità degli atti con il diritto alla privacy dei soggetti. Già la direttiva 2003/98/CE affermava il principio, ancora

[343] Grazie a questo indicatore, in base ai dati raccolti da SceMaps, è stato possibile far emergere che le aziende in Romania e Bulgaria che hanno ottenuto oltre l'80% dei loro ricavi totale grazie ad appalti pubblici nel periodo 2010-2019 hanno ricevuto dalle amministrazioni 2,85 miliardi di euro, somma che rappresenta circa il 3% dell'importo totale dei contratti pubblici nei relativi settori economici.

valido, di disponibilità dei dati da parte delle amministrazioni, che devono rendere accessibili i propri documenti, ma la condivisione deve essere responsabile e controllata[344]. Spetterà alle autorità indipendenti preposte, in primis al Garante per la tutela dei dati personali, valutare di volta in volta a seconda nel caso concreto, se debba prevalere l'una o l'altro. Bisogna considerare che l'analisi computazionale dei big data nel procurement con l'ausilio dell'intelligenza artificiale, può creare un ostacolo all'attività di vigilanza da parte delle autorità di controllo, poiché i dati vengono processati dagli algoritmi in maniera del tutto automatizzata. Tuttavia il trattamento dei dati sensibili, compreso il trasferimento ad altre amministrazioni o l'accesso da parte di soggetti interessati dovrebbe avvenire sempre previo controllo umano, così come stabilito dal GDPR, e soprattutto conseguentemente ad un'informazione al titolare dei dati. Quest'ultimo deve sempre essere in grado di conoscere quali sono i dati in possesso dell'amministrazione, da chi vengono richiesti e a chi vengono inviati, per poter opporsi ad un determinato trattamento, appellandosi al Garante o tramite una procedura d'urgenza giudiziaria. Soltanto le suddette cautele, in combinato con il rispetto delle disposizioni previste dal GDPR, possono ristabilire un'effettiva tutela dei dati personali, senza possibilità di utilizzi illegittimi, sconsiderati, o comunque lesivi della privacy. Altro punto da considerare è quello dell'espansione, nei casi in cui sia possibile, di piattaforme dotate di funzionalità blockchain e peer-to-peer nell'invio, scambio ed organizzazione dei dati, in modo da essere sempre sotto il controllo e con la possibilità di cancellazione, da parte del titolare. L'utente dovrebbe sempre avere, difatti, il diritto di conoscere le modalità tecniche di trattamento dei propri dati e di accedere agli stessi, modificarli, cancellarli, limitarne la raccolta e la conservazione per il tempo necessario.

Nell'ambito delle procedure per l'approvvigionamento di beni e servizi delle amministrazioni pubbliche, il rispetto della privacy e la rispondenza a livelli adeguati di sicurezza, sono stati oggetto di un parere del Garante riguardante la sicurezza nel procurement, predisposto da AGID[345]. Il documento comprende delle linee guida e best practices da seguire in tutte le fasi del processo di acquisizione, ed è di particolare rilevanza poiché chiarisce aspetti non completamente definiti nell'ambito del procurement dalla normativa, fissando altresì criteri pratici concreti per facilitare l'applicazione del Regolamento europeo del 2016 (GDPR). In particolare il documento conferma

[344] Cfr. Lorè F., *Il trattamento dei dati personali nella pubblica amministrazione tra Open data, Big Data e privacy*, in *Ratio Iuris*, 07/2019, p. 14.
[345] Parere sullo schema di "Linee guida - La Sicurezza nel procurement ICT" predisposto da AgID – n. 16 del 30 gennaio 2020 [9283857].

che i fornitori di servizi informatici di cui si avvalgono le amministrazioni sono responsabili del trattamento dei dati e devono fornire "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato". Anche nell'ambito degli appalti pubblici la protezione dei dati deve avvenire fino dalla fase di progettazione per impostazione predefinita, in rispondenza all'art. 25 del Regolamento europeo. Il contratto che vincola il responsabile al titolare dei dati deve individuare l'ambito, durata, natura e finalità del trattamento, il tipo di dati, le categorie di interessati, gli obblighi ed i diritti del titolare del trattamento. Tutto ciò conferisce maggiore certezza, in particolare per ciò che riguarda la ripartizione delle responsabilità. A tal fine, nel rispetto del principio di accountability, devono essere puntualmente definiti i compiti del responsabile della protezione dei dati personali dell'amministrazione o del fornitore di servizi informatici, evitando esoneri di responsabilità soprattutto in caso di contratti standard. Devono, poi, in conformità all'art. 32 del Regolamento, essere adeguatamente e preventivamente individuate e garantite misure di sicurezza tecniche ed organizzative, specialmente con riguardo all'adozione di procedure informatiche per la gestione delle violazioni di dati personali, nonché ai rischi per i diritti e le libertà degli interessati che derivino dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati[346].

Nonostante le tutele del diritto alla privacy contenute nel GDPR, il c.d. Decreto Capienze del 2021[347] rischia di inficiare l'applicazione della normativa sulla protezione dei dati nei rapporti con le pubbliche amministrazioni[348] ed in particolare nel procurement pubblico. Nel decreto in parola

[346] Per l'articolo 32 commi 1 e 2 del Regolamento europeo "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

[347] D.l. n. 139 dell'8 ottobre 2021 convertito in legge n. 205 del 3 dicembre 2021.

[348] Per amministrazioni pubbliche si intendono quelle di cui all'art. 1, comma 2, del d.lgs. 30 marzo 2001, n. 165, a cui vanno aggiunte le Autorità indipendenti, le amministrazioni inserite nell'elenco annuale dall'Istituto nazionale di statistica (ISTAT) di cui all'articolo 1, comma 3, della L. 31 dicembre 2009, n. 196, e le società a controllo pubblico statale ai sensi dell'art. 16 del d. lgs. 19 agosto 2016, n. 175.

sono presenti, difatti, alcune disposizioni urgenti in materia di privacy e protezione dei dati personali. Le modifiche apportate riguardano la relazione fra il trattamento dei dati personali e le finalità di interesse pubblico. L'articolo 9, comma 1, lett. a) del d.l. n. 139/2021 aggiunge all'articolo 2-ter del Codice della Privacy, d.lgs. 196 del 2003, il nuovo comma 1-bis, ai sensi del quale il trattamento dei dati personali da parte di un'autorità pubblica "è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti". Inoltre, il decreto legge prevede che se la finalità del trattamento non è espressamente prevista da una norma di legge o regolamento, questa verrà decisa ed indicata dall'amministrazione "in coerenza al compito svolto o al potere esercitato". Nonostante ai sensi del Considerando 45 GDPR le finalità del trattamento di dati dovrebbero essere definite con atto legislativo, la nuova normativa permette alla Pubblica Amministrazione di determinare le finalità del trattamento, pur se non espressamente definite da norma di legge o regolamento. In sostanza, con un semplice atto amministrativo ogni ente pubblico può definire il motivo per cui sarà necessario trattare dati personali, consentendo la loro trasmissione tra enti pubblici anche se non formalmente prevista da una norma di legge, purché sia necessaria all'esecuzione del compito di interesse pubblico. Il Decreto agisce quindi come una sorta di nulla osta preventivo sull'attività della Pubblica Amministrazione, che potrà trattare e comunicare dati anche senza specifica norma di legge. Oltre ad essere caratterizzata dalla indeterminatezza, la norma potrebbe avere profili di incostituzionalità per violazione del GDPR, gerarchicamente superiore alle norme nazionali, il quale prevede che la finalità di trattamento venga definita con norma di legge. Unico limite previsto dall'art. 9, comma 1, lett. a) per la P.A. consiste nell'obbligo di un'adeguata pubblicità al titolare dei dati, con la comunicazione del trattamento che lo riguardi e fornendo ogni informazione necessaria per assicurarne la trasparenza.

Il decreto abolisce, poi, il potere di controllo preventivo ed intervento del Garante per la protezione dei dati personali per i trattamenti a rischio elevato. L'art. 9, comma 1, lettera b) del Decreto Capienze, difatti, abroga l'articolo 2-quinquiesdecies del Codice della Privacy, il quale stabiliva che "con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare". La novella del decreto n. 139 del 2021, di fatto, elimina l'imposizione alla P.A. di consultare il Garante prima di

porre in essere trattamenti ad alto rischio, nell'interesse pubblico. Il Garante non ha, difatti, più alcun potere di intervenire nei confronti dell'attività della Pubblica Amministrazione con provvedimenti di carattere generale per prescrivere misure obbligatorie a garanzia dei diritti dei cittadini nel caso di trattamenti a rischio elevato[349] svolti nello svolgimento di un interesse pubblico. Rimuovere il potere di intervento preventivo del Garante della privacy in un'epoca, come quella odierna, di transizione digitale della Pubblica Amministrazione, rischia di far perdere l'effetto deterrente dei suoi provvedimenti. La nuova normativa, difatti, non consente più di bloccare i trattamenti a rischio elevato, come ad esempio l'obbligo di valutazione d'impatto previsto all'art. 35 del Regolamento, consentendo alle amministrazioni di non rispettare la normativa europea. Tale disposizione appare, altresì, in contrasto con l'orientamento europeo di ampliamento dei poteri inibitori e sanzionatori delle autorità indipendenti nazionali e sovranazionali, quali il Garante della privacy.

L'orientamento del decreto legge verso una tutela più attenuata del diritto alla privacy viene confermato non solo dal comma 3 dell'art. 9, il quale stabilisce un termine perentorio molto breve, di soli trenta giorni, entro il quale l'Autorità Garante potrà pronunciarsi su riforme, misure e progetti del Piano Nazionale di Ripresa e Resilienza (PNRR), decorso il quale il Governo potrà procedere a prescindere dall'acquisizione del parere[350], ma altresì dall'abrogazione del comma 5 dell'art. 132 Codice della Privacy, ossia delle misure di garanzia per la conservazione dei dati di traffico telematici[351].

Le novelle del d.l. 139/2021 lasciano, in definitiva, poteri troppo ampi ad amministrazioni e società partecipate riguardo al trattamento dei dati personali, in palese violazione del GDPR, ove

[349] Il Garante, prima dell'entrata in vigore del decreto n. 139 del 2021, si è avvalso di tale potere previsto all'art. 36 GDPR, per bloccare alcuni trattamenti sui dati personali da parte dell'app dei servizi pubblici IO e il green pass.

[350] Appare evidente che la ratio di un termine così ridotto sia quella di rendere impossibile per il Garante pronunciarsi su riforme, misure e progetti del PNRR.

[351] L'art. 132 comma 5 del Codice della Privacy prevedeva che il trattamento e la conservazione di dati personali, compresi i tabulati telefonici, per le finalità di accertamento e repressione dei reati venisse effettuato nel rispetto delle misure e degli accorgimenti a garanzia delle persone, prescritti dal Garante della Privacy, secondo le modalità dell'art. 2 quinquiesdecies. L'abrogazione del comma 5 dell'art. 132 viola palesemente la sentenza della Corte di Giustizia dell'Unione Europea del 2 marzo 2021 (Causa C-746/18, H.K. c./ Prokuratuur) con cui si affermano i principi di proporzionalità e del bilanciamento tra sicurezza pubblica e diritti fondamentali nelle operazioni di conservazione e uso dei dati e metadati telefonici. Per la Corte, riunita in Grande Sezione, l'accesso, per fini penali, ad un insieme di dati di comunicazioni elettroniche relativi al traffico o all'ubicazione, che permettano di trarre precise conclusioni sulla vita privata, è autorizzato soltanto allo scopo di lottare contro gravi forme di criminalità o di prevenire gravi minacce alla sicurezza pubblica. Secondo la Corte "al fine di garantire, in pratica, il pieno rispetto di tali condizioni, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette".

quest'ultimo individua nella valutazione dei rischi e nella limitazione delle finalità del trattamento gli argini della P.A. in materia di dati. Se a tale dilatazione dei poteri combiniamo la riduzione delle funzioni di intervento e di controllo dell'Autorità Garante, si può individuare, con l'entrata in vigore del Decreto Capienze, un rischio maggiore per la privacy delle persone fisiche.

3.3.2. Una nuova regolamentazione sulla privacy nel procurement pubblico

Tutto quanto fino ad ora affermato riguardo alla progressiva digitalizzazione, acquisizione delle informazioni ed utilizzo dei big data nel procurement pubblico, nonché trasparenza, consenso informato, minimizzazione, pseudonimizzazione ed anonimizzazione dei dati, mostra in maniera inequivocabile i passi avanti fatti negli ultimi anni in materia di tutela dei dati personali a livello europeo, soprattutto per merito del GDPR del 2016. Tuttavia permangono, a livello nazionale, dei punti di difficile applicazione dello stesso ed aree ancora scoperte, nelle quali risulta complessa una effettiva tutela dei soggetti sottoposti al trattamento dei dati. Uno dei più importanti progressi in materia di tutela della privacy è, indubbiamente, rappresentato dalla istituzione e dal progressivo ampliamento dei poteri del Garante per la protezione dei dati personali, organo amministrativo indipendente con funzione di vigilanza e controllo, ma anche con potere sanzionatorio, di impulso e consultazione, in materia di privacy. Dal 2018 è, poi, divenuto pienamente applicabile in tutti gli Stati membri dell'UE il Regolamento 2016/679, ossia il già citato GDPR (General Data Protection Regulation). Ciò che crea maggiore incertezza sono le aree di autonomia dei Paesi membri nel disciplinare in maniera più specifica, rispetto al GDPR, aspetti non ricompresi nella competenza UE in base al principio di attribuzione. In Italia dal settembre 2018 è entrato in vigore il d.lgs. n. 101 del 10 agosto 2018, che ha introdotto disposizioni per l'adeguamento della normativa nazionale italiana (d.lgs. n. 196/2003) alle disposizioni del GDPR. Oltre a recepire le disposizioni del GDPR, il decreto in parola ha regolamentato specifici aspetti rimessi alla potestà legislativa nazionale, fra cui la previsione di fattispecie di illeciti penali, e sanzioni pecuniarie già previste nel Regolamento europeo. Un elemento nel passato sottovalutato, che col GDPR è diventato punto cardine della tutela dei dati è la valorizzazione del principio di accountability, ossia la responsabilizzazione dei titolari del trattamento. Per responsabilizzazione si intende l'adozione di comportamenti atti a dimostrare la concreta attuazione del GDPR e di misure tecniche e organizzative adeguate alla tutela dei dati personali. Un punto fondamentale del GDPR non completamente attuato dalle legislazioni nazionali, riguarda le disposizioni sul c.d. data breach, ossia la violazione della sicurezza dei dati, che

comporta illecitamente o anche accidentalmente la divulgazione, perdita, alterazione, distruzione non autorizzata dei dati, ovvero l'accesso o trasmissione degli stessi[352].

Le maggiori difficoltà di adeguamento al GDPR riguardano proprio la Pubblica Amministrazione, non solo per la complessità dovuta al superamento dei problemi connessi alla burocrazia di cui soffre il nostro Paese, ma anche per la difficoltà di conformare le problematiche attinenti al trattamento dei dati con le necessità amministrative strettamente inerenti ai poteri pubblici. Ne è un chiaro esempio il c.d. Decreto Capienze, che ha esteso i poteri della P.A. riguardo il trattamento dei dati personali, nei casi in cui siano coinvolte finalità di interesse pubblico[353]. Ciò costituisce un notevole passo indietro in materia di tutela dei dati personali nel procurement pubblico, anche in considerazione della limitazione di poteri operata dal decreto nei confronti del Garante, nel rapporto con le amministrazioni, relativamente ai trattamenti ad alto rischio. Secondo alcuni autori, tuttavia, ciò ha connotato le amministrazioni di maggiore accountability, per l'assunzione del rischio della non conformità delle scelte effettuate sia in termini di liceità del trattamento sia sulla corretta individuazione ed implementazione delle misure di sicurezza poste a presidio dei trattamenti[354].

Nel considerare la possibilità di una nuova regolamentazione in materia di tutela dei dati personali, più concreta e performante di quella vigente, con particolare riguardo al procurement pubblico, è necessario partire dal Regolamento europeo 2016/679, quale solida base normativa sovranazionale su cui fondare le nuove regole nazionali. In primis è necessaria una piena applicazione del GDPR da parte della normativa nazionale, senza deroghe e poteri specifici conferiti all'amministrazione. A tal fine sarebbe ineluttabile una novella al Decreto Capienze, che ponesse un controllo all'operato della Pubblica Amministrazione in materia di dati personali. Difatti, oggi, in violazione del Considerando 45 del Regolamento europeo non è più una norma di legge ma lo stesso ente pubblico a definire il motivo per cui è necessario trattare dati personali. Nello specifico, ferma restando la disposizione dell'articolo 9, comma 1, lett. a) del d.l. n. 139/2021 per la quale è sempre consentito il trattamento dei dati personali da parte di

[352] Cfr. Guzzo A., *Data breach nel GDPR: cos'è e come fare segnalazione e prevenzione*, in *Agenda Digitale*, 28 maggio 2018.
[353] D.l. n. 139/2021, articolo 9, comma 1, lett. a), con l'aggiunta del nuovo comma 1-bis all'articolo 2-ter del d.lgs. 196 del 2003.
[354] Di tale parere, Cataleta A., Longo A., Natale R., *GDPR, tutto ciò che c'è da sapere per essere in regola*, in *Agenda Digitale*, 21 gennaio 2022, ove si fa riferimento al provvedimento sanzionatorio del Garante per la protezione dei dati personali contro Roma Capitale, Provvedimento del 7 marzo 2019 [9121890].

un'autorità pubblica se ciò sia necessario per l'adempimento di un compito svolto nel pubblico interesse, è necessaria una modifica che consenta l'esercizio di tale potere soltanto se la finalità del trattamento sia prevista da una norma di legge, ed in nessun caso può essere l'amministrazione a definire la finalità dello stesso. In tal modo si crea un limite al potere della P.A. riguardo al trattamento dei dati personali, rappresentato dalla riserva di legge. È, poi, necessario ripristinare la funzione di controllo preventivo del Garante per la protezione dei dati personali, nei trattamenti a rischio elevato. Tale potere del Garante, cancellato dal Decreto Capienze, è previsto nel combinato disposto degli articoli 35 e 36 del GDPR, e rappresenta un deterrente di particolare rilevanza riguardo alla violazione del Regolamento da parte delle amministrazioni, nei trattamenti che presentino dei rischi elevati, pertanto con maggior necessità di tutela.

Oltre alle modifiche che dovrebbero essere attuate alla normativa vigente per un effettivo rispetto della privacy, si evidenzia che per regolamentare la tutela dei dati personali sia altresì opportuno avvalersi con maggior frequenza anche di atti di soft law, nello specifico linee guida dell'AgID (Agenzia per l'Italia digitale) e del Garante per la protezione dei dati personali[355]. Tali atti hanno il pregio di semplificare la regolamentazione, rendendo più agevoli anche eventuali novelle, e nel contempo creare i presupposti per la corretta attuazione delle norme in materia di privacy. Gli atti di soft law contengono, inoltre, regole meno astratte di quelle della legge, facilmente adattabili e modificabili in funzione del progresso tecnologico, nonché immediatamente ed uniformemente applicabili. Le Linee Guida predisposte nel 2020 da AgID attinenti alla sicurezza nel procurement[356], oggetto di parere da parte del Garante per la tutela dei dati personali, hanno chiarito alcuni aspetti applicativi riguardanti le garanzie relative alle misure tecniche e organizzative adeguate al fine di tutelare i diritti del titolare dei dati. Tuttavia il documento, nella rappresentazione delle best practices, lascia alcuni punti scoperti, che dovrebbero essere integrati con ulteriori provvedimenti della stessa tipologia. Le linee guida sono, nel complesso, generiche e poco articolate, limitandosi a ribadire quanto disposto in alcuni articoli del GDPR. Nello specifico, non vengono individuate le garanzie che i fornitori di servizi informatici di cui si avvalgono le amministrazioni, devono prevedere per far sì che il trattamento soddisfi i

[355] Già in varie occasioni le linee guida dell'AGID sono state sottoposte al parere del Garante per la tutela dei dati personali, come nel caso delle linee guida operative per la fruizione dei servizi SPID da parte di minori, e quelle dell'app IO.

[356] Determinazione n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT.

requisiti del Regolamento e tuteli i diritti dell'interessato. Le linee guida dovrebbero, invece, specificare ed attuare concretamente tutte le disposizioni contenute nel GDPR, fornendo alle amministrazioni e ai fornitori di servizi le raccomandazioni e le indicazioni riguardanti i comportamenti da tenere per tutelare i dati personali. Dovrebbero, poi, contenere suggerimenti tecnici riguardanti la conservazione e l'analisi dei dati ed essere costantemente aggiornate tramite una revisione sistematica della letteratura e della casistica. Oltre alla qualità delle stesse, basata sull'autorevolezza degli esperti che le redigono, devono essere connotate di flessibilità ed adattabilità alle mutevoli condizioni locali, ed esplicitare gli effetti in caso di mancato rispetto delle stesse. Certamente caratterizzate da una maggiore accuratezza e precisione, sono le Linee guida in materia di trattamento di dati personali per profilazione on line del Garante per la protezione dei dati personali[357]. Tuttavia esse risalgono ad un periodo anteriore al GDPR e non hanno avuto alcun aggiornamento successivo. Inoltre non riguardano in maniera specifica il procurement pubblico e si adattano con difficoltà agli attuali sistemi di open data e big data.

In definitiva si può certamente affermare che la normativa europea, ed in particolare il Regolamento 2016/679, rappresenta le fondamenta su cui edificare una regolamentazione nazionale con un efficace apparato di tutele riguardanti i dati personali. Il GDPR deve, tuttavia, essere considerato dai singoli Stati membri, come un apparato di tutele minime in materia di dati personali, mai derogabili in *peius* ma sempre in *melius* con riferimento ai soggetti da tutelare, e senza possibilità di attribuire maggiori poteri alle amministrazioni. A livello nazionale è, certamente, necessario un apparato capillare di regole, non solo costituite dalle norme di legge, ma anche e soprattutto da atti di soft law, ed in particolare da linee guida predisposte da autorità indipendenti quali il Garante della privacy, che delineino in maniera specifica ed approfondita le buone pratiche da seguire da parte dei responsabili della tutela dei dati, amministrazioni e relativi fornitori di servizi informatici. Infine, la responsabilizzazione di determinati soggetti deputati a far rispettare la tutela dei dati personali, non può essere racchiusa in un ambito soltanto formale, ma deve divenire effettiva, sia a livello di singola amministrazione che negli organismi nazionali, tramite la predisposizione di un sistema gerarchico di controlli esterni permanenti e periodici, che prevedano dettagliate relazioni di audit a distanza di tempi molto brevi (mensili o al massimo bimestrali), ed oltre ai provvedimenti disciplinari di tipo sanzionatorio, considerino anche

[357] Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015 [3881513].

meccanismi premiali nei confronti di quei funzionari che applichino in maniera pedissequa e continua i regolamenti in materia di privacy.

Capitolo 4. Il conflitto d'interessi nel procurement sanitario pubblico

4.1. La sanità in Italia

4.1.1. Servizio Sanitario Nazionale e privatizzazione

La tutela della salute costituisce un diritto fondamentale sancito dalla Costituzione all'art. 32. Tale diritto viene tutelato principalmente dal Servizio Sanitario Nazionale (SSN), un sistema di servizi e strutture che ha il fine di garantire a tutti gli individui, in condizioni di uguaglianza, l'accesso all'erogazione delle prestazioni sanitarie. Un principio fondamentale su cui si basa il SSN sin dalla sua istituzione[358] è quello dell'universalità, ossia l'estensione delle prestazioni sanitarie a tutta la popolazione, garantendo uniformemente i LEA (Livelli Essenziali di Assistenza). L'accesso al SSN deve, poi, avvenire senza discriminazioni di condizioni individuali, sociali o economiche, e gratuitamente per gli indigenti, che vengono esentati dal pagamento di ogni prestazione sanitaria. Strettamente connesso al principio di eguaglianza è quello di equità, che consente ai pazienti parità di accesso in rapporto ai medesimi bisogni di cure, garantendo la trasparenza del servizio anche tramite un'informazione corretta sulla prestazione sanitaria (consenso informato), ed adeguata al grado di comprensione ed istruzione del paziente. Il paziente è libero di scegliere anche strutture private convenzionate col SSN.

Secondo i dati del Ministero della Salute sia la spesa sanitaria che i posti letto a partire dal 2010, fino all'emergenza sanitaria da Covid-19 si sono notevolmente ridotti in tutto il territorio nazionale, con un divario ancor più ampio fra nord e sud Italia. I posti letto sono diminuiti mediamente del 15,5 per cento rispetto alla popolazione, con un calo molto più marcato nelle strutture pubbliche, del 17,1 per cento, rispetto a quelle private accreditate, che è fermo al 9 per cento. Il calo di posti letto in Italia è superiore sia alla media OCSE36 che alla media dell'Unione europea[359]. Nonostante la pandemia presente già dai primi mesi del 2020, le previsioni riguardanti la spesa sanitaria pubblica rese note dal Governo sono decisamente al ribasso: dal 6,6 per cento del PIL nel 2020, si è riscontrata una risalita al 7,3 per cento nel 2021 per il Covid, mentre per il 2022 si scende nuovamente al 6,7 per cento, nel 2023 è prevista al 6,6 per cento e 6,3 per cento

[358] Avvenuta con legge n. 833 del 1978.

[359] Del 4,5 per cento rispetto alla media OCSE e del 6,7 per cento rispetto all'UE. Per i dati OCSE la fonte è: OECD (2019), Health at a Glance 2019: OECD Indicators, OECD Publishing, Paris, https://doi.org/10.1787/4dd50c09-en. I dati riguardanti tutti i Paesi UE sono estratti dal data browser Eurostat, raggiungibile collegandosi al link: https://ec.europa.eu/eurostat/databrowser/view/tps00046/default/table?lang=en.

nel 2024[360]. L'emergenza sanitaria ha mostrato le fragilità del nostro sistema nazionale, penalizzato da decenni di de-finanziamento, tagli al personale, contrazione dei posti letto ed indebolimento della medicina territoriale. Tuttavia non vi è stato alcun cambio di rotta, poiché continua il taglio delle risorse umane e strutturali, l'inefficienza del sistema con liste d'attesa sempre più lunghe, e l'espansione dell'offerta privata di pari passo alla riduzione di quella pubblica.

Quest'ultimo punto è di particolare rilevanza, poiché interessi personali e conflitti d'interesse hanno favorito i soggetti privati per l'accesso ai finanziamenti europei, penalizzando il sistema pubblico e trasformando sempre più i servizi sanitari in interessi aziendali, il cui fine principale non è il benessere del paziente ma i ricavi nel bilancio, se non addirittura il profitto personale. I vincoli che limitano assunzioni stabili nel sistema sanitario pubblico, poi, creano ulteriore incertezza favorendo gli istituti di cura privati, che possono avvalersi di personale più esperto, meglio pagato, ed assunto stabilmente. I pazienti si rivolgono sempre più al privato aumentandone il potere di mercato ed indebolendo l'offerta pubblica, ed il recente PNRR (Piano Nazionale di Ripresa e Resilienza) prevede ulteriori forme di privatizzazione in servizi quali l'assistenza ad anziani, disabili e soggetti fragili. La quota di spesa del Servizio Sanitario Nazionale assorbita dai privati ha, oggi, abbondantemente superato il venti per cento di quella totale, ed il trend è in continuo aumento. Nel complesso, il privato accreditato gestisce quasi un terzo[361] dei posti letto ospedalieri a livello nazionale. Preoccupante è la proposta di riforma del marzo 2021 per aumentare la concorrenza nel settore sanitario, avanzata al Governo dall'Autorità Garante della Concorrenza e del Mercato, la quale sollecita maggiore apertura "all'accesso delle strutture private all'esercizio di attività sanitarie non convenzionate" e l'eliminazione del "vincolo della verifica del fabbisogno regionale di servizi sanitari". Il modello proposto dal Garante è il medesimo che ha lentamente cancellato la rete dei servizi territoriali pubblici e ha messo in campo una concorrenza squilibrata tra pubblico e privato, e a favore di quest'ultimo. È, invece, necessaria la riqualificazione di un servizio sanitario pubblico universalista, egalitario, senza discriminazioni di accesso e finanziato dalla fiscalità generale, il quale dovrebbe collocarsi nel disegno di una più ampia espansione di tutti quei servizi collettivi di welfare che sono stati colpiti o riconfigurati in funzione del profitto dalle politiche neoliberali, e dovrebbe essere

[360] Cfr. Bindi R., Dirindin N., Geddes M., *La sanità italiana verso una privatizzazione strisciante. Il Governo fermi questa deriva*, in *Quotidiano sanità*, 14 settembre 2021.
[361] Precisamente il 31,3 per cento (fonte Rapporto OASI, Cergas Bocconi).

indissolubilmente legato al principio dell'integrazione socio-sanitaria, e ad una programmazione nazionale dei servizi coordinata a livello regionale. A tal fine bisognerebbe in primis restituire alla sanità integrativa il suo ruolo originario, ovvero il rimborso delle sole prestazioni non incluse nei LEA, impedendo così che fondi pubblici, sotto forma di incentivi fiscali, alimentino i profitti dell'intermediazione finanziaria e assicurativa. In un periodo come quello attuale di riorganizzazione sanitaria dovuta alla pandemia, appare sempre più urgente una nuova legislazione che ponga un freno alla privatizzazione nel settore sanitario, per evitare che vengano erose sempre più risorse alla finanza pubblica per essere redistribuite in maniera iniqua, con conseguente aumento della spesa sanitaria totale, grave danno economico alle famiglie, diminuzione della qualità del servizio e aumento dei rischi per la salute delle persone legati a fenomeni di sovra-diagnosi e sovra-trattamento[362].

L'aziendalizzazione, regionalizzazione e privatizzazione nella sanità, introdotte col decreto legislativo n. 502 del dicembre 1992, guardano in una direzione opposta ai principi ispiratori che nel 1978 hanno istituito il Servizio Sanitario Nazionale. La tendenza a rendere la sanità un business di livello aziendale e non un diritto dei cittadini costituzionalmente garantito, si è ulteriormente dilatata negli ultimi anni di emergenza sanitaria, in particolare nello specifico settore del procurement, poiché l'approvvigionamento di strumentazione medica e dispositivi di protezione ha richiesto l'investimento di notevoli risorse economiche. Il paradigma che lega la tutela della salute alla sostenibilità economica del sistema sanitario non può prescindere dalla lotta al conflitto di interessi, e di conseguenza allo spreco di risorse e alle inefficienze, rendendo il sistema incapace di rispondere ai bisogni di cura dei pazienti. L'idea di un procurement strategico finalizzato a generare valore sociale per soddisfare i bisogni di salute ed essere altresì vettore di innovazione e investimenti, ad oggi non si è pienamente realizzata, proprio per i troppi interessi privati in gioco e per un'ingerenza di figure politiche troppo spesso in conflitto di interessi. L'intero sistema sanitario avrebbe, invece, bisogno di maggiore efficacia ed efficienza nella gestione, ed in particolare per ciò che riguarda l'approvvigionamento, maggiore trasparenza e controlli dal basso, ovvero da parte di autorità effettivamente imparziali e *super partes*. Secondo il report dell'OCSE "Tackling wasteful speding on health", difatti, gran parte delle risorse destinate alla

[362] Cfr. Fondazione Gimbe, *Sanità verso la privatizzazione: oltre 4 miliardi di agevolazioni fiscali per fondi integrativi e welfare aziendale*, in Il Sole 24 Ore, 25-06-2019, alla pagina web: www.sanita24.ilsole24ore.com/art/aziende-e-regioni/2019-06-25/sanita-la-privatizzazione-oltre-4-miliardi-agevolazioni-fiscali-fondi-integrativi-e-welfare-aziendale-174644.php?uuid=AC1x0ZU&refresh_ce=1.

spesa sanitaria vengono sprecate inutilmente, con grave nocumento per la salute pubblica, ed insoddisfazione dei pazienti[363].

4.1.2. Health technology assessment

Negli ultimi anni, nel settore medico si sente sempre più parlare di HTA, health technology assessment, il cui obiettivo principale è la condivisione di informazioni riguardanti le tecnologie per poter concertare politiche sanitarie efficaci ed efficienti in termini economici, ma soprattutto orientate al paziente. È, più specificamente, uno strumento di valutazione delle tecnologie sanitarie[364], che aiuta nell'individuazione di quelle più valide da inserire nella sanità sia a livello nazionale che locale, per mezzo della previsione degli effetti che esse potrebbero generare nel sistema sanitario[365]. In Italia nel 2016 è stato istituito presso l'Istituto Superiore di Sanità, il Centro nazionale per l'health technology assessment col compito ultimo di migliorare la qualità e gli standard dei servizi sanitari e della pratica clinica, tramite un costante supporto al processo decisionale, producendo informazioni sugli effetti clinici, economici, organizzativi, sociali, legali ed etici delle tecnologie sanitarie. Nello specifico il Centro svolge un'attività di promozione dell'utilizzo di documenti HTA nella pianificazione degli obiettivi del Sistema Sanitario Nazionale e nell'ambito della pratica clinica. Si propone, inoltre, di creare prove di evidenza sulle tecnologie nella pratica clinica al fine di contribuire ad una corretta valutazione del loro utilizzo.

La stessa Organizzazione Mondiale della Sanità[366] ha esortato la creazione di sistemi nazionali di valutazione indipendente delle tecnologie in sanità, per favorire l'utilizzo sistematico di tali valutazioni con compito di supporto, al fine di informare ed orientare le decisioni politiche. Le valutazioni sono maggiormente rilevanti nella gestione del sistema di approvvigionamento, nonché nella formulazione di sistemi di finanziamento per la farmaceutica, nella stesura di linee guida per la pratica clinica e protocolli per programmi di salute pubblica. Dalle analisi di HTA emergono, poi, indicazioni in merito alle aree terapeutiche e tecnologiche che il sistema pubblico

[363] Secondo l'OCSE, report "Tackling wasteful speding on health", 2017, "una parte significativa della spesa sanitaria è – nella migliore delle ipotesi – spreco, o peggio danneggia la nostra salute".
[364] Secondo la definizione dell'OMS, Organizzazione Mondiale della Sanità - WHO definition (EB 134/30): "Health technology assessment is the systematic evaluation of properties, effects and/or impacts of health technologies and interventions".
[365] Banta D., *What is technology assessment?*, in *International Journal Technology Assessment Health Care*, 2009, n. 25 suppl. 1, p. 7-9.
[366] OMS, risoluzione WHA67.23 del 24 maggio 2014.

ritiene prioritarie, e soprattutto verso cui indirizza risorse finanziarie e promuove programmi di ricerca.

L'obiettivo di focalizzare le scelte relative all'assistenza sanitaria sull'efficienza ed efficacia, senza tuttavia trascurare le esigenze dei pazienti, può essere raggiunto soltanto attraverso processi trasparenti e sistematici ai quali tutte le parti interessate possano contribuire[367]. In Italia rappresenta una valida risposta all'incontrollata diffusione di costose tecnologie sanitarie, introdotte nel sistema nazionale al solo fine di favorire determinati operatori economici. L'HTA rappresenta, pertanto, uno strumento di orientamento delle decisioni basato sulla valutazione delle evidenze ed a vantaggio esclusivo del paziente. È, tuttavia, necessario mantenere al centro di ogni decisione l'efficacia e l'efficienza dei processi[368], nell'ambito della spesa pubblica, e non permettere che le scelte effettuate poggino sugli interessi economici privati, sul conflitto di interessi, sulla corruzione e sul malaffare. L'approccio multidimensionale dell'HTA riguarda l'analisi delle implicazioni medico-cliniche, sociali, organizzative, economiche, ma anche etiche e legali di una tecnologia, attraverso la valutazione di più dimensioni quali l'efficacia, la sicurezza, i costi, l'impatto sociale-organizzativo. Tale approccio non può non considerare quale elemento di rilevanza principale, l'impatto delle tecnologie data driven utilizzate nel sistema sanitario per l'individuazione di situazioni a rischio corruzione, di conflitto di interessi, di maladministration. Negli ultimi anni la valutazione della tecnologia è stata caratterizzata da un crescente interesse istituzionale e dalla diffusione di applicazioni c.d. hospital-based HTA, interessando la gestione di: piani di investimento per dispositivi medico sanitari; prestazioni sanitarie; sistemi di supporto all'attività clinica e ricerca applicata; modalità clinico-organizzative dell'assistenza.

Peculiarità principale dell'HTA è la condivisione e l'analisi dei dati, senza i quali le scelte non potranno essere libere e trasparenti, ma condizionate da gruppi di influenza e multinazionali. Secondo il Ministero della salute il ricorso all'HTA rende i documenti di valutazione delle tecnologie "asettici da influenze legate ad interessi specifici e contrastanti"[369]. Tale affermazione rappresenta certamente la realtà, ma ciò può essere sostenuto e avvalorato soltanto ove non vi

[367] In tal senso, Health Equality Europe, edizione italiana a cura di La Torre G., Monteduro A., Kheiraoui F., *Comprendere l'Health Technology Assessment (HTA)*, Editore Prex s.p.a., 2009, p. 3 e ss.
[368] Health Equality Europe, edizione italiana a cura di La Torre G., Monteduro A., Kheiraoui F., *Comprendere l'Health Technology Assessment (HTA)*, Editore Prex s.p.a., 2009, p. 15 "Dinanzi alle sfide che la malattia comporta le persone hanno necessità di ricevere trattamenti e cure efficaci che diano loro la migliore opportunità di salute. Allo stesso tempo, vi è un'esigenza della sanità pubblica di prevenire le malattie, ove possibile. Tuttavia, le risorse disponibili possono essere limitate e devono essere adeguatamente allocate, sulla base dei principi di economicità e di efficacia".
[369] Ministero della Salute, *Adapted HTA Report*, luglio 2014.

siano conflitti di interessi che vedano protagonisti i redattori dei documenti di valutazione stessi. Da un HTA e dalle linee guida di agenzie regolatorie possono dipendere gli orientamenti nel procurement sanitario ed è, pertanto, essenziale che coloro che sono coinvolti in decisioni di tale importanza debbano essere al di sopra di qualsivoglia rischio di conflitto di interessi. Al riguardo, lo scrivente considera insufficiente una mera dichiarazione di assenza di conflitto di interessi, ma sarebbero necessarie ricerche approfondite tramite l'incrocio di dati, e valutazioni indipendenti da parte di organi di controllo, prima di adibire il ricercatore alla commissione di sviluppo di un documento HTA.

4.2. L'incidenza del conflitto d'interessi nella sanità pubblica

4.2.1. Il procurement sanitario pubblico

Il procurement pubblico, inteso come processo di acquisizione di beni o servizi a favore dello Stato o enti pubblici da parte di imprese esterne è sempre più spesso, nel nostro Paese, al centro di contese politiche e controversie giudiziarie. Ciò in quanto, soprattutto in alcuni settori di particolare rilevanza economica, quali l'approvvigionamento di beni in sanità[370], l'aggiudicazione di una procedura di gara può essere fonte di guadagni milionari per le imprese. L'apparato normativo ha il difficile compito di definire le regole del procurement pubblico, col preciso fine di soddisfare i bisogni delle amministrazioni, cercando nel contempo di avvalersi di procedure trasparenti ed eque. Solo in tal modo è possibile ottenere il soddisfacimento delle esigenze di tutti gli stakeholder, ossia del cittadino potenziale utente di un servizio, dell'amministrazione, e degli operatori economici che possono muoversi in un regime di competizione, concorrenza e pari opportunità. Per conseguire detti risultati è necessario non solo un apparato di norme equilibrate e coerenti, ma anche il rispetto delle regole che può essere ottenuto soltanto con organismi e con strumenti di controllo efficienti, che impediscano il verificarsi di sprechi di denaro pubblico e favoritismi di qualsivoglia natura.

Efficacia ed efficienza sono due punti fondamentali della pubblica amministrazione. L'efficacia indica la capacità di raggiungere un obiettivo prefissato da parte dell'amministrazione, ed è *condicio sine qua non* dell'efficienza, ossia della capacità di raggiungere tali obiettivi impiegando le risorse minime possibili, non solo economiche ma anche di tempo e lavoro. Al fine di garantire

[370] Amatucci F., Mele S., *I processi di acquisto di beni e servizi nelle aziende sanitarie. Elementi di innovazione e modelli di accentramento*, II edizione, Egea, 2016, p. 102 ss.

un procurement sanitario che sia non solo efficace ma anche efficiente, in termini di risultati ottenuti e di costi di gestione, è necessario porre l'accento sull'individuazione dei fabbisogni dei soggetti pubblici e sui processi di spesa, nel rispetto delle norme. Questi ultimi dovranno essere pianificati in modo da permettere il raggiungimento degli obiettivi dell'amministrazione, coniugando un difficile equilibrio tra lotta all'illegalità e alla corruzione e spazio decisionale dell'amministrazione stessa. Per il raggiungimento di tale finalità è di primaria importanza una normativa sugli appalti pubblici chiara e precisa e nello stesso tempo elastica per ciò che riguarda i ruoli dei soggetti coinvolti e le necessità concrete dell'amministrazione, ma soprattutto aperta alle nuove tecnologie. Per ottenere alte performance di efficienza è necessaria non solo un'apertura ma una simbiosi fra normativa e tecnologia. Quest'ultima dovrà essere presente in ogni fase, non solo in quella relativa ai controlli ed alle verifiche, ma a partire dalla pubblicazione del bando, al fine di rendere l'intera procedura di aggiudicazione più sicura e meno esposta al rischio di comportamenti illeciti. Il maggior antagonista di un procurement sanitario efficace ed efficiente è un apparato normativo che riceva un rispetto puramente formale, unito ad una mancata programmazione dei fabbisogni ed organizzazione delle spese. Tutto ciò deve, in maniera inequivocabile, essere inserito in una previsione di obiettivi chiari e predeterminati. Soltanto una normativa capace di adattarsi alle esigenze dell'amministrazione e degli stakeholder, modificando gli assetti organizzativi basati sulle responsabilità degli operatori e sulle competenze e ruoli professionali, può avere la capacità di produrre risultati positivi. L'esigenza di adeguare il sistema del procurement pubblico ai cambiamenti della società e dell'amministrazione ha dato vita al Codice dei contratti pubblici, D.lgs. n. 50 del 2016. Tuttavia il Codice del 2016 non ha rispettato appieno le premesse, suscitando critiche e successive revisioni.

Bisogna considerare che corruzione e conflitto di interessi costituiscono il primario elemento ostativo dell'efficienza di un'amministrazione, nonché della trasparenza e correttezza delle procedure con conseguente spreco di denaro pubblico, che si sarebbe dovuto invece impiegare per le cure del paziente[371]. È, pertanto, necessaria un'opera di contrasto dei fenomeni corruttivi, tramite la prevenzione e la repressione degli stessi, evitando il conflitto di interessi, spesso alla base di pratiche scorrette e comportamenti tendenziosi se non anche illeciti. Sono proprio gli alti

[371] Sul procurement pubblico: F. Baldassarre, A.S. Labroca, *Public procurement. Gli acquisti pubblici fra vincoli giuridici e opportunità gestionali*, Franco Angeli Editore, 2013; ed E. Valeriani, *Public procurement. Mercato, comportamenti, contratti e conflitti*, Istituto Editoriale Cisalpino, dicembre 2013.

livelli di corruzione, la mancanza di trasparenza e il conflitto di interessi a rappresentare, nel nostro Paese, una minaccia al funzionamento della sanità e pubblica amministrazione in generale. La determinazione dei danni cagionati dalla corruzione ed inefficienza in sanità, soltanto in Italia, è approssimativamente quantificata in oltre 30 miliardi di euro annuali, quasi un quinto del totale dell'intero settore. La sanità è, per tale motivo, stata più volte oggetto dell'attenzione dell'ANAC, la quale ha individuato le aree maggiormente a rischio[372], fornendo alle pubbliche amministrazioni efficaci strumenti per contrastare gli eventi corruttivi. Le quattro aree a rischio generale, individuate da ANAC sono:

a. contratti pubblici;
b. incarichi e nomine;
c. gestione delle entrate, delle spese e del patrimonio;
d. controlli, verifiche, ispezioni e sanzioni.

A queste si aggiungono altre quattro aree a rischio specifico:

a. attività libero professionale e liste di attesa;
b. rapporti contrattuali con privati accreditati;
c. farmaceutica, dispositivi e altre tecnologie: ricerca, sperimentazioni e sponsorizzazioni;
d. attività conseguenti al decesso in ambito intraospedaliero.

Una base fondamentale da cui partire onde evitare il conflitto di interessi è sicuramente la pianificazione di tipo manageriale, necessaria sia nel pubblico che nel privato. Le maggiori criticità, in primis corruzione e sprechi, hanno, difatti "le loro radici principalmente nella mancata programmazione degli acquisti in relazione agli obiettivi da raggiungere"[373]. È, pertanto, necessaria un'attenta organizzazione dei processi di approvvigionamento con l'elaborazione del *procurement plan*, oltre alla loro definizione e all'attività di controllo nell'attuazione, al fine di garantire agli stakeholder la trasparenza riguardo eventuali rischi e le spese da sostenere. Essa deve ricomprendere, nello specifico, un'accorta analisi del rischio, al fine di prevenire il pericolo

[372] ANAC, Ministero della Salute, Agenzia Nazionale per i Servizi Sanitari regionali, Linee Guida per l'adozione dei Codici di comportamento negli enti del SSN.
[373] R. Colangelo, *Una visione sistemica del procurement pubblico*, Contributo per la definizione del progetto laboratorio MAAP (Master in Management degli Approvvigionamenti ed Appalti Pubblici), cap. 10 in G. Atti (a cura di) *La quarta rivoluzione industriale: verso la supply chain digitale*, Franco Angeli, Milano 2018.

di costi non computati, dovuti sia al ciclo di vita dei beni oggetto di appalto, che ad eventuali risarcimenti dei danni a terzi da essi provocati.

Nell'analisi del rischio devono essere necessariamente considerati anche i fenomeni corruttivi e i conflitti di interessi, molto frequenti nel procurement sanitario. Particolare impegno deve essere dedicato alla definizione ed al periodico aggiornamento degli indicatori di rischio, soprattutto in riferimento al conflitto di interessi. Qualora gli indicatori di rischio non fossero individuati con precisione ovvero non venissero costantemente aggiornati a seconda delle variazioni nel tessuto sociale, neanche le tecnologie più moderne, compresi big data e machine learning, potrebbero essere d'aiuto nel contrasto al conflitto d'interessi e nella prevenzione degli illeciti. Una corretta definizione degli indicatori di rischio richiede, principalmente, una scomposizione dell'intero processo di approvvigionamento, ed una analisi degli stessi indicatori in tutte le fasi della procedura, compresa quella prodromica, nonché quella successiva alla chiusura della stessa. Un altro elemento determinante nell'individuazione dei conflitti di interessi nel procurement consiste nella standardizzazione delle metodologie di individuazione degli indicatori. Ciò renderebbe maggiormente oggettivi i risultati delle analisi dei dati, ferma restando la necessità di differenziare settori profondamente diversi dagli altri, quali la sanità pubblica. Sarebbe, inoltre, necessario ad avviso dello scrivente, nell'analisi degli indicatori, predisporre ed interrogare un archivio storico dei dati utilizzati in precedenza, che possa tenere in debita considerazione proprio quegli orientamenti e cambiamenti della società, dell'etica e del costume, che spesso disorientano le ricerche statistiche. Soltanto con tali precauzioni potranno essere monitorati fenomeni che altrimenti resterebbero occultati nelle fitte maglie delle procedure di approvvigionamento pubblico[374].

4.2.2. Etica e deontologia nella sanità pubblica

Nella sanità pubblica i principi etici di base sono quelli direttamente attinenti alla tutela della salute, ossia i contenuti della deontologia medica. Gli obiettivi dell'azienda sanitaria, che si identificano con l'efficacia determinante la qualità del servizio sanitario, possono essere raggiunti con differenti gradi di efficienza, perciò con utilizzo di risorse più o meno contenuto. L'integrità

[374] Cfr., *Libro bianco sulla corruption in sanità*, ISPE (Istituto per la promozione dell'etica in sanità), p. 158 ss., ove si auspica l'inserimento di una nuova metodologia di supporto alle attività di controllo dirette alla prevenzione degli illeciti, il SOCC (strumento operativo di controllo della corruzione), utile per l'individuazione di potenziali comportamenti non etici o situazioni di rischio, in ambiti ove questi siano difficilmente evidenziabili.

delle scelte manageriali sul piano organizzativo e della gestione degli appalti è, pertanto, a prescindere da illegalità e corruzione, un dovere fondamentale che si fonde con la deontologia. Problemi che influenzano negativamente efficacia ed efficienza, in entità complesse come quelle sanitarie, sono la lottizzazione politica, nonché il ruolo del direttore generale dell'azienda sanitaria, il quale gode di poteri particolarmente ampi, ma anche la superficialità con cui il dipendente comune ed il funzionario affrontano problematiche complesse che richiederebbero, invece, un impegno particolare. Con riguardo alle assunzioni nella sanità pubblica la situazione è apparentemente meno complessa, poiché il relativo accesso avviene, ex art. 97 ultimo comma della Costituzione, tramite concorso. Tuttavia il sistema non è esente da mancanze e contraddizioni, giacché i candidati non possono essere valutati sul campo per le loro doti pratiche, ma solo per le conoscenze teoriche.

Sul piano del conflitto di interessi si può distinguere fra comportamenti che violano la legge e comportamenti non perseguibili giudizialmente ma eticamente o deontologicamente scorretti, in quanto generano inefficienza ed inefficacia del sistema. L'insieme di tali azioni è identificata con il termine anglosassone "corruption", ossia non solo atti illeciti, ma anche leciti e soltanto deontologicamente scorretti che creano disfunzioni, inefficienze e sprechi[375]. La pratica, abusata nel nostro Paese, dei tagli lineari, non ha migliorato la situazione ponendo un freno a tali condizioni, ma ha finanche acuito il problema. Essa, difatti, non ha ottimizzato l'efficienza del sistema aziendale sanitario, ma ha contenuto l'esborso di risorse, riducendo conseguentemente l'efficacia intesa come qualità dei servizi sanitari. La disponibilità di minori risorse non ha minimamente intaccato quelle destinate a corruzione e generate dai conflitti di interessi, ma si è andata a ripercuotere sul servizio offerto all'utente finale, il paziente, ossia colui che dovrebbe, invece, essere al centro dell'impegno dell'azienda sanitaria. Ciò ha comportato l'effetto di una cronica mancanza di personale in sanità, aggravata altresì da un sistema di *recrutement* obsoleto e dal filtro del numero chiuso per l'accesso ai corsi di laurea delle professioni sanitarie.

Pertanto non solo la corruzione, ma anche sprechi ed inefficienze minano la sostenibilità del nostro sistema sanitario. Sempre più frequentemente il confine fra attività illecita ed inefficienza è labile, e può essere varcato in qualsiasi momento. Non si deve, difatti, pensare alla corruzione

[375] Sul tema: Manca F., Angius E.D., *Management e performance nella sanità pubblica*, Ipsoa, 2018, p. 112 ss.; Bacci A., *Lean healthcare management*, Ipsoa, 2017, p. 14 ss.; AA.VV., *Corruzione e sprechi in sanità*, progetto di Transparency International Italia, a cura di RISSC, in collaborazione con ISPE Sanità, p. 24 ss.

come ad un fenomeno statico, ma come un virus che muta e si adatta continuamente per difendersi dalle politiche di contrasto e che cerca di eludere qualunque attività volta a bloccarne la potenza distruttiva. È, pertanto, necessaria una continua evoluzione sia delle politiche che delle tecniche anticorruzione, ma anche di tutti quegli strumenti, sia giuridici che manageriali, ma soprattutto tecnologici, messi a disposizione della sanità pubblica per raggiungere standard di efficienza, favorendo altresì una gestione entro i binari della legalità. Risultati di particolare rilevanza hanno ottenuto le disposizioni che tutelano i comportamenti etici di coloro che denuncino atti illeciti, corruttivi e conflitti d'interessi, come la legge n. 190 del 2012. Un'ampia quota degli episodi di corruzione emerge difatti, secondo recenti studi[376], tramite segnalazione diretta, ma anche telefonica o tramite mezzi tecnologici, di utenti comuni ed impiegati nel settore della sanità.

ANAC, con Delibera n. 158 del 30 marzo 2022, ha dato precise indicazioni in merito alla gestione del possibile conflitto d'interessi all'interno delle Amministrazioni Pubbliche, con particolare riguardo all'ambito sanitario, richiamando le amministrazioni stesse al rispetto pedissequo dei codici di comportamento. L'Autorità Anti corruzione sottolinea la particolare predisposizione del settore sanitario al conflitto di interessi, poiché "anche la sola percezione di situazioni di conflitto può avere rilevanti ripercussioni dal punto di vista economico e sociale". ANAC ribadisce, poi, il proprio ruolo in merito, finalizzato a indicare "integrazioni dei codici di condotta e dei piani anticorruzione" stimolando le amministrazioni a "implementare le proprie misure, per esempio attraverso un'integrazione del contenuto delle dichiarazioni da rilasciare". L'Autorità insiste sull'obbligo di pubblicazione dei nominativi dei consulenti nella sanità pubblica, richiedendone l'inserimento in elenchi pubblici consultabili, nei quali venga altresì definito l'oggetto, la durata e il compenso dell'incarico, nonché l'attestazione della avvenuta verifica di insussistenza di situazioni, anche potenziali, di conflitto di interessi. Infine ANAC chiede alle amministrazioni sanitarie di "indicare, a monte, direttive precise sugli eventi e sulle occasioni in cui è necessario che il personale presenti le dichiarazioni inerenti il conflitto d'interessi, attività propedeutica alla successiva verifica delle stesse, al fine di evitare che situazioni similari vengano trattate in modo dissimile"[377].

[376] Statistiche 2021 della Association of Certified Fraud Examiners.
[377] Delibera ANAC n. 158, approvata nel Consiglio del 30 marzo 2022.

Le caratteristiche che rendono la sanità vulnerabile alla *maladministration* e alla corruzione riguardano principalmente l'ingerenza politica nelle scelte amministrative, la eccessiva discrezionalità nelle scelte dei vertici gerarchici, l'espansione della sanità privata, la scarsa trasparenza nel procurement, l'asimmetria informativa fra paziente, sistema sanitario e fornitori. Uno studio effettuato presso la Commissione Europea ha messo in evidenza sei tipologie di corruzione principali:

a. erogazione dei servizi medici;
b. aggiudicazione di appalti;
c. rapporti commerciali illeciti;
d. utilizzo di posizioni di prestigio;
e. richieste di rimborso ingiustificate;
f. truffe e malversazioni relative a medicinali e a dispositivi medici.

Il principale moto di diffusione di abusi è, secondo il Rapporto sulla corruzione in sanità[378], la tolleranza da parte degli operatori del settore, ma anche dei pazienti e dei cittadini comuni, al fenomeno corruttivo ed una sorta di rassegnazione riguardo le inefficienze e gli sprechi. Il Rapporto raccomanda ai Paesi membri, innanzitutto una legislazione contro la corruzione chiara ed applicata in modo puntuale ed efficace, accompagnata alla centralizzazione degli acquisti, a strutture gestionali più efficaci e meccanismi di finanziamento adeguati, maggiori fondi per la ricerca medica indipendente, ed infine ad una distribuzione equa delle risorse. Il c.d. federalismo sanitario[379], che avrebbe dovuto creare un ostacolo ai fenomeni corruttivi e al conflitto di interessi, tramite lo spostamento dei centri decisionali dallo Stato alle strutture locali, lasciando ampia autonomia alle Regioni e puntando su un rapporto di prossimità con i cittadini, non ha prodotto gli effetti sperati. Ha, anzi, dilatato le diseguaglianze presenti nel nostro territorio, amplificando sacche di dispersione economica e di corruzione, con una fotografia, per nulla incoraggiante, di standard ospedalieri non raggiunti in molte aree del Paese, in particolare del centro sud, costi sanitari e liste di attesa profondamente differenti da una zona all'altra, e l'amara conseguenza che un paziente su dieci rinuncia alle cure, oppure, se ne ha le possibilità, si rivolge alla sanità privata.

[378] Rapporto a cura di ECORYS & EHFCN sulla corruzione nella Sanità in UE.
[379] Con le novelle al Titolo V della Costituzione viene ridisegnata, nel 2001, la mappa delle autonomie locali e dell'attribuzione di poteri a Stato, Regione ed Enti locali.

4.2.3. Contrasto alla corruzione e al conflitto d'interessi nel procurement sanitario

Nel settore sanitario il conflitto di interessi è da sempre considerato una problematica di rilevanza maggiore che in altri ambiti. Ciò non solo perché la sanità è maggiormente esposta a fenomeni opportunistici per il suo rilievo in termini di spesa pubblica, ma soprattutto perché l'interesse personale, nel confliggere con quello istituzionale, coinvolge un bene primario di rango costituzionale quale la salute. Il conflitto di interessi in ambito sanitario si concretizza in quella condizione soggettiva, per cui l'interessamento primario della salute del paziente può essere condizionato dall'interesse secondario, costituito dal vantaggio economico e personale del soggetto in conflitto, rischiando di danneggiare il sistema sanitario poiché determina scelte condizionate e generalmente inappropriate. Esso contribuisce in maniera consistente ad alimentare l'illegalità nel settore sanitario, pur non costituendo un comportamento, ma una condizione per il cui verificarsi è sufficiente un legame in grado di compromettere l'indipendenza dell'operatore. L'interesse secondario si trasforma in conflitto quando tende ad osteggiare l'interesse primario, diventando illecito solo ove vi sia una norma giuridica che lo sanziona. Nel procurement sanitario il conflitto di interessi può arrecare un danno diretto ai pazienti, in quanto tende a sollecitare consumi sanitari inappropriati ed approvvigionamenti privilegiati. Si pensi a quanto possa nuocere a soggetti malati, o anche a persone senza patologie, la somministrazione di terapie o farmaci inutili, se non addirittura dannosi, prescritti al solo scopo di favorire specifiche industrie farmaceutiche. Non è, tuttavia, da sottovalutare il danno indiretto, provocato da un distorto ed inappropriato utilizzo delle risorse per la spesa sanitaria, ed un conseguente minor finanziamento statale per singolo paziente e per posto letto. Fra gli effetti conseguenti ai conflitti di interessi, si può primariamente rilevare una minore efficienza della sanità pubblica a vantaggio di quella privata, che risulterà agli occhi delle persone più performante, ossia qualitativamente superiore, più tempestiva e maggiormente aderente alle necessità del paziente. I grandi centri di sanità privata potranno, pertanto, acquisire ulteriore potere con conseguente decremento della concorrenza, maggiori sovvenzioni, nonché controlli pressoché assenti.

Gli esercenti le professioni sanitarie dispongono delle facoltà di influenzare il procurement sia dal lato dell'offerta che della domanda. L'informazione scientifica non è sempre indipendente, proprio perché i conflitti di interessi possono minare la ricerca medica favorendo determinati studi e analisi scientifiche soltanto in base all'interesse personale. Difatti l'attività di ricerca è in ampia misura finanziata dai produttori di tecnologie o dalle case farmaceutiche, e l'informazione

scientifica è spesso condizionata dagli interessi dei produttori. Le stesse riviste scientifiche e biomediche, aventi ampio potere nell'orientare la ricerca e la sperimentazione, sono in gran parte sponsorizzate proprio dalle industrie farmaceutiche. Nella ricerca i maggiori problemi sono da riscontrare nel condizionamento da parte delle imprese farmaceutiche e manipolazione dei dati di analisi, per mezzo di sistemi corruttivi. Ciò si traduce, a livello di procurement, in procedure di gara non corrette o prioritariamente orientate, irregolarità nell'approvvigionamento, acquisti non necessari o fuori mercato. Il procurement deve sempre più rappresentare una funzione strategica basata sulla capacità di gestire gli approvvigionamenti sanitari in modo efficiente, evitando sprechi di denaro che possano nuocere al budget destinato alla spesa medica[380].

È proprio nel settore farmaceutico che si rileva il rischio maggiore, soprattutto nei passaggi della c.d. "catena del farmaco", poiché i ricavi delle imprese farmaceutiche dipendono dal rilascio dei permessi per la sperimentazione e distribuzione[381]. Tra i possibili eventi corruttivi in area sanitaria, è da porre particolare attenzione alla sempre più diffusa pratica del comparaggio, disciplinato dal Testo Unico delle Leggi Sanitarie e dal Codice del Farmaco, consistente nell'accordo collusivo tra operatore sanitario e case farmaceutiche, al fine di favorire la prescrizione di determinati farmaci o strumentazioni diagnostiche in luogo di altre, al solo scopo di agevolare l'indebito arricchimento e l'accrescimento di potere delle parti. Il comparaggio, nel caso in cui vi sia un accordo del medico o veterinario per ricevere denaro o altra utilità, costituisce una fattispecie di reato punita con l'arresto fino ad un anno ed un'ammenda[382]. Altre tipologie di

380 Con l'emergenza da Covid-19 si è reso evidente uno dei maggiori problemi del procurement sanitario nel nostro Paese: la mancata condivisione di azioni ed obiettivi dei diversi livelli di gestione degli acquisti, e l'assenza di una strategia comune. Secondo N. Cusumano, esperto in procurement sanitario e docente di "government, health and not for profit" presso SDA Bocconi School of Management "Gli acquisti in ambito sanitario avvengono a più livelli, ma il processo non è stato disegnato in modo strategico: ci sono le aziende sanitarie, le centrali di committenza regionali e Consip a livello nazionale, tre livelli di procurement che a volte non dialogano tra di loro".

381 Cfr. Calascibetta F., Davidde M., D'Orio D., Fahle S., Mancini A., Mercogliano M.R., Quercetti A.C., *Dalla farmacia territoriale alle grandi catene di distribuzione: origini, contesto attuale e sviluppo di nuovi scenari*, Fondazione ISTUD, 2015; Gotzsche P.C., *Medicine letali e crimine organizzato*, Fioriti Editore, 2016.

382 Testo Unico delle leggi sanitarie, R.D. 27 luglio 1934 n. 1265, articoli 170-172. Per l'art. 170 "Il medico o il veterinario che ricevano, per sé o per altri, denaro o altra utilità ovvero ne accettino la promessa, allo scopo di agevolare, con prescrizioni mediche o in qualsiasi altro modo, la diffusione di specialità medicinali o di ogni altro prodotto a uso farmaceutico, sono puniti con l'arresto fino a un anno e con l'ammenda da euro 206,58 a euro 516,45. Se il fatto violi pure altre disposizioni di legge, si applicano le relative sanzioni secondo le norme sul concorso dei reati. La condanna importa la sospensione dall'esercizio della professione per un periodo di tempo pari alla durata della pena inflitta". Anche il Codice del Farmaco, d.lgs. 24 aprile 2006 n. 219, punisce il comparaggio agli articoli 123 e 147 comma 5. Per l'art. 123 comma 1 "Nel quadro dell'attività di informazione e presentazione dei medicinali svolta presso medici o farmacisti è vietato concedere, offrire o promettere premi, vantaggi pecuniari o in natura, salvo che siano di valore trascurabile e siano comunque collegabili all'attività espletata dal medico e dal farmacista". Per l'art. 147 comma 5 "Chiunque, in violazione dell'articolo 123, comma 1, concede, offre o promette premi, vantaggi pecuniari o in natura, è punito con l'arresto fino ad un anno e con l'ammenda da quattrocento euro a mille euro. Le

illecito sono basate sulle frodi riguardo i rimborsi delle ricette da parte del Servizio Sanitario Nazionale a fronte di false prescrizioni. Di un approfondito controllo necessitano anche la gestione dell'assegnazione degli incarichi e le nomine, soprattutto nei periodi di transizione, nonché la gestione delle liste d'attesa. Quest'ultimo problema nasce dalla difficoltà del sistema sanitario pubblico di rispondere alle numerose richieste di prestazioni sanitarie, ed alla possibilità di alcuni soggetti di avvalersi di corsie preferenziali[383]. Fra le conseguenze di tale situazione, le crescenti richieste da parte dei pazienti alle strutture private, che vanno così a sostituirsi a quelle pubbliche con acquisizione sproporzionata di poteri e risorse.

Il rischio che interessi individuali possano essere lesivi di quelli pubblici e generali, ovvero di soggetti più deboli quali i pazienti meno abbienti, è stato evidenziato anche dall'ONU che, nel decalogo stilato nel Global Corporate Sustainability Report, ha posto l'accento sull'impegno contro la corruzione in ogni sua forma e manifestazione. In maniera ancor più esplicita l'ISM, Institute for Supply Management[384], nel definire i princìpi cui devono attenersi i professionisti del procurement management ha indicato, quali punti fondamentali, il contrasto alla corruzione, assunzione di un comportamento etico, trasparenza nei rapporti, promozione di salute e sicurezza.

Nell'ambito degli appalti, in sanità vi è una maggiore esigenza di affrontare in modo sistemico i conflitti di interessi, proprio perché vengono coinvolti valori essenziali e di livello primario[385]. È, pertanto, necessario predisporre misure per una corretta gestione dei conflitti, basate sulla prevenzione degli stessi grazie alla divulgazione di informazioni, una normativa chiara e difficile da eludere, una cultura etica e deontologica da diffondere e far rispettare da parte degli ordini professionali. Sono, dunque, necessarie: misure preventive fondate sulla responsabilizzazione dei professionisti; misure deterrenti tramite la costituzione di comitati etici; misure repressive sia all'interno dell'ordine professionale, con la possibilità di radiazione dall'albo, che giudiziale. A tale

stesse pene si applicano al medico e al farmacista che, in violazione dell'articolo 123, comma 3, sollecitano o accettano incentivi vietati. La condanna importa la sospensione dall'esercizio della professione per un periodo di tempo pari alla durata della pena inflitta".

[383] Secondo l'ultimo paper del Censis "Il quadro delineato mette in luce un sistema con evidenti elementi di opacità che favoriscono comportamenti opportunistici e l'uso inappropriato delle risorse".

[384] L'Institute of Supply Management (ISM), precedentemente noto come Associazione nazionale di gestione degli acquisti (NAPM), è un'organizzazione che offre agli specialisti della catena di approvvigionamento la possibilità di ricevere la certificazione della catena di approvvigionamento. A partire dal 2010, ISM conferisce due tipi di certificazioni: Certified Professional in Supply Management (CPSM) e Certified Purchasing Manager (CPM).

[385] Sugli appalti in sanità: De Nictolis R., *Gli appalti pubblici dell'emergenza sanitaria*, Zanichelli Editore, 2021.

riguardo è opportuno rimarcare l'importanza di strumenti di soft-law, quali linee guida e codici deontologici, a volte più efficaci di norme giuridiche ed atti legislativi. Le situazioni a rischio di conflitto devono essere gestite dalle aziende sanitarie in modo che i contatti con gli operatori economici da parte dei medici siano sempre ed in ogni punto regolamentati in termini di procedure e linee guida, così da non lasciare nulla al libero arbitrio dei soggetti coinvolti. Ciò può avvenire favorendo un interessamento diretto dell'azienda nelle procedure delle gare d'appalto, e non limitandosi al coinvolgimento del singolo professionista, che potrebbe essere in una situazione di conflitto d'interessi, ovvero oggetto di offerte illecite da parte degli interessati. Maggiori controlli e verifiche necessitano, infine, gli appalti in house, aggiudicati in deroga ai princìpi di concorrenza, non discriminazione e trasparenza, tramite un affidamento diretto da parte dell'Amministrazione ad una società esterna che presenti caratteristiche tali da poterla qualificare come una derivazione dell'ente stesso, da cui è interamente controllata[386].

I Paesi come l'Italia, ad alto rischio di corruzione[387] e con presenza di elevate concentrazioni di conflitti di interessi, sono stati maggiormente colpiti da fenomeni quali: ingerenza politica nelle nomine, pantouflage o revolving doors, spoils system. Per ciò che riguarda l'ingerenza politica nelle nomine, uno dei settori maggiormente interessati è proprio quello sanitario. Si è tentato, invero, più volte di disincentivare il rapporto sanità-politica nelle nomine di direttori generali delle ASL, primari, e più in generale di posti di maggior rilievo e potere nella sanità[388]. Tuttavia le norme per prevenire o reprimere tali pratiche sono risultate isolate, poco convincenti e facilmente eludibili. Gli strumenti messi a disposizione a tal fine, hanno difatti sortito effetti pressoché irrilevanti, nonché poco duraturi.

A rendere più complessa la soluzione di tale problema è, indubbiamente, la irrazionale ripartizione di poteri, operata dal Titolo V della Costituzione fra Stato e Regioni, in materia di sanità pubblica. Ciò ha reso più complessa l'identificazione di responsabilità e di connessioni fra

[386] Sullo specifico argomento degli appalti in house: Resta E., *Gli appalti in house. Il caso delle sanità service*, Cacucci, 2018.

[387] Secondo l'Ocse la corruzione nella sanità italiana fa sì che: "Una parte significativa della spesa sanitaria è – nella migliore delle ipotesi – spreco, o peggio danneggia la nostra salute".

[388] Un tentativo, non riuscito, di arginare il fenomeno si è avuto con l. 189 del 2012, che ha introdotto una diversa procedura per la nomina dei direttori generali delle ASL. Il d.lgs. n. 39 del 2013 ha disposto in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni, non riuscendo, tuttavia, ad incidere in alcun modo sull'ingerenza della politica nelle nomine. La giurisprudenza è orientata nel senso della fiduciarietà dell'incarico dirigenziale ed ha informato le proprie pronunce al rispetto dell'ampia discrezionalità riconosciuta nell'individuazione del soggetto da incaricare (Consiglio di Stato, sez. IV, n. 3649 del 2000).

organi deputati alle nomine e soggetti nominati, ed un allargamento e sovrapposizione di poteri, già di per sé di difficile controllo. La riforma costituzionale avvenuta con la legge n. 3 del 18 ottobre 2001, ha affidato la tutela della salute alla legislazione concorrente tra Stato e Regioni, delineando un sistema caratterizzato da un pluralismo di centri di potere. L'art. 117 della Costituzione, nello stabilire che lo Stato mantiene la competenza legislativa esclusiva nelle materie specificamente elencate, mentre le Regioni possono legiferare nelle materie di competenza concorrente, nel rispetto dei princìpi fondamentali definiti dallo Stato, ha di fatto finito per generare una deriva regionalista, con una frammentazione di sistemi sanitari dove l'accesso a servizi e prestazioni sanitarie è profondamente diversificato e iniquo. Infatti, Le diseguaglianze regionali e locali dimostrano che l'universalità e l'equità di accesso ai servizi sanitari, la copertura in base alle necessità assistenziali dei cittadini e la portabilità dei diritti in tutto il territorio nazionale, non configurano il quadro reale della situazione, ed hanno dato vita a maggiori speculazioni ed espansione dell'illiceità e del malaffare[389].

Illegalità e corruzione non sono sinonimi di conflitto d'interessi: i primi sono rappresentati da illeciti, anche di rilevanza penale nel caso della corruzione, mentre il conflitto d'interessi non rappresenta necessariamente uno sconfinamento nell'illegalità e nella condotta penalmente rilevante. Esso può coinvolgere anche elementi al di fuori del giuridico, quali l'etica, la deontologia e l'opportunità. Anche in sanità il tema della legalità e quello della corruzione sono, tuttavia, strettamente connessi e speculari al problema irrisolto del conflitto d'interessi. Secondo la "Rete europea contro le frodi e la corruzione nel sistema sanitario" in Europa i fenomeni di corruzione in sanità gravano in ragione del 5,6% del totale dei fondi destinati ai servizi sanitari di primaria necessità. Il problema si ingigantisce se esaminiamo il sistema italiano, notoriamente ad alto tasso di corruzione. Quest'ultima si insinua in modalità multiforme nel nostro sistema sanitario, dagli appalti all'abusivismo professionale, dalle pratiche per l'accreditamento ai pagamenti delle forniture.

Il costo elevato della corruzione ha richiesto per decenni un impianto legislativo che potesse restituire credibilità al Paese, incentivare gli investimenti e riavviare lo sviluppo economico. Solo nell'ultimo decennio è stato apprezzabile lo sforzo nel varare alcune disposizioni al fine di porre un freno all'ormai dilagante ed incontrollato fenomeno della corruzione. L'illegalità ha prodotto

[389] Cfr Cartabellotta N., *Diritto alla salute e riforma del Titolo V*, in *Salute Internazionale*, maggio 2015.

effetti indiretti anche sulla tutela della salute, riducendo l'accesso ai servizi per i pazienti con conseguente aumento dell'indice di mortalità. A tale scopo il contrasto all'illegalità in sanità costituisce un impegno primario, soprattutto in conseguenza alla grave pandemia che ha colpito l'intero pianeta. È, pertanto, importante una legislazione chiara e precisa che individui conflitti d'interessi dettati da un mero legame conflittuale, comportamenti scorretti o inopportuni deontologicamente e comportamenti illeciti, in quanto contrari ad una norma giuridica. È, tuttavia, opportuno rimarcare che anche quando il conflitto d'interessi non sfocia in comportamenti illeciti può, comunque, danneggiare il sistema sanitario e tutti i cittadini, con spese improprie, nonché ricerca ed informazione scientifica manipolate e pilotate da produttori di tecnologie farmaceutiche. I c.d. "drivers" di corruzione in sanità, ossia le vulnerabilità da cui possano derivare rischi di corruzione[390] sono:

a. incertezza o debolezza del quadro normativo;
b. asimmetria informativa tra utente e sistema sanitario e tra sistema sanitario e fornitori privati;
c. elevata parcellizzazione della domanda sanitaria;
d. fragilità nella domanda di servizi di cura;
e. forte ingerenza della politica nelle scelte tecnico-amministrative;
f. elevata complessità del sistema;
g. ampi poteri e discrezionalità nelle scelte aziendali e ospedaliere;
h. basso livello di accountability del personale pubblico;
i. bassi standard etici degli operatori pubblici;
j. crescita della sanità privata;
k. scarsa trasparenza nell'uso delle risorse.

Tutto ciò ha portato a serie problematiche del settore sanitario, quali:

a. ricerca scientifica fittizia;
b. prescrizioni mediche non necessarie;
c. gare orientate, inutili, o con procedure scorrette o irregolari;
d. false attestazioni di forniture;

[390] Studio sviluppato da RiSSC e Transparency International Italia, nell'ambito del progetto "Unhealthy Health System".

e. prescrizioni a pazienti fantasma;
f. dirottamenti verso la sanità privata;
g. monopoli e cartelli;
h. ostacolo all'ingresso nel mercato di piccole realtà sanitarie o farmaceutiche;
i. eccessiva discrezionalità degli amministratori;
j. prestazioni degli specialisti erogate in regime di intramoenia con conseguente falsità delle dichiarazioni.

La sanità è uno dei settori che ha maggiormente beneficiato della rete di vigilanza anticorruzione predisposta dalla Legge 190 del 2012 o legge Severino[391], articolata sia a livello centrale e nazionale fino ai livelli locali e aziendali. Essa ha avuto il merito di rafforzare strutture già esistenti, creando e potenziando, altresì, nuovi organismi di controllo quali l'ANAC. La legge c.d. anticorruzione, orientata al contrasto alla corruzione nella pubblica amministrazione ha, fra i suoi punti di forza, l'introduzione tra i dirigenti amministrativi della figura del "Responsabile della prevenzione della corruzione e della trasparenza" il quale risponde personalmente con sanzioni in caso di inadempienza, le disposizioni in materia di trasparenza (all'art. 1 commi 15-39) ed in materia di conflitto d'interessi (art. 1, commi 40-43), ed una nuova disciplina per la tutela del dipendente che segnala gli illeciti nella P.A. (comma 51). Viene, infine, favorito il sistema della rotazione degli incarichi dei dirigenti di settori particolarmente esposti alla corruzione.

Recentemente, in Italia, la politica si è posta delle solide basi da cui partire per limitare il problema della corruzione e del conflitto di interessi nel procurement sanitario, prevedendo l'utilizzo di sistemi informatici avanzati e scambio di informazioni su piattaforme on-line che favoriscano la trasparenza delle operazioni. Nella seduta della Camera dei Deputati n. 898 del 2017[392] si affermava riguardo il procurement sanitario "è necessario implementare sistemi uniformi di controllo esterno ed informatizzati che consentano di rilevare, sulla base di indici di rilevazione automatizzati, l'esistenza di anomalie negli acquisti tali da rappresentare un allarme di spreco, inefficienza o corruzione; il sistema dovrebbe essere integrato con un programma operativo contabile e patrimoniale, unico per tutte le strutture sanitarie del territorio nazionale, che consenta ai cittadini, attraverso un'interfaccia accessibile a chiunque, di indagare, in tempo reale,

[391] Supra, capitolo 1, par. 1.2.1.
[392] Testi allegati all'ordine del giorno della seduta della Camera dei Deputati n. 898 del 2017, *Mozioni concernenti iniziative volte a contrastare il fenomeno della corruzione in ambito sanitario*.

l'intera filiera". Una delle conclusioni più significative della predetta seduta della Camera stabilisce la necessità di "contrastare fenomeni corruttivi in ambito sanitario, a diffondere ed incentivare con tecnologie e con metodi innovativi l'utilizzo degli open data (tutte le informazioni devono essere trasparenti e accessibili) e la semplificazione di tutte le procedure, anche nell'ambito della open government partnership, promuovendo così la cultura della trasparenza nella pubblica amministrazione, poiché trasparenza, accountability e partecipazione devono essere obbiettivi fondamentali per un'azione di Governo contro la corruzione"[393].

La trasformazione digitale in ambito sanitario, tuttora in corso, ha effettivamente avuto un'accelerazione, non solo per ciò che attiene all'individuazione e prevenzione di fenomeni corruttivi e conflitti d'interessi, ma ancora più a monte, nella formazione degli atti da cui potrebbero derivare attività illecite. Ci si riferisce, in particolare all'utilizzo sempre più diffuso degli innovativi smart contract[394], contratti intelligenti che vengono creati in automatico necessitando della sola sottoscrizione dei contraenti, qualora alcune condizioni siano soddisfatte. Il succitato impiego delle tecnologie informatiche avanzate e dell'intelligenza artificiale nella lotta preventiva alla corruzione in ambito sanitario rafforza notevolmente i sistemi sanitari, giacché le condizioni riguardanti il conflitto di interessi vengono automaticamente verificate divenendo *condicio sine qua non* della stipulazione dei contratti. Tale sistema consente, inoltre, il tracciamento protetto ed immodificabile delle informazioni, nel rispetto del diritto alla privacy, grazie all'utilizzo della già citata tecnologia blockchain[395].

La legge anticorruzione del 2012 e le normative emanate negli anni successivi rappresentano indubbiamente una pietra miliare ma non sono sufficienti, pertanto diventa importante il ruolo della deontologia e dell'etica sanitaria, con il conferimento di maggiori poteri agli organi di controllo per il rispetto dei Codici deontologici e di comportamento, del Regolamento Aziendale, delle misure generali e specifiche previste dall'ANAC e dalle singole strutture. Manca, tuttavia, una normativa che regolamenti le relazioni fra aziende farmaceutiche, medici e organi della sanità pubblica, rendendole trasparenti al fine di evitare casi di collusioni illecite o di malasanità, quali l'iperprescrizione di farmaci. Nell'attuale sistema, inoltre, i piani delle amministrazioni evidenziano carenze riguardo i processi interni, la capacità di individuare e gestire i rischi, di

[393] Id.
[394] Cfr. Battaglini R. - Giordano M.T. (a cura di), *Blockchain e smart contract*, Giuffré Editore, 2019.
[395] Supra, capitolo 2, par. 2.2.2.

assicurare la trasparenza e contrastare la corruzione. Necessitano, pertanto, di un maggior impegno da parte di tutti i soggetti coinvolti, ma soprattutto di maggiori investimenti riguardo all'utilizzo di moderne tecnologie ed il loro orientamento verso l'efficienza e la legalità del sistema sanitario, nonché nella istruzione e formazione del personale.

4.2.4. Conflitto di interessi in sanità: l'inchiesta "Camici"

Una recente vicenda emblematica dello stretto legame fra appalti pubblici in sanità e conflitto di interessi, e della facilità con cui quest'ultimo possa eventualmente tramutarsi in comportamenti penalmente rilevanti, riguarda il coinvolgimento del Presidente della Regione Lombardia, Attilio Fontana, nella c.d. inchiesta Camici. Secondo l'accusa vi era stato un accordo collusivo fra Fontana e suo cognato Andrea Dini, per una fornitura di camici durante l'emergenza per la pandemia da Covid-19, da parte della società Dama S.p.A., gestita da quest'ultimo. Nello specifico, la vicenda riguarda l'affidamento del 16 aprile 2020 alla predetta società, della fornitura per un importo di oltre mezzo milione di euro, di camici ed altri dispositivi di protezione individuale. A parere dei Pubblici ministeri "si anteponevano all'interesse pubblico, l'interesse e la convenienza personali del Presidente di Regione Lombardia", il quale da "soggetto attuatore per l'emergenza Covid […] ingeriva nella fase esecutiva del contratto in conflitto di interessi". Il Presidente Fontana e gli altri indagati, ossia il cognato Dini, il vicesegretario generale della Regione, l'ex direttore e una dirigente di Aria (Centrale Acquisti Regione Lombardia) vengono, così, accusati di frode nelle pubbliche forniture, reato previsto e punito ex art. 356 c.p.[396]. La fornitura a titolo oneroso veniva, poi, trasformata in donazione parziale[397], a parere della Procura al solo scopo di coprire il reato.

Il conflitto di interessi oggetto della questione è di quelli più diffusi e facili da individuare, poiché derivante da rapporti di parentela, facilmente identificabili e dimostrabili. Difatti nel favorire la Dama S.p.A., emergeva un conflitto di interessi con un coinvolgimento ancor più ampio del Presidente, poiché anche sua moglie possedeva il dieci per cento delle quote societarie della stessa. Secondo quanto ricostruito nell'indagine, nel tentativo di risarcire il cognato per il mancato introito dei camici, Fontana effettuava un bonifico di 250 mila euro da un suo conto in Svizzera,

[396] A norma dell'art. 356 c.p. "Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente".

[397] La donazione fu bloccata dall'ufficio legale della Centrale Acquisti di Regione Lombardia (Aria), poiché essendo donazione di "non modico valore" avrebbe necessitato di atto pubblico notarile.

bloccato in quanto l'operazione veniva segnalata come sospetta dall'Unità di informazione finanziaria della Banca d'Italia. Da ciò nasceva un nuovo filone di indagini a carico del Governatore, successivamente archiviato, per i reati di autoriciclaggio e falso nella voluntary.

A prescindere dalla vicenda giudiziaria, che ha visto tutti i soggetti coinvolti prosciolti all'udienza preliminare perché il fatto non sussiste[398], il punto centrale del c.d. caso Camici ai fini della presente ricerca attiene strettamente alle conseguenze del conflitto di interessi nel procurement pubblico, in grado di eludere la regolamentazione sui contratti pubblici, e nello specifico la procedura negoziata per l'acquisto, nonché la concessione di autorizzazioni riguardanti i dispositivi di protezione individuali ad uso medico, generalmente soggetti a complesse procedure. L'affidamento diretto della commessa alla società gestita dal cognato del Presidente della Regione Lombardia, la quale non era presente nell'elenco ufficiale dei fornitori della Regione, è stato svelato da un'inchiesta della trasmissione Report. A questo punto ci si chiede perché sia stata un'inchiesta giornalistica ad avere ricoperto una funzione di impulso nell'emersione del conflitto di interessi, e non le autorità di controllo preposte a tale compito, che avrebbero invece dovuto vigilare, in via preventiva, per ciò che concerne vicende quanto meno di dubbia chiarezza. Con particolare riguardo al caso in esame, l'emersione del conflitto di interessi sarebbe stata di agevole rilevabilità ancor prima della *notitia criminis*, non solo per la notorietà dei soggetti coinvolti e per gli stretti rapporti endofamiliari fra gli stessi, ma anche per le palesi anomalie nella procedura d'appalto, nonché per l'importanza dei beni oggetto della commessa. Il tutto, poi, in un periodo storico in cui, stante l'incremento dei casi di Covid-19 e la necessità di forniture mediche specifiche, si sarebbero dovuti effettuare controlli serrati da parte degli organi preposti. Nel contrasto al conflitto di interessi e alle attività illecite e corruttive nel procurement pubblico, la fase più importante è proprio quella della sorveglianza e del controllo, al fine di destare una maggior fiducia delle imprese nelle gare d'appalto, nonché efficienza e trasparenza dell'amministrazione. A tal fine è necessario che le autorità deputate al controllo del conflitto di interessi e delle irregolarità negli appalti, vengano messe nelle condizioni di operare in maniera efficace nell'emersione di tutte quelle situazioni a rischio, soprattutto in settori di rilevanza costituzionale come la sanità pubblica.

[398] Tuttavia la vicenda non è ancora conclusa, poiché la Procura di Milano ha depositato un ricorso nei confronti della sentenza di non luogo a procedere del Giudice dell'Udienza Preliminare dott. Chiara Valori.

4.3. Individuazione del conflitto di interessi in sanità

4.3.1. Gestione del conflitto d'interessi nella sanità pubblica

Il Forum per l'integrità in sanità, l'ANAC e l'Istituto Superiore di Sanità, hanno in più occasioni evidenziato che il procurement nella sanità pubblica sia uno dei settori più sensibili a corruzione e conflitti di interessi[399]. In base ai dati analizzati da Euros for Docs, in Italia circa un miliardo di euro è stato speso da parte delle più grandi aziende farmaceutiche per ottenere favori da operatori e organizzazioni sanitarie nel triennio 2017-2019. La trasparenza dei rapporti dei produttori di apparecchiature mediche e di farmaci, con il personale sanitario e le strutture sanitarie, è il principale elemento per garantire che gli interessi privati e il tornaconto personale non prevalgano sulla salute dei cittadini e sul benessere dei pazienti[400], fornendo agli organi di controllo gli strumenti per prevenire e contrastare conflitti di interessi e malaffare. Per potenziare la trasparenza, nonché la prevenzione delle situazioni di conflitto di interessi, è pertanto necessaria la conoscenza dei rapporti nel procurement intercorrenti tra le imprese produttrici e i soggetti operanti nel settore della salute. Tale conoscenza può essere ottenuta attraverso la creazione di un registro pubblico telematico in cui tutte le informazioni riguardanti la promozione e lo sviluppo dei prodotti farmaceutici e sanitari, sono raccolte e rese disponibili in modalità open access, aperta a tutti. Nel 2016 l'associazione delle imprese del farmaco, Farmindustria, ha adottato un codice deontologico che richiede a tutte le aziende associate la pubblicazione dei dati sui trasferimenti di valore verso professionisti e aziende sanitarie. Tuttavia, non essendovi obblighi giuridici in tal senso, il 45 per cento delle società facenti parte dell'associazione non ha pubblicato tali informazioni, rendendo inefficace l'autoregolamentazione.

La gestione del conflitto d'interessi nel procurement pubblico richiede un impegno sia del sistema sanitario, a tutti i livelli, che delle aziende coinvolte nelle gare ad evidenza pubblica. Sarebbe necessario, secondo Transparency International Italia e REACT[401]: un migliore tracciamento dei trasferimenti di valore in tutti i loro passaggi, dall'erogatore iniziale fino al beneficiario finale,

[399] Secondo Transparency International Italia in sanità avviene il 17,33 per cento dei casi di corruzione, mentre una ricerca di REACT rileva che il 95 per cento degli operatori sanitari considera che vi sia ampia diffusione della corruzione in Italia.

[400] La trasparenza nei rapporti fra aziende sanitarie e imprese è alla base del c.d. Sunshine Act, il disegno di legge approvato dal Senato il 23 febbraio 2022, sostenuto da Transparency International e REACT.

[401] Nel Forum per l'Integrità in Sanità, Transparency International Italia e REACT hanno pubblicato un policy paper contenente osservazioni e proposte rivolte ai decisori pubblici per rendere più efficace la trasparenza dei rapporti tra pubblico e privato e favorire la prevenzione dei conflitti di interesse ed il miglioramento del Sistema Sanitario.

indicando eventuali intermediari; l'abbassamento delle soglie di valore oltre le quali è previsto l'obbligo di dichiarazione dei trasferimenti; l'estensione dell'oggetto della trasparenza anche agli accordi che producono vantaggi non monetizzabili; l'indicazione dell'organizzazione di appartenenza dell'operatore sanitario in modo da avere un tracciamento completo; la predisposizione di un registro pubblico telematico che sia interoperabile con altri dataset. Anche l'Istituto Superiore di Sanità considera la trasparenza, l'interscambio e il tracciamento delle informazioni, un elemento primario per il contrasto di fenomeni di illiceità e conflitti di interessi[402].

In particolare è necessario che le aziende sanitarie agenti in qualità di amministrazioni aggiudicatrici nelle procedure di appalto, prestino particolare attenzione ai rapporti fra gli operatori economici e i dipendenti dell'amministrazione stessa, al fine di ridurre il rischio che si verifichino situazioni di conflitto di interessi nel corso della procedura di gara nonché di esecuzione del contratto. È lo stesso Codice dei contratti pubblici a richiedere, all'art. 42 comma 1, che le amministrazioni aggiudicatrici adottino misure atte ad individuare e prevenire il conflitto di interessi, in un contesto di trasparenza e parità di trattamento a vantaggio di tutte le parti[403]. Obiettivo della strategia di prevenzione è, difatti, non solo la regolarità dell'azione amministrativa, ma anche la salvaguardia degli interessi delle Aziende Sanitarie e dei partecipanti alla gara d'appalto, nonché la tutela degli stessi dipendenti delle amministrazioni aggiudicatrici da possibili successive accuse di conflitti di interessi o di mancata comunicazione di essi. Ai soggetti coinvolti nei vari processi decisionali si chiede di firmare una dichiarazione di assenza di conflitto di interessi prima della nomina, ovvero appena prendono parte alla procedura. Tale dichiarazione ha lo scopo principale di creare una base giuridica di assunzione di responsabilità, grazie alla quale diviene possibile perseguire coloro[404] che altrimenti non potrebbero essere incriminati o sanzionati per il solo fatto di trovarsi in una posizione di conflitto di interessi senza averlo dichiarato. La dichiarazione contiene l'identificativo del firmatario e della procedura in questione, la sua posizione in seno all'organizzazione e la sua posizione nella procedura d'appalto, la

[402] ISS, Allegato n. 1, Delibera n. 16 del C.d.A. del 09.10.2018, p. 3.

[403] Il d.lgs. n. 50 del 2016 all'art 42 co 1 dispone che "Le stazioni appaltanti prevedono misure adeguate per contrastare le frodi e la corruzione nonché per individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione degli appalti e delle concessioni, in modo da evitare qualsiasi distorsione della concorrenza e garantire la parità di trattamento di tutti gli operatori economici".

[404] A livello amministrativo e disciplinare possono essere applicate sanzioni quali l'obbligo di astensione delle procedure d'appalto, la sospensione dal lavoro, il richiamo scritto. Diversa è la questione sul piano penalistico. Il conflitto di interessi non è perseguibile penalmente, ma è possibile perseguire per false attestazioni o dichiarazioni coloro che autocertificano falsamente di non avere conflitti di interessi, accertati invece dalla magistratura.

dichiarazione di non trovarsi in situazione di conflitto di interessi reale, potenziale o apparente, l'assunzione di responsabilità in riferimento alle norme, alle conseguenze ed alle sanzioni previste in materia di falsità ideologica nelle dichiarazioni. Dal momento che le situazioni di conflittualità possono mutare, è importante che le dichiarazioni di assenza di conflitti di interessi siano periodicamente verificate e aggiornate.

L'individuazione delle situazioni di conflitto di interessi può avvenire tramite gli strumenti di controllo e di verifica presenti in ogni amministrazione e di cui sono dotate anche autorità di controllo esterne, comprese le procure della Repubblica. I controlli possono essere effettuati a campione, ovvero possono essere mirati ogni qual volta vi siano dubbi circa la sussistenza di situazioni di conflitto di interessi, anche in considerazione delle autocertificazioni di assenza di conflitto effettuate dallo stesso dichiarante. Nella maggior parte dei casi, tuttavia, le segnalazioni provengono da soggetti interni all'amministrazione stessa, quali colleghi o superiori gerarchici, ovvero anche da soggetti esterni alla Pubblica Amministrazione. Particolare impegno al fine del contrasto alle situazioni di maladministration in sanità deve, poi, essere profuso nella possibilità di individuare i conflitti di interessi nel procurement sanitario, grazie all'utilizzo della tecnologia, tramite l'analisi di dati incrociati fra loro e processati al fine di scoprire aree e soggetti in cui il conflitto può avere una deriva verso la corruzione. Ove la situazione di conflitto di interessi non sia provata, ovvero vi siano soltanto dei dubbi circa l'imparzialità di un dipendente dell'amministrazione aggiudicatrice, l'esclusione dalla procedura, a scopo preventivo e di immagine sia dell'amministrazione che del dipendente stesso, appare una misura idonea in un contesto di trasparenza e buona fede. Ogni azione intrapresa in risposta a situazioni di conflitto di interessi deve essere annotata in un registro speciale, nella piena disponibilità degli organismi esterni di controllo. Inoltre è buona prassi di ogni amministrazione sanitaria, la conservazione della documentazione di eventuali conflitti di interessi per dimostrare come sono stati affrontati, nonché avere un punto di riferimento per i futuri casi analoghi.

4.3.2. Linee guida ANAC per le professioni sanitarie

Le linee guida per l'adozione dei codici di comportamento nel Servizio Sanitario Nazionale, prodotte da ANAC[405], AGENAS[406] e Ministero della Salute, sono un utile strumento di prevenzione

[405] Approvate in via definitiva nell'adunanza del 29 marzo 2017, con delibera n. 358 "Linee Guida per l'adozione dei Codici di comportamento negli enti del Servizio Sanitario Nazionale".
[406] Agenzia Nazionale per i servizi sanitari regionali.

alla corruzione ed individuazione e gestione delle situazioni di conflitto d'interessi. Oltre al rispetto degli obblighi di dichiarazione di assenza di conflitto di interessi, le raccomandazioni assicurano la tutela dei soggetti che, al di fuori delle responsabilità penali per calunnia o diffamazione, segnalino alle autorità preposte illeciti di cui siano venuti a conoscenza in ragione della loro attività lavorativa (c.d. whistleblowing). È, poi, ribadito il divieto di accettare regalie, compensi ed altre utilità, al di fuori dei casi espressamente consentiti dai relativi regolamenti, consistenti generalmente in beni di modesto valore. Il codice di comportamento deve prevenire ogni situazione foriera di conflitto d'interessi, tramite la comunicazione al responsabile dell'ufficio preposto. Deve, inoltre, prevedere procedure univoche per la gestione del conflitto di interessi e comunicazioni tempestive, non oltre dieci giorni dal momento in cui il conflitto potenziale o attuale si è manifestato. Gli obblighi del RPCT non sono soltanto di controllo e vigilanza, ma si estendono anche alle fasi successive, ed in particolare all'adozione dei provvedimenti conseguenti situazioni di conflitti d'interessi.

La valutazione sul potenziale conflitto di interessi deve essere effettuata caso per caso, anche con riguardo al diritto di far parte di associazioni o organizzazioni che possano avere interessi in una determinata procedura. Le strutture sanitarie dovrebbero, poi, mappare preliminarmente gli ambiti di attività che, in quanto parzialmente coincidenti con le funzioni proprie dell'Ente sanitario, potrebbero determinare situazioni soggettive di conflitto di interessi. I codici di comportamento degli Enti del SSN devono vietare: di porre in essere comportamenti, anche al di fuori dell'orario lavorativo, che possano pregiudicare gli interessi dell'amministrazione o nuocere alla sua immagine; di influenzare la gestione non corretta di pratiche dell'ufficio; di anticipare o diffondere gli esiti dei procedimenti di gara, di concorso, o di selezione pubblica prima che siano conclusi e ne sia stata data pubblicizzazione. In riferimento al conflitto di interessi, i codici devono invece contenere i seguenti obblighi: riportare nelle comunicazioni tutti gli elementi idonei all'individuazione del responsabile dell'attività amministrativa; pubblicizzare la conoscenza dei sistemi aziendali per la gestione dei rischi contenuti nel Documento di Valutazione dei Rischi; porre in essere misure di trasparenza volte a tracciare i contatti tra i professionisti e i soggetti incaricati dalle suddette aziende; indicare agli addetti URP le modalità di gestione delle segnalazioni da parte degli utenti. I codici devono contenere, altresì, indicazioni specifiche riguardo: l'obbligo per il personale sanitario di tenere distinte attività istituzionale e attività libero professionale; il divieto di condizionare il paziente orientandolo verso la visita in regime di libera professione; l'obbligo del medico di garantire la tracciabilità delle somme incassate nell'attività

libero professionale intramuraria; il divieto di percepire corrispettivi nell'esercizio delle proprie funzioni istituzionali che non siano consentiti dalla legge, nonché autorizzati dalla propria azienda; il richiamo all'osservanza dei principi deontologici e di imparzialità nella prescrizione di farmaci e prodotti terapeutici diversi dai farmaci.

Con specifico riferimento alle attività negoziali, al fine di favorire la trasparenza e la regolarità delle gare, viene fatto divieto di inserire nei capitolati speciali caratteristiche tecniche non oggettivamente giustificate. Il codice di comportamento deve fare riferimento al divieto di chiedere o accettare *benefit* impropri per uso privato, quali: eccedenze di fornitura; campioni gratuiti di beni in quantità superiore a quanto previsto dalla normativa; regali che, seppur con valore al di sotto della soglia consentita, siano percepiti dal ricevente di valore superiore o elargiti con ricorrenza; comodati d'uso che non siano stati autorizzati dalla direzione aziendale; benefici economici a qualunque titolo derivanti dall'instaurarsi di relazioni extra ufficio. Con riguardo alla vigilanza e monitoraggio le singole amministrazioni devono far sì che i responsabili delle strutture predispongano una relazione annuale da consegnare all'UPD e al RPCT, nella quale venga dato atto delle segnalazioni relative a condotte illecite o situazioni di conflitto di interessi.

4.4. Nuove tecnologie e protezione dei dati sanitari

4.4.1. Tutela dei dati in sanità

Le informazioni personali di carattere particolare, così definite dagli artt. 9 e 10 del Regolamento UE 2016/679 (GDPR), rappresentano la sfera più intima e delicata della persona, ragion per cui è fondamentale garantire un quadro di tutele, etiche e legislative, utili a conservare la dignità e la libertà delle persone fisiche.

L'assistenza sanitaria è considerata una delle più grandi industrie intensive di dati. Grandi quantità di informazioni, riferite allo stato di salute dei cittadini, sono trattate dalle strutture sanitarie al fine di migliorare il percorso di cura degli assistiti: questa mole di dati viene definita "health big data". Si è in presenza di un fenomeno dalle dimensioni vastissime, per il quale il legislatore e i tecnici informatici devono, e dovranno sempre più prodigarsi per consentire un uso etico e funzionale dei big data. Il Codice in materia di protezione dati, con la sua ultima modifica, nella parte avente ad oggetto la ricerca scientifica, riprende i principi espressi dall'art. 89, paragrafo 1 del GDPR, nella parte in cui si prevede che "il trattamento a fini di archiviazione nel pubblico

interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato" e dal Considerando 33 che espressamente prevede che "dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica". Esemplare è lo studio condotto dal McKinsey Global Institute, secondo il quale se il sistema sanitario degli Stati Uniti utilizzasse i big data in maniera funzionale per garantire qualità ed efficienza nel percorso diagnostico degli assistiti, lo stesso sistema ne trarrebbe un valore stimabile intorno ai 300 miliardi di dollari per ogni anno e la spesa sanitaria verrebbe abbattuta di circa l'8%.

L'analisi dei big data analytics comprende il processo di estrazione di conoscenza da grandi porzioni di informazioni, dalla cui adozione derivano serie criticità legate alla gestione dei dati, alla loro complessità, all'onerosità e all'indisponibilità di soluzioni computazionali messe ancor più in evidenza in un settore particolarmente delicato quale quello della ricerca sanitaria. La soluzione alle problematiche prospettate risiede nella progettazione e nella standardizzazione di procedure analitiche, il cui sviluppo favorirebbe sia l'adozione di nuovi modelli che i flussi di lavoro fruibili dal personale addetto. Inoltre, si consideri che la crescita costante dei big data implica che i grandi volumi di dati sanitari siano continuamente generati ed incrementati in tempi molto brevi. Una analisi effettuata dalla School of Health Information Science della University of Victoria ha portato, conseguentemente ad uno studio comparativo delle ricerche scientifiche effettuate dalla comunità, all'adozione di cinque passi, che di seguito si analizzeranno, per la creazione di una struttura da utilizzare come linea guida negli "Health Big Data Analytics".

Il primo passo, la *data aggregation*, per il trasferimento dei dati attraverso networks che rappresentano una significativa sfida in ordine alle criticità della data protection e della sicurezza informatica. Secondo il succitato studio, una soluzione potrebbe essere rinvenibile nell'adozione di programmi di trasferimento file ad alta velocità attraverso reti di lavoro di ultima generazione o sistemi di compressione dei dati che consentano un livello di velocità molto alto nello scambio (inteso come trasferimento) dei dati. Il secondo passo riguarda la manutenzione dei dati. Le possibili soluzioni prospettate possono essere, ad esempio, il *cloud computing*, il *grid computing* e altri sistemi di conservazione dei big data, con un archivio dei dati disponibile su richiesta. Con riferimento alla protezione dei dati e alla sicurezza delle informazioni, i dati conservati localmente non sono, di default, più sicuri di quelli contenuti nel cloud, poiché nella maggioranza dei casi si

tratta di grandi colossi quali, ad esempio, Google, Micorosft e Amazon, che hanno destinato considerevoli investimenti in denaro agli aspetti di sicurezza, allo scopo di prevenire criticità in ordine alla protezione dei sistemi informativi. Molti fornitori di servizi cloud replicano i dati degli utenti in più località fisiche al fine di incrementare la ridondanza e l'indipendenza nel caso di eventuali avarie del sistema, innalzando, così, anche i livelli di tutela per garantire la continuità operativa e la *disaster recovery*. Tuttavia, il cloud è una risorsa condivisa con altri soggetti della piattaforma. Il dispositivo di conservazione e la condivisione succitate richiamano una serie di criticità in ordine alla protezione dei dati personali, all'uso e alla proprietà intellettuale. La regolazione europea in materia di protezione dei dati personali, alla luce del Regolamento UE 2016/679, potrebbe avere seri impatti con le applicazioni cloud. La normativa privacy, infatti, impone al fornitore cloud maggiore chiarezza e trasparenza in ordine alle condizioni di servizio e, contestualmente, alle aziende pubbliche. Lo chiede espressamente l'art. 28 del GDPR, ove sono tassativamente previsti una serie di compiti ai quali i *cloud provider* (responsabili del trattamento) dovranno attenersi dopo un accordo contrattuale (o *addendum* nel caso in cui il contratto di servizi produca gli effetti giuridici) e l'art. 82 del GDPR che introduce il regime di responsabilità solidale tra *controller* e *processor*, secondo un principio di accountability[407]. Il responsabile del trattamento dovrà porre in essere misure tecniche-organizzative per riconoscere prima e poi comunicare la violazione della sicurezza delle informazioni personali (c.d. data breach). Vi è l'obbligo del provider di assistere e cooperare con l'azienda cliente, titolare del trattamento, nel notificare gli eventuali data breach alle Autorità di controllo e nel comunicarli agli interessati, ove necessario. Ulteriore elemento di assoluta novità sui compiti del fornitore cloud, in qualità di responsabile del trattamento, risiede nell'assistenza tecnica che il data controller deve assicurare al titolare nella valutazione di impatto privacy (DPIA), prevista dall'art. 35 del GDPR, e nell'eventuale consultazione preventiva all'Autorità di controllo ai sensi dell'art. 36 del Regolamento UE 2016/679.

Con riferimento alla trasparenza, vengono fissate maggiori garanzie in caso del ricorso al subappalto: il contratto dovrà disciplinarlo espressamente, pena l'impossibilità del responsabile

[407] Considerando 74 Regolamento UE 2016/679. "È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

del trattamento di ricorrere a subappaltatori. Il provider dovrà, inoltre, garantire il rispetto da parte dei subappaltatori degli stessi obblighi vincolanti il titolare del trattamento, in materia di protezione dati e di sicurezza delle informazioni, conservando la responsabilità nei confronti del cliente in caso di eventuali inadempimenti della propria catena di subfornitura. Qualora il contratto autorizzi, in via generale, il provider a ricorrere al subappalto, eventuali variazioni, in ordine alla modifica o alla sostituzione di taluno dei subappaltatori, dovranno essere comunicate al cliente, al quale, in ipotesi di dissenso rispetto all'intervenuta modifica nella catena di subfornitura, dovrà essere accordata la possibilità di opporsi (Considerando 81 GDPR). Altra clausola di assoluta importanza risiede nella necessità di prevedere, all'interno dell'accordo contrattuale, l'obbligo, alla cessazione del servizio, di restituzione e/o di cancellazione dei dati personali e del relativo formato. Il GDPR attraverso l'adesione ai codici di condotta e ai meccanismi di certificazione, accentua l'attenzione nei confronti dei servizi cloud, specie qualora l'offerta sia orientata verso pratiche contrattuali trasparenti.

Altro punto importante è rappresentato dalla integrazione dei dati. In questa fase la sfida riguarda la necessità di integrare e trasformare il dato in un formato adeguato per una conseguente analisi. Tuttavia i big data sono masse di dati incredibilmente grandi, non strutturati ed eterogenei che rendono complesse sia l'integrazione che l'informazione. Le tecniche più accreditate per migliorare l'integrazione dei dati, consistono nel caricamento degli obiettivi del sistema sanitario di riferimento e, successivamente, l'individuazione del più appropriato, ed una soluzione con un approccio probabilistico, con riguardo alla relazionalità alternativa tra coppie di oggetti dello schema.

4.4.2. Case study: So.Re.Sa. S.p.A. nel procurement sanitario

Al fine di approfondire la ricerca riguardante il procurement sanitario pubblico e trasferire su un piano concreto le considerazioni tratte fino ad ora, ivi compresa la difficoltà nella realizzazione di una piattaforma *digital data* che riesca a contemperare esigenze di trasparenza con il diritto alla tutela dei dati, il presente paragrafo farà riferimento ai servizi di innovazione digitale realizzati da So.Re.Sa. (Società Regionale per la Sanità), società strumentale costituita dalla Regione Campania, col compito di gestione acquisti dei prodotti destinati alle aziende del servizio sanitario regionale, del sistema informativo sanitario regionale e delle attività di programmazione sanitaria, nonché controllo di gestione aziendale. La società si è impegnata per un ripensamento organizzativo e

strutturale della sanità regionale guidato dall'innovazione tecnologica e soprattutto volto ad un efficace utilizzo dei dati, promuovendo una sanità più moderna, che si avvale della tecnologia quale strumento per migliorare i servizi ai cittadini ed ai pazienti[408]. La valorizzazione delle risorse della Pubblica Amministrazione, compreso il patrimonio informativo, è uno dei suoi obiettivi principali, ed è realizzabile tramite l'introduzione di figure di alto profilo tecnico, distinzione delle competenze e delle responsabilità, *reskilling*, *upskilling* ed alta formazione. In occasione dei vaccini contro il Covid-19, So.Re.Sa. S.p.A. ha predisposto la piattaforma per la prenotazione, effettuando un costante monitoraggio sui flussi vaccinali erogati sul territorio regionale. È stata, inoltre, messa a disposizione dell'utenza una *app* per facilitare la visualizzazione dell'esito del tampone molecolare, sierologico o rapido[409].

Nell'ambito dell'e-procurement So.Re.Sa., con funzioni di centrale di committenza e di soggetto aggregatore della Regione Campania, nel contesto del Sistema informativo appalti pubblici in sanità (SIAPS) ha reso disponibile una innovativa piattaforma, con una distinta sezione definita mercato elettronico, utilizzabile dalle imprese per le forniture di beni e servizi di importo inferiore alla soglia di rilevanza comunitaria, ai sensi dell'art. 36 del Codice dei Contratti Pubblici (d.lgs. n. 50/2016). L'accesso al "mercato elettronico" consente la partecipazione degli operatori economici in un'ottica di massima trasparenza e nel contempo di tutela dei dati, poiché sono visibili agli utenti soltanto le informazioni strettamente necessarie, non personali, e rese pubbliche da colui che le inserisce. Un'importante novità della piattaforma di e-procurement in oggetto è l'implementazione di un algoritmo di machine learning, utilizzato in fase di valutazione economica condotta dalla stazione appaltante, il quale ha il compito di individuare offerte anomale che verranno sottoposte ad una verifica da parte di un operatore. Qualora la verifica da parte dell'uomo, condotta in merito all'anomalia riscontrata non sortisse esito positivo, l'operatore economico verrebbe escluso dalla gara[410].

[408] Nello specifico So.Re.Sa. si avvale di tecniche modernissime di intelligenza artificiale, big data analytics, machine learning basato sul riconoscimento di pattern per l'apprendimento automatico e l'utilizzo di motori semantici, e natural language processing al fine di favorire l'interazione col paziente e più in generale col cittadino.

[409] La piattaforma e l'app, denominate Sinfonia, consentono non solo la gestione delle prenotazioni al vaccino e la visualizzazione ed il download del certificato vaccinale, ma anche la visualizzazione dell'esito del tampone ed infine la consultazione in tempo reale dei dati sullo stato delle somministrazioni nella regione.

[410] Cfr. *Regolamento per la istituzione e gestione del Mercato elettronico di So.Re.Sa S.p.A.*, p. 7 ss., documento consultabile dalla pagina web: https://www.soresa.it/societatrasparente/Documents/Regolamento%20ME.PDF, e *Sistema Informativo Appalti Pubblici Sanità (SIAPS) – Manuale per operatori economici*.

Già dal 2016 So.Re.Sa., in quanto soggetto aggregatore[411], aveva sottoscritto un Protocollo di azione di vigilanza collaborativa con l'Autorità Nazionale Anticorruzione (ANAC), successivamente rinnovato, disciplinante lo svolgimento dell'attività anche preventiva "finalizzata a verificare la conformità degli atti di gara alla normativa del Codice dei Contratti Pubblici, all'individuazione di clausole e condizioni idonee a prevenire tentativi di infiltrazione criminale, nonché al monitoraggio dello svolgimento della procedura di gara e dell'esecuzione dell'appalto"[412]. Tale forma di collaborazione ha, nel presente studio, una notevole rilevanza poiché ha attribuito a So.Re.Sa. il compito di segnalare all'ANAC ricorrenti o particolari criticità tali da determinare un'attività di vigilanza ordinaria o speciale, ed in presenza di ricorrenti indici di elevato rischio corruttivo o di conflitto di interessi, di promuovere una verifica preventiva di documentazione, atti di gara ed altri provvedimenti utili all'uopo. L'accordo ha, poi, conferito all'azienda poteri di deroga al Codice dei contratti pubblici che, tuttavia, se utilizzati devono essere motivati ad ANAC. L'accordo ha impegnato, infine, So.Re.Sa. ad inserire nella documentazione di gara relativa a ciascun affidamento la clausola risolutiva espressa di cui all'art. 1456 c.c.[413] relativamente ai casi in cui nei confronti dell'aggiudicatario sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per reati di corruzione.

Con riguardo alla privacy, So.Re.Sa. S.p.A., nel pieno rispetto del Regolamento europeo n. 679 del 2016, impronta il trattamento dei dati personali alla massima riservatezza e sicurezza. I dati personali, pur se volontariamente forniti, non vengono in alcun caso comunicati o diffusi, e la loro conservazione non sarà superiore al tempo necessario agli scopi per cui essi sono stati raccolti. Quest'ultima garanzia, seppur nel rispetto del GDPR, appare in ogni caso generica e priva di qualsivoglia deterrenza, poiché per come è formulata, lascia una discrezionalità eccessivamente elevata al titolare del trattamento, con riguardo al tempo di conservazione del dato. I soggetti cui si riferiscono i dati personali devono avere in qualunque momento la possibilità di accedervi e di esercitare i diritti di cui agli artt. 15-23 del Regolamento UE 2016/679, in particolare la facoltà di

[411] La deliberazione ANAC del 23 luglio 2015 ha incluso So.re.sa. Spa nell'elenco dei soggetti aggregatori, istituito all'art. 9 comma 1 del d.l. n. 66 del 2014 convertito con legge n. 89 del 2014, "nell'ambito dell'Anagrafe unica delle stazioni appaltanti di cui all'articolo 33-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, operante presso l'Autorità".

[412] Art. 2 comma 1 Protocollo di azione di vigilanza collaborativa ANAC-So.Re.Sa. S.p.A., sottoscritto a Roma il 20 aprile del 2016.

[413] Per l'art. 1456 c.c. "I contraenti possono convenire espressamente che il contratto si risolva nel caso che una determinata obbligazione non sia adempiuta secondo le modalità stabilite. In questo caso, la risoluzione si verifica di diritto quando la parte interessata dichiara all'altra che intende valersi della clausola risolutiva".

ottenere la conferma dell'esistenza dei medesimi dati, conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, ovvero la rettifica o cancellazione. Se il diritto di accesso della persona cui si riferiscono i dati non viene soddisfatto entro tempi brevi, l'interessato potrà far valere le proprie ragioni innanzi al Garante per la protezione dei dati personali mediante apposito reclamo, ricorso o segnalazione, ovvero all'autorità giudiziaria. L'interessato ha diritto di opporsi, in qualsiasi momento, in tutto od in parte, al trattamento dei dati, revocare il consenso prestato, e nel caso in cui siano presenti le condizioni per l'esercizio del diritto alla portabilità, di ricevere in un formato di uso comune e leggibile da dispositivo automatico, i dati forniti al titolare, per poterli trasmettere ad altro titolare senza impedimenti. Quest'ultimo diritto dell'interessato, nonostante sia previsto dal GDPR, non è, tuttavia, tecnicamente attuabile in ogni situazione, poiché i dati non sempre sono strutturati e possono essere inviati nella loro completezza all'interessato. Sono, poi, adottate specifiche misure volte a garantire la sicurezza e la riservatezza dei dati, evitare la perdita, distruzione, accessi non autorizzati o trattamenti non consentiti degli stessi. In ottemperanza alle norme nazionali ed al GDPR è sempre individuato un responsabile per la protezione dei dati ed un responsabile del trattamento.

Un rischio elevato riguardo la riservatezza dei dati è rappresentato dal fatto che essi potranno essere trattati, pur se nel rispetto della normativa vigente, da società esterne, incaricate dalla So.Re.Sa. S.p.A.[414] di svolgere la manutenzione e l'assistenza delle piattaforme, delle app, ovvero dei servizi tecnologici offerti all'utenza, compreso il sito Internet. La società in parola, difatti, per effetto dell'esecuzione di specifici contratti, può demandare alcuni servizi che prevedono il trattamento di dati personali di cui è responsabile a soggetti esterni alla propria struttura. Tali società esterne sono, a loro volta, nominate quali "responsabili esterni del trattamento", considerati ai sensi dell'art. 4 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". Predette società, tuttavia, potrebbero trattare i dati personali in modo illecito diffondendoli, riutilizzandoli, ovvero alienandoli ad altre società per motivi commerciali. A tal fine So.Re.Sa. S.p.A., oltre a svolgere una funzione di controllo, inserisce nella stipulazione del contratto

[414] Il titolare del trattamento, Regione Campania, ha designato la So.Re.Sa. S.p.A. quale responsabile esterno del trattamento dei dati. Quest'ultima può a sua volta avvalersi di sub responsabili, secondo quanto previsto nell'informativa relativa al trattamento dei dati personali del progetto Sinfonia, nel pieno rispetto del Regolamento europeo del 2016.

specifiche clausole riguardanti la riservatezza ed il trattamento dei dati. Secondo la normativa vigente, il responsabile esterno del trattamento deve essere nominato con apposito contratto o atto giuridico[415], ed è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del Regolamento europeo e garantire la tutela dei diritti dell'interessato. Il responsabile esterno, inoltre, non può ricorrere ad un altro responsabile senza previa autorizzazione del titolare originario, ed in caso di autorizzazione è tenuto a nominare il subfornitore come responsabile del trattamento e ad imporgli i suoi medesimi doveri in materia di protezione dei dati personali.

Per una maggiore tutela dei dati personali, anche a livello aziendale sono state predisposte delle linee guida, in particolare: per la gestione del registro dei trattamenti; per la conduzione delle attività di *Data Protection Impact Assessment*; per le verifiche di conformità e adeguatezza; per la tutela della privacy e la gestione della sicurezza nei servizi applicativi informatizzati; per la gestione delle violazioni della sicurezza dei dati personali (data breach); per la conduzione delle verifiche di conformità e adeguatezza delle misure preposte alla tutela dei dati personali; per l'analisi periodica dell'integrità dei dati personali; per la gestione degli incidenti di sicurezza; sull'uso della crittografia, pseudonimizzazione e anonimizzazione dei dati personali. Tali linee guida sono di estrema utilità poiché, pur non avendo il potere vincolante di leggi e regolamenti, hanno una più efficace funzione di prossimità ed una diffusione capillare, potendosi altresì avvalere di controlli interni all'azienda mirati, e certamente più frequenti di quelli delle autorità istituzionali.

Particolare attenzione è rivolta alla DPIA[416], valutazione d'impatto sui dati personali, in carico al titolare del trattamento, la quale deve essere condotta ogni qualvolta sia implementato un nuovo servizio o sia impiegata una nuova tecnologia in attività di trattamento già effettuate o in nuove attività. Essa deve contenere una valutazione sulla necessità e proporzionalità dei trattamenti in relazione alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure

[415] Il contratto tra il titolare ed il responsabile esterno del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

[416] Al fine di definire le regole di riferimento finalizzate ad assicurare il rispetto delle norme in materia, a livello aziendale è stata predisposta una specifica Linea Guida in merito alla "Conduzione delle attività di Data Protection Impact Assessment".

di sicurezza previste per affrontare tali rischi garantendo costantemente la protezione dei dati personali.

In conformità all'articolo 25 del GDPR, l'azienda pone particolare attenzione a misure tecniche ed organizzative atte a proteggere i dati personali sin dalla fase di progettazione e dal momento della determinazione dei mezzi di trattamento (principio di c.d. *privacy by design*), e misure che garantiscano il trattamento, per impostazione predefinita, solo dei dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine (principio di *privacy by default*). Ciò in un'ottica di adozione di misure tecniche ed organizzative adeguate a garantire l'applicazione dei principi di protezione dei dati come impostazione di default e ad assicurare che vengano trattati solo i dati personali necessari al perseguimento delle specifiche finalità del trattamento.

Capitolo 5. Analisi comparativa fra normative europee sul conflitto di interessi

5.1. Comparazione fra Italia e Spagna nel contrasto al conflitto d'interessi

5.1.1. Il contrasto ai fenomeni corruttivi e al conflitto di interessi in Spagna

Negli ultimi anni, come l'Italia, anche la Spagna ha rafforzato la propria normativa anticorruzione, in termini di repressione ma soprattutto di prevenzione. Sebbene il Paese iberico non si avvalga di una strategia globale contro i fenomeni corruttivi, le contromisure nei confronti della criminalità organizzata, adottate nel febbraio del 2019, hanno sortito effetti positivi per ciò che riguarda l'individuazione delle situazioni di conflitto di interessi e la deterrenza nei confronti della corruzione. L'obiettivo principale prefissato è quello di migliorare la capacità d'indagine, l'accesso alle banche dati finanziarie e la cooperazione tra agenzie e soggetti istituzionali. In particolare per ciò che riguarda la cooperazione fra le autorità di contrasto alla corruzione, il GRECO (Group of States against Corruption) ha evidenziato la necessità di potenziamento del coordinamento fra polizia e guardia civile. Nonostante le recenti novelle al Codice penale e di Procedura penale, anche in materia di corruzione e reati contro la Pubblica Amministrazione, è in esame un nuovo progetto di legge che modifica ulteriormente il codice di rito. In particolare viene presa in considerazione la possibilità di lasciare la conduzione delle indagini ai pubblici ministeri, cosa che invece già avviene nel sistema penale italiano, e non più al giudice istruttore che ricoprirebbe, così, in tale fase, unicamente un ruolo di garante[417], secondo gli schemi di un sistema prevalentemente accusatorio. Nel luglio 2020 è stato novellato l'articolo 324 del codice di procedura penale spagnolo al fine di prolungare i termini per le indagini, considerati oggi troppo brevi per reati che richiedono una fase di accertamento più complessa, come quelli in materia di corruzione.

Il consolidamento spagnolo degli ultimi anni contro i fenomeni corruttivi è volto al perseguimento e all'allargamento delle ipotesi di responsabilità penale in materia di corruzione attiva e passiva nelle transazioni commerciali e alla sua prevenzione con l'arricchimento di strumenti di individuazione dei conflitti di interessi. Il quadro giuridico risulta migliorato col rafforzamento dei meccanismi di integrità del settore pubblico e potenziamento del regime relativo all'informativa

[417] Spagna, Art. 5 della legge n. 50 del 30 dicembre 1981.

patrimoniale, ai conflitti di interesse e all'incompatibilità dei funzionari nell'amministrazione statale centrale. Oltre all'estensione dei termini di prescrizione, i reati legati alla corruzione sono puniti con maggiore severità, anche per ciò che riguarda le pene c.d. accessorie, con un periodo più lungo di interdizione dai pubblici uffici. La definizione di traffico di influenza è stata modificata, e l'ambito del reato di corruzione commerciale privata è stato ampliato per includere soggetti che accettano la promessa di un beneficio o di un vantaggio. Inoltre, la responsabilità penale delle imprese è stata ampliata fino a comprendere il reato di appropriazione indebita di risorse pubbliche, e quindi ai soggetti giuridici che gestiscono risorse pubbliche o ne sono responsabili[418]. Sono state, poi, proposte modifiche legislative sulle lobby, ed un progetto di legge omnibus contro la corruzione.

Il conflitto di interessi e l'incompatibilità per gli alti funzionari pubblici e i membri del governo sono stabiliti dalla legge n. 3 del 30 marzo 2015. Già dal 1995 la legge n. 12 aveva introdotto in Spagna una novità vicina al *blind trust* del diritto nordamericano, per ciò che riguarda i conflitti di interessi delle alte cariche pubbliche. In caso di forme di partecipazione o controllo di società commerciali che emettono titoli negoziabili di valore non superiore ai 100.000 euro, l'articolo 13 della legge dispone che l'amministrazione di tali interessi debba essere delegata, a cura degli stessi interessati, ad un'entità finanziaria registrata presso la *Comisión Nacional del Mercado de Valores* per tutto il periodo della durata in carica e per i due anni successivi al termine dell'incarico. Nel 2006 è stato istituito l'Ufficio per i conflitti di interesse, ossia l'OCI ("*Oficina de Conflictos de Intereses*"), il quale ha avuto un adeguato potenziamento nel 2015. Esso agisce con piena autonomia funzionale ed è responsabile del controllo delle dichiarazioni patrimoniali, delle incompatibilità e dei conflitti di interesse delle cariche politiche, nonché della gestione del regime di incompatibilità dei dipendenti pubblici statali. Il 28 febbraio 2019 il Congresso ha approvato il codice di condotta, che disciplina il comportamento dei deputati obbligandoli ad adottare tutte le misure necessarie per evitare di trovarsi in situazioni di conflitto di interessi. Nell'aprile 2019 è stato adottato un nuovo codice etico per i membri del Parlamento, Governo ed alti funzionari, che istituisce un ufficio per il controllo e la verifica dei conflitti di interessi, il quale ha la responsabilità di verificare il contenuto delle dichiarazioni che figurano nel registro degli interessi[419]. Tra le modifiche del codice di condotta figura l'obbligo per tutti i deputati di

[418] Art. 435 della legge spagnola n. 1 del 2019.
[419] Commissione europea, Relazione sullo Stato di diritto 2020. Capitolo sulla situazione dello Stato di diritto in Spagna, Bruxelles, 30/09/2020, p. 4 ss.

pubblicare nel portale per la trasparenza del Congresso il loro programma istituzionale, comprese le riunioni con i rappresentanti di gruppi d'interesse.

Le competenze per l'attuazione di politiche anticorruzione e per l'individuazione del conflitto di interessi sono, in Spagna, suddivise tra diverse autorità di contrasto. Quelle principali sono l'Ufficio per i conflitti di interesse, istituito nel 2015, responsabile del controllo della situazione patrimoniale, ed il Consiglio di trasparenza e buon governo, istituito nel 2014, che controlla l'accesso alle informazioni e il rispetto degli obblighi in materia di trasparenza e buona amministrazione. Il perseguimento degli illeciti in materia di corruzione rientra, invece, nella giurisdizione di un organo giudiziario ad hoc: la Procura speciale contro la corruzione e la criminalità organizzata (ACPO)[420]. Oltre allo svolgimento delle indagini relative all'azione penale, l'ACPO può intervenire direttamente nei procedimenti penali per reati specifici di corruzione, quali l'appropriazione indebita di fondi pubblici, reati relativi al traffico di influenza e casi di corruzione all'estero. L'attività d'indagine è supportata dall'attività inquirente di quattro distinte unità: ispettori fiscali, responsabili del controllo, autorità di contrasto e funzionari di polizia specializzati.

5.1.2. Punti di forza e criticità del sistema spagnolo anti corruzione

La percezione della corruzione è minore in Spagna che nel nostro Paese: nell'indice di Transparency International sulla percezione della corruzione del 2021, è al trentaquattresimo posto a livello mondiale con un punteggio di 61/100, mentre l'Italia è al quarantaduesimo posto con un punteggio sensibilmente inferiore, ossia 56/100[421]. Il 94 per cento degli intervistati nell'indagine Eurobarometro 2020, considera nel Paese iberico, la corruzione diffusa, contro una media dell'Unione europea del 71 per cento, mentre il 58 per cento si sente personalmente danneggiato dalla corruzione, contro una media UE del 26 per cento. Più della metà delle imprese spagnole ritiene la corruzione un limite all'attività imprenditoriale, soprattutto in termini di mancanza di concorrenza: nello specifico il 52 per cento considera la corruzione un problema radicato nell'impresa, contro una media europea del 37 per cento. Altro dato particolarmente interessante è rappresentato dalla mancanza di fiducia nei confronti della giustizia: solo il 21 per

[420] La legge n. 10 del 24 aprile 1995 ha istituito l'ufficio del procuratore speciale per la repressione dei reati economici relativi alla corruzione.
[421] Transparency International, Indice sulla percezione della corruzione (anno 2021).

cento delle imprese ritiene che i corruttori vengano puniti in maniera adeguata e proporzionata al danno cagionato alle imprese concorrenti e al Paese.

I punti ancora da migliorare nel sistema spagnolo di contrasto alla corruzione ed al conflitto di interessi, sono da individuare, principalmente, nella necessità di rafforzare l'accesso ai dati finanziari nelle fasi antecedenti a quella giudiziaria, nonché la cooperazione ed il coordinamento tra le forze impegnate nella lotta contro la corruzione, in particolare polizia e guardia civile. Risulta, poi, ancora da rafforzare il sistema di individuazione e contrasto del conflitto di interessi, in un'ottica di prevenzione e deterrenza dei reati corruttivi. Nonostante l'inasprimento delle pene riguardanti l'interdizione dai pubblici uffici, non sono state adeguatamente considerate altre pene accessorie, utili nel contrasto ai fenomeni corruttivi, quali l'incapacità di contrattare con la pubblica amministrazione e la sospensione dall'esercizio degli uffici direttivi delle persone giuridiche e delle imprese. Per quanto riguarda la prevenzione della corruzione, a livello regionale e locale non sono disponibili specifiche strategie preventive. Il vulnus maggiore del sistema spagnolo contro corruzione e conflitto di interessi è, tuttavia, l'assenza di una normativa generale di tutela dei segnalatori di reati (c.d. whistleblower), presente in Italia già dal 2012 e potenziata nel 2017. Alcune normative settoriali spagnole offrono tutele soltanto parziali ed insufficienti ai segnalatori. Soltanto nel 2019 è stata presentata una proposta legislativa organica sulla protezione degli informatori, sul tipo di quella italiana, con l'obiettivo di colmare le carenze del sistema uniformandosi alla normativa europea.

Ciò che, invece, è stato applicato in Spagna in maniera più incisiva confronto ad altri Paesi europei, compresa l'Italia, è l'utilizzo massiccio dell'intelligenza artificiale nell'identificazione dei conflitti di interessi e della corruzione, quale valido supporto alle autorità governative nell'individuazione delle misure preventive da adottare o rimodulare. I dati personali processati sono, tuttavia, trattati nel pieno rispetto del GDPR. La protezione dei diritti fondamentali nei rapporti con l'amministrazione è garantita da autorità indipendenti, quali il "*Defensor del Pueblo*". Tale organo non riceve istruzioni da alcuna altra autorità e svolge i propri compiti in modo autonomo. Ogni anno trasmette al Parlamento una relazione sulle sue attività. In materia di trasparenza dal 2013 il governo spagnolo ha introdotto norme di amministrazione aperta allo scopo di rafforzare i legami tra cittadini e autorità e di sviluppare un dialogo permanente per coinvolgere maggiormente i cittadini nell'attuazione delle politiche pubbliche. In tale contesto, la Spagna ha

elaborato i "Piani per il governo aperto", volti a semplificare le procedure e migliorare la trasparenza e l'accessibilità alle informazioni.

Per la tutela dei dati personali, la funzione di autorità garante, analoga a quella italiana, è ricoperta dalla "*Agencia Española de Protección de Datos*". La maggior differenza nei confronti del nostro Paese, sta nel fatto che le comunità autonome dello Stato iberico possono costituire autorità territoriali indipendenti[422]. La Agencia Española de Protección de Datos viene creata con Ley Orgánica 5/1992, quale organo indipendente unipersonale, e viene configurata con Ley Orgánica 15/1999 come "ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada". L'autonomia viene in evidenza sia con riguardo alla propria indipendenza da ogni autorità pubblica o politica, sia per l'autonomia patrimoniale e di bilancio. Le funzioni dell'*Agencia* riguardano il rispetto della normativa sulla protezione dei dati ed il controllo della sua applicazione, con specifico riferimento ai diritti di informazione, accesso, rettifica, opposizione e cancellazione dei dati. I suoi poteri specifici sono: di indagine e di ispezione; sanzionatori; di risoluzione di controversie riguardanti l'inosservanza delle norme sulla protezione dei dati; potere normativo, limitato a dettare indicazioni sui trattamenti automatizzati. L'Agenzia è tenuta alla piena trasparenza delle proprie delibere e delle attività svolte, ed i suoi criteri di vigilanza e controllo devono avere massima diffusione. In particolare: risponde a richieste e reclami dei cittadini; informa i cittadini sui diritti riconosciuti; promuove campagne di divulgazione riguardanti il consenso sui dati personali; garantisce la pubblicità dei trattamenti pubblicando annualmente un elenco e mantenendo il Registro Generale della Protezione dei Dati. Rilevante è il ruolo dell'Agenzia nella produzione normativa, con particolare riguardo ai settori del commercio elettronico, delle comunicazioni, della sanità e delle assicurazioni. Ancor più importante della funzione sanzionatoria dell'Agenzia, è la funzione preventiva, che si manifesta principalmente nello svolgimento dei cosiddetti "piani ispettivi d'ufficio", attraverso i quali viene effettuato un audit del trattamento, con l'obiettivo di emettere raccomandazioni che permettano di migliorare le procedure in un determinato settore[423].

[422] Cfr., Puente A., *La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal*, Azpilicueta, 20, 2008, p. 20 "la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, prevé la existencia de la Agencia Española de Protección de Datos en su artículo 35, pero asimismo tiene en consideración el modelo autonómico consagrado en nuestra Constitución, permitiendo a las Comunidades Autónomas constituir autoridades autonómicas de control, en su artículo 41".
[423] Cfr., Puente A., id., p.28 ss.

Nel 2013 è stata approvata la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*. La legge ha posto tre obiettivi: incrementare e rafforzare la trasparenza nell'attività pubblica, mediante obblighi di pubblicità attiva per le amministrazioni; riconoscere e garantire l'accesso all'informazione; stabilire gli obblighi del buon governo che devono soddisfare responsabili pubblici e le conseguenze giuridiche derivanti dall'inosservanza di tali obblighi, con precise responsabilità per tutti coloro che svolgono attività di rilevanza pubblica. In particolare l'art. 27 della legge in parola, relativo ai reati e alle infrazioni in materia di conflitto di interessi, sancisce che l'inosservanza delle norme di incompatibilità o di quelle che disciplinano le dichiarazioni di incompatibilità, sono sanzionate in conformità a quanto disposto dalla normativa in materia di conflitti di interessi dell'Amministrazione generale dello Stato e secondo la rispettiva normativa applicabile.

5.2. Francia e Inghilterra nel contrasto al conflitto di interessi

5.2.1. Meccanismi dell'ordinamento francese per il contrasto al conflitto d'interessi

A differenza di Italia e Spagna, il legislatore francese dal 2013 ha formulato una definizione giuridica di conflitto di interessi. L'art. 2 della legge n. 2013-907 dell'11 ottobre 2013 afferma, difatti, che "costituisce un conflitto di interessi ogni situazione di interferenza tra un interesse pubblico e degli interessi pubblici o privati che è di natura tale da influenzare o da sembrare influenzare l'esercizio indipendente, imparziale e obiettivo di una funzione"[424].

La predetta legge stabilisce gli obblighi di probità ed imparzialità che è tenuto a rispettare ogni responsabile di una funzione pubblica. In particolare prescrive che ogni persona incaricata di una missione pubblica ha il dovere di evitare di porsi in una situazione di conflitto di interessi o di rimediarvi immediatamente nel caso del suo sopraggiungere. La definizione ha il merito di includere anche il conflitto apparente, in quanto vengono considerati dalla legge francese conflitti di interessi anche quelle condizioni in cui l'interferenza sembri influenzare l'esercizio indipendente di una funzione pubblica. I meccanismi di prevenzione di eventuali conflitti di

[424] Art. 2, par. 1, loi n. 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, modifié par loi n. 2017-1339 du 15 septembre 2017 "Au sens de la présente loi, constitue un conflit d'intérêts toute situation d'interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou à paraître influencer l'exercice indépendant, impartial et objectif d'une fonction".

interesse posti dalla presente legge sono applicabili a diversi soggetti: membri del Governo, loro collaboratori, membri di autorità amministrative indipendenti, dirigenti e dipendenti pubblici, ossia i *fonctionnaires de l'État*. Le novelle degli ultimi anni al codice penale francese sono orientate verso un inasprimento delle sanzioni previste per coloro che commettono il reato di "*prise illégale d'intérêts*"[425].

L'art. 432-12 del codice penale dispone che "il fatto, commesso da una persona depositaria dell'autorità pubblica o incaricata di una missione di servizio pubblico o da una persona investita di un mandato elettivo pubblico, di difendere, ottenere di tutelare, o conservare, direttamente o indirettamente, un interesse qualsiasi presso un'impresa o nell'ambito di un'operazione di cui tale persona, al momento dell'atto, è incaricata, in tutto o in parte, di assicurare la sorveglianza, l'amministrazione, la liquidazione o il pagamento, è sanzionato con una pena di detenzione fino a 5 anni e con un'ammenda fino a 500.000 euro, il cui importo può essere condotto al doppio del prodotto derivante dall'infrazione". Alla pari degli altri Paesi europei come l'Italia, la norma non punisce la situazione soggettiva di conflitto di interessi, ma il fatto giuridico di colui che, investito di una funzione pubblica, tuteli un proprio interesse a detrimento di quello pubblico. In Francia, poi, la "difesa illegale di interessi" è considerata un reato[426] anche per i titolari di funzioni pubbliche che hanno cessato il loro incarico. L'attenzione del legislatore francese nei confronti di coloro che hanno cessato un incarico pubblico, è già presente da molti anni nell'ordinamento d'oltralpe, con le norme sul divieto di pantouflage. Tale divieto è stato inserito, dopo la Convenzione delle Nazioni Unite di Merida del 2003[427], nella maggior parte dei Paesi europei, ed è presente nell'ordinamento italiano dal 2012 con la legge n. 190[428]. La regolamentazione del fenomeno del pantouflage vieta agli ex-titolari di incarichi pubblici, l'assunzione di incarichi o collaborazioni presso società sottoposte in precedenza alla loro sfera di attribuzioni[429].

Con riferimento ai dipendenti pubblici il regime delle loro incompatibilità e la prevenzione dei conflitti di interesse di cui possono risultare protagonisti, sono disciplinati dalla c.d. Loi Le Pors, legge n. 83-634 del 13 luglio 1983 "recante diritti ed obblighi dei dipendenti pubblici". Nello

[425] Difesa illegale di interessi, reato previsto e punito agli articoli 432.12 e 432-13 del codice penale francese.
[426] Previsto e punito dall'art. 432-13 del codice penale francese.
[427] Convenzione delle Nazioni Unite contro la corruzione (UNCAC), adottata dall'Assemblea generale con la Risoluzione n. 58/4 del 31 ottobre 2003 ed aperta alla firma dal 9 all'11 dicembre 2003 a Merida.
[428] La quale ha aggiunto il comma 16 ter dell'art. 53 del D.Lgs. 165/2001.
[429] Camera dei Deputati, documentazione per le Commissioni, *Conflitto di interessi e cariche di governo in Francia, Germania, Regno Unito, Spagna e Stati Uniti (A.C. 275, A.C. 1059, A.C. 1832)*, n. 7 aprile 2014, pp. 10 ss.

specifico l'art. 25 della legge del 1983 identifica le attività private che non possono essere esercitate da un dirigente o dipendente pubblico. I soggetti che ricoprono incarichi pubblici sono, poi, tenuti a presentare a l'Haute Autorité pour la transparence de la vie publique, una dichiarazione sulla situazione patrimoniale. Dal 2013[430] è stato introdotto l'obbligo di presentare all'autorità di cui sopra, anche una dichiarazione di interessi, al fine di promuovere meccanismi facilitanti la prevenzione dei conflitti di interessi e un efficace contrasto alla corruzione. Nello specifico la dichiarazione sulla situazione patrimoniale consente un controllo sui beni personali ottenuti prima e dopo l'assunzione di incarichi pubblici, al fine di valutare se i soggetti pubblici hanno usufruito della particolare posizione di potere acquisita al fine di un illecito arricchimento. La dichiarazione di interessi consente, invece, di verificare se il soggetto pubblico ha perseguito un interesse personale anteponendolo all'interesse generale, sia durante che dopo lo svolgimento di un incarico pubblico.

Tali stringenti norme contro la corruzione e il conflitto di interessi, hanno fatto sì che la Francia, abbia scalato le classifiche sulla percezione della corruzione, ponendosi nell'anno 2021 al ventiduesimo posto nella classifica mondiale, con uno score di 71/100[431].

5.2.2. Il conflitto di interessi nel sistema di common law del Regno Unito

La legge anti corruzione britannica, il Bribery Act, è considerata una delle più severe del mondo, ed ha il merito di fissare gli attuali standard per il contrasto ai fenomeni corruttivi di molti Paesi europei. Il Regno Unito, nel 2010 ha voluto, difatti, rafforzare il contrasto alla corruzione con norme esclusivamente di carattere penale non dotandosi, a differenza di altri Stati quali l'Italia e la Francia, di un corpo normativo di carattere amministrativo orientato alla prevenzione della corruzione. Le regole riguardanti il conflitto d'interessi sono, pertanto, rimaste ad un livello di codici etici e deontologici. Nel 2014, tuttavia, è stata percepita la necessità di un controllo e coordinamento nel contrasto alla corruzione, ed una strategia di intervento fondata non solo sulle sanzioni e la deterrenza, ma su una vera e propria attività di prevenzione. A tal fine è stato istituito l'Inter-Ministerial Group on Anti-Corruption, un comitato interministeriale formato da membri dell'esecutivo, direttori delle forze di polizia, tra cui il direttore del Serious Fraud Office, dal

[430] Con la Legge organica n. 2013-906 dell'11 ottobre 2013 "relativa alla trasparenza della vita pubblica", con la Legge n. 2013-907 e con decreto n. 2013-1212 del 23 dicembre 2013. I provvedimenti sono stati adottati su precisa richiesta del Presidente dell'epoca Hollande.

[431] Transparency International, Indice di percezione della corruzione, anno 2021.

Director of Public Prosecutions e dalla nuova figura dell'Anti-Corruption Champion, attivo dal luglio del 2015[432].

L'esperienza del Regno Unito nella prevenzione della corruzione è orientata verso la logica del coordinamento delle attività delle varie figure eterogenee che fanno parte dell'Inter-Ministerial Group on Anti-Corruption. A differenza del modello italiano si può riscontrare un'assenza di poteri di vigilanza diretta da parte di autorità indipendenti. Le attività di sorveglianza e controllo rimangono, difatti, prerogativa esclusiva delle forze dell'ordine, circoscritte nella logica britannica di contrasto pan-criminalistico alla corruzione. Ciò rappresenta sicuramente uno svantaggio nei confronti del sistema italiano, che con il conferimento dei poteri di controllo all'ANAC, autorità indipendente dall'esecutivo, ha risposto in maniera più decisa con le attività di prevenzione dei fenomeni corruttivi. Il modello italiano appare più incisivo ed efficiente, in quanto in grado di sommare capacità ispettive e di dialogo con istituzioni e società civile in modo indipendente, e di formare un proprio patrimonio conoscitivo a disposizione di tutte le Pubbliche Amministrazioni.

È da dire, tuttavia, che l'Italia ha dovuto affrontare il problema della corruzione in maniera più radicale nei confronti del Regno Unito. La percezione della corruzione in Gran Bretagna è, difatti, storicamente, ampiamente più contenuta che nel nostro Paese. Il fenomeno non viene considerato dai cittadini britannici, di particolare allarme sociale. L'indice di percezione della corruzione di Transparency International del 2021 vede il Regno Unito all'undicesimo posto nella classifica mondiale, con un rank di 78/100, a differenza dell'Italia, che occupa il quarantaduesimo posto, con un rank di 56/100. Il radicamento del principio della trasparenza, si fa risalire ad un rapporto Nolan Committee del 1995, ove si affermavano i princìpi di *selflessness*, stabilendo che "i detentori di cariche pubbliche devono agire solamente in nome del pubblico interesse, e non al fine di perseguire benefici economici o di altra natura per se stessi o i loro familiari o amici", di *integrity* per cui essi "non devono assumere obblighi di natura economica o di altro tipo verso persone od organizzazioni esterne che potrebbero tentare di influenzarli nello svolgimento del loro ufficio", ed infine di *honesty* per cui è previsto che chiunque ricopra uffici pubblici deve

[432] Il modello è analogo al Service Central pour la Prevention de la Corruption (SCPC), attivo in Francia fin dal 1993, competente nel coordinamento dell'attività governativa, raccolta e condivisione di informazioni, collaborazione con l'Autorità giudiziaria.

"dichiarare ogni privato interesse correlato alle loro cariche pubbliche, e di adoperarsi per risolvere ogni conflitto in maniera da tutelare l'interesse pubblico"[433].

5.3. La corruzione nei Paesi del Nord Europa

5.3.1. Il conflitto di interessi in Germania

Secondo l'indice di percezione della corruzione di Transparency International, la Germania rientra fra i Paesi più virtuosi, essendo posizionata al decimo posto nella classifica mondiale. Tuttavia le raccomandazioni contenute nel rapporto di valutazione sul Paese realizzato dal GRECO, Gruppo di Stati contro la corruzione, l'organo del Consiglio d'Europa che monitora il livello di conformità delle legislazioni dei Paesi membri agli standard anticorruzione previsti dall'organizzazione, affermano che la Germania debba adottare regole più rigide per migliorare la prevenzione del conflitto di interessi e per ottenere una maggiore trasparenza nei processi decisionali, rendendo pubbliche le ingerenze delle lobby e delle aziende e garantendo il diritto dei cittadini ad accedere a dati e informazioni riguardanti la Pubblica Amministrazione[434]. Il Paese viene, inoltre, sollecitato a rafforzare le disposizioni normative e le politiche contro corruzione e conflitto di interessi, come la Direttiva anticorruzione e il Freedom of information act (Foia), per migliorare la trasparenza nel governo. Secondo il rapporto, poi, la Germania è riuscita ad attuare solo parzialmente le raccomandazioni, rimanendo in ritardo non solo per ciò che riguarda la trasparenza, ma anche per il conflitto di interessi dei dirigenti della Pubblica Amministrazione e degli organi di governo. Gli osservatori del GRECO, sottolineano inoltre l'urgenza dell'intervento della Germania riguardo ai conflitti di interessi al termine di un incarico pubblico, col rafforzamento del *cooling off period*, periodo di tempo in cui è precluso a un ex dipendente di svolgere attività che siano in relazione nei confronti di funzioni precedentemente ricoperte.

Nonostante la Germania resti uno dei Paesi più virtuosi in materia di corruzione e conflitto di interessi, nelle ultime valutazioni il GRECO sottolinea la carenza di miglioramenti significativi per aumentare la trasparenza dei processi legislativi. Inoltre il Paese è attualmente sottoposto a una procedura di non conformità per non avere applicato le raccomandazioni riferite alla prevenzione della corruzione nei confronti dei membri del Bundestang, dei giudici e dei pubblici ministeri.

[433] First Report of the Committee on Standards in Public Life, Chairman Lord Nolan, may 1995.
[434] Quinto ciclo di valutazioni del GRECO pubblicato a dicembre 2020.

5.3.2. L'esempio virtuoso dei Paesi scandinavi

I Paesi scandinavi sono storicamente particolarmente virtuosi in materia di corruzione e conflitto di interessi. Secondo gli indici di Transparency International del 2021 Svezia e Norvegia sono appaiate al quarto posto nella classifica mondiale per ciò che riguarda la percezione della corruzione con un punteggio di 85/100, mentre la Finlandia occupa addirittura il primo posto appaiata alla Danimarca, con un punteggio di 88/100. Anche la tipologia di conflitti di interessi è differente da quella della maggior parte dei Paesi UE, poiché sono prevalenti quelli di natura non pecuniaria. La normativa in materia di corruzione e conflitti di interessi è ridotta confronto al modello italiano, per la tendenza all'autoregolamentazione e all'adozione di approcci basati su regole non vincolanti, quali codici etici e protocolli. L'Italia, al pari degli altri Paesi caratterizzati da livelli elevati di burocrazia, presenta una densità normativa sensibilmente maggiore rispetto ai Paesi nordici, contraddistinti da Pubbliche Amministrazioni impostate su modelli più manageriali e meno burocratici[435].

Il Gruppo di Stati contro la corruzione, GRECO, afferma che la Norvegia sia uno dei Paesi che ha attuato o affrontato in modo soddisfacente tutte le raccomandazioni proposte, a partire dall'anno 2014, dall'organismo stesso, risultando così un vero e proprio modello di riferimento mondiale per la prevenzione ai fenomeni corruttivi e per il contrasto al conflitto di interessi. A partire dal rapporto del 2014, difatti, la Norvegia ha introdotto linee guida etiche, elaborate con la partecipazione dei membri dello Storting (parlamento norvegese) per affrontare questioni come la prevenzione dei conflitti di interesse, l'accettazione di doni e altri vantaggi e i contatti con terze parti, compresi i lobbisti. Sono stati notevoli, inoltre, gli sforzi per potenziare ulteriormente la trasparenza e prevenire i conflitti di interesse nel Parlamento e fra i dirigenti della Pubblica Amministrazione.

Infine è da rilevare che il Codice etico del 2017 per i membri dell'autorità giudiziaria, viene ora applicato a tutti i pubblici ministeri, ed ai membri della polizia. In conclusione si può affermare che la Norvegia rappresenta il modello di riferimento per gli altri Paesi europei in materia di corruzione e conflitto di interessi e per il potenziamento della trasparenza pubblica. Sarebbe, tuttavia, ingenuo poter pensare che l'utilizzo di strumenti, regole ed organizzazioni simili anche

[435] Cfr. European Parliament, *The Effectiveness of Conflict of Interest Policies in the EU-Member States*, Policy Department for Citizens' Rights and Constitutional Affairs EN Directorate-General for Internal Policies PE 651.697 - October 2020.

in altri Paesi, possa conseguire risultati analoghi. La complessità di un problema multidimensionale di tale portata, difatti, fa sì che risulti sempre necessario considerare il tessuto sociale in cui ci si muove, l'etica della politica e di ogni amministrazione che si pongono quale esempio per i cittadini, i valori e la storia di ogni singolo territorio.

5.4. La gestione del conflitto di interessi nell'Unione europea

5.4.1. Le regole europee sulla corruzione e conflitto di interessi

La frode e la corruzione costituiscono una grave minaccia per la sicurezza e gli interessi finanziari dell'Unione europea, poiché creano incertezza tra le imprese, riducendo i livelli di investimento ed impedendo il corretto funzionamento del mercato unico, ma soprattutto minando la fiducia nei governi, nelle istituzioni pubbliche e nella democrazia in generale. La protezione di tali interessi rappresenta, pertanto, una priorità assoluta per le istituzioni dell'Unione. La corruzione, in particolare, costituisce un terreno fertile per la criminalità organizzata ed il terrorismo, gravi minacce alla libertà dei cittadini europei. La base giuridica per la lotta contro la corruzione ed ogni altra attività illecita lesiva degli interessi finanziari dell'UE è costituita dall'articolo 325 del Trattato sul Funzionamento dell'Unione Europea (TFUE)[436], che affida all'Unione e ai suoi Paesi membri il compito di proteggerne il bilancio ed in generale gli interessi finanziari. L'articolo 83 paragrafo 1 del TFUE[437] individua, poi, nella corruzione un crimine di particolare gravità che presenta una dimensione transnazionale. Negli ultimi anni le istituzioni dell'UE hanno voluto razionalizzare e

[436] Articolo 325 TFUE (ex articolo 280 del TCE) "1. L'Unione e gli Stati membri combattono contro la frode e le altre attività illegali che ledono gli interessi finanziari dell'Unione stessa mediante misure adottate a norma del presente articolo, che siano dissuasive e tali da permettere una protezione efficace negli Stati membri e nelle istituzioni, organi e organismi dell'Unione. 2. Gli Stati membri adottano, per combattere contro la frode che lede gli interessi finanziari dell'Unione, le stesse misure che adottano per combattere contro la frode che lede i loro interessi finanziari. 3. Fatte salve altre disposizioni dei trattati, gli Stati membri coordinano l'azione diretta a tutelare gli interessi finanziari dell'Unione contro la frode. A tale fine essi organizzano, assieme alla Commissione, una stretta e regolare cooperazione tra le autorità competenti. 4. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, previa consultazione della Corte dei conti, adottano le misure necessarie nei settori della prevenzione e lotta contro la frode che lede gli interessi finanziari dell'Unione, al fine di pervenire a una protezione efficace ed equivalente in tutti gli Stati membri e nelle istituzioni, organi e organismi dell'Unione. 5. La Commissione, in cooperazione con gli Stati membri, presenta ogni anno al Parlamento europeo e al Consiglio una relazione sulle misure adottate ai fini dell'attuazione del presente articolo".

[437] Articolo 83 (ex articolo 31 del TUE), paragrafo 1 "Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni. Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata".

modernizzare le norme giuridiche aventi un impatto sulla corruzione e monitorare gli sviluppi nel contrasto al conflitto di interessi nei Paesi membri mediante finanziamenti, assistenza tecnica e scambio reciproco di esperienze.

Un passo in avanti contro la corruzione è rappresentato dall'istituzione dell'Ufficio europeo per la lotta antifrode (OLAF), il quale conduce indagini amministrative indipendenti su frodi, corruzione e ogni altra attività illecita di tipo finanziario, al fine di garantire che il denaro dei contribuenti dell'UE sia utilizzato nel miglior modo possibile per la crescita dell'Unione stessa. L'OLAF ha anche il compito di indagare sugli abusi gravi ed atti corruttivi commessi dal personale e dai membri delle istituzioni dell'UE, contribuendo in tal modo a rafforzare la fiducia dei cittadini nei confronti di tali istituzioni. Un nuovo organismo col compito di indagare in materia di corruzione, riciclaggio e frodi transfrontaliere, e soprattutto perseguire e portare in giudizio i reati che ledono gli interessi finanziari dell'UE, diventato operativo dal mese di giugno del 2021 è la Procura europea (EPPO[438]). Sia le istituzioni che le persone fisiche devono segnalare alla Procura europea qualsiasi condotta criminosa a danno del bilancio dell'UE, unico organo sovranazionale che ha il potere di avviare indagini o azioni penali negli Stati membri. EPPO rappresenta un passo fondamentale nella creazione dello "Spazio di libertà, sicurezza e giustizia"[439], in un proposito di cooperazione rafforzata anche a livello giudiziario, ed integrazione giuridica fra gli Stati membri. La Procura europea ha, difatti, compiti di indagine ed azione penale a livello sovranazionale ed un trasferimento di competenze di natura giudiziaria, da organi pubblici nazionali ad un'autorità europea indipendente. Un punto fondamentale dell'EPPO per il contrasto alla corruzione e al conflitto di interessi riguarda l'interazione e la collaborazione con gli organi di supervisione bancaria e finanziaria, con particolare riguardo al ruolo che gli intermediari finanziari possono assumere come canale per commettere reati di competenza della Procura europea. A tal fine, è essenziale verificare la sussistenza di tutti gli strumenti normativi e organizzativi necessari perché lo scambio di informazioni possa avvenire in modo efficiente, e al tempo stesso con garanzie incontestabili di legalità.

In materia di conflitto di interessi, nell'ultimo decennio l'UE ha voluto rafforzare in maniera decisa la regolamentazione con la Direttiva sugli appalti pubblici 2014/24/UE del Parlamento europeo e

[438] European Public Prosecutor's Office, il cui ufficio centrale con sede in Lussemburgo, è formato da un collegio di ventidue procuratori europei, ovvero da un procuratore per ogni Paese membro che ha aderito alla EPPO.
[439] Lo "Spazio di libertà, sicurezza e giustizia" è disciplinato dagli articoli 67-89 (Titolo V, parte III) del TFUE, Trattato sul Funzionamento dell'Unione Europea.

del Consiglio, del 26 febbraio 2014, e con il Regolamento finanziario 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione[440]. Il Regolamento del 2018 si è interessato alla prevenzione ed alla gestione diretta ed indiretta dei conflitti di interessi, estendendo il campo d'azione anche alle autorità degli Stati membri ed a chiunque attui un fondo UE in regime di gestione concorrente. Con tale Regolamento le istituzioni europee sono giunte alla determinazione che i conflitti di interessi non gestiti correttamente, anche nella fase preventiva, possano incidere negativamente sul processo decisionale degli organismi pubblici, provocando una perdita di fiducia del cittadino nella capacità del settore pubblico di operare in modo imparziale e nell'interesse generale della società. La riformulazione della definizione di conflitto di interessi ne ha ampliato l'applicabilità, ricomprendendo qualsiasi interesse personale (motivi familiari, affettivi, di affinità politica o nazionale, interesse economico) diretto o indiretto che possa pregiudicare l'esercizio imparziale ed obiettivo delle funzioni. I soggetti che partecipano all'esecuzione del bilancio UE devono adottare misure atte a prevenire l'insorgere di conflitti di interessi nell'ambito delle funzioni poste sotto la loro responsabilità. Devono, inoltre, risolvere quelle situazioni che possano anche soltanto essere percepite oggettivamente come comportanti un conflitto di interessi. All'insorgenza di tali rischi, il funzionario in questione avrà l'obbligo di informare il superiore gerarchico o il delegato competente. Qualora il conflitto venga accertato, il soggetto in questione dovrà cessare ogni sua attività nella materia[441]. Un fondamentale passo avanti nei confronti del previgente Regolamento del 2012, consiste della diretta applicabilità delle nuove disposizioni in tutti gli Stati membri partecipanti all'esecuzione del bilancio UE, senza la necessità di adozione di

[440] Il Regolamento finanziario n. 2018/1046 abroga il previgente regolamento n. 966/2012.

[441] Articolo 61 Regolamento finanziario UE n.1046/2018 (Conflitto d'interessi), secondo il quale "Gli agenti finanziari ai sensi del capo 4 del presente titolo e le altre persone, comprese le autorità nazionali a tutti i livelli, che partecipano all'esecuzione in regime di gestione diretta, indiretta e concorrente del bilancio, anche per quanto riguarda i relativi atti preparatori, all'audit o al controllo, non adottano azioni da cui possa derivare un conflitto tra i loro interessi e quelli dell'Unione. Essi adottano inoltre misure adeguate a prevenire l'insorgere di conflitti d'interessi nell'ambito delle funzioni poste sotto la loro responsabilità e per risolvere le situazioni che possono oggettivamente essere percepite come comportanti un conflitto d'interessi. Laddove esista un rischio di conflitto d'interessi che coinvolga un membro del personale di un'autorità nazionale, la persona in questione ne informa il proprio superiore gerarchico. Qualora tale rischio sussista per un membro del personale statutario, la persona in questione ne informa l'ordinatore delegato competente. Il superiore gerarchico competente o l'ordinatore delegato conferma per iscritto se è accertata l'esistenza di un conflitto d'interessi. Laddove esista un conflitto d'interessi, l'autorità che ha il potere di nomina o l'autorità nazionale competente assicura che la persona in questione cessi ogni sua attività nella materia. L'ordinatore delegato o l'autorità nazionale competente assicura che sia intrapresa qualsiasi altra azione appropriata conformemente al diritto applicabile. Ai fini del paragrafo 1, esiste un conflitto d'interessi quando l'esercizio imparziale e obiettivo delle funzioni di un agente finanziario o di un'altra persona di cui al paragrafo 1 è compromesso da motivi familiari, affettivi, da affinità politica o nazionale, da interesse economico o da qualsiasi altro interesse personale diretto o indiretto".

misure nazionali di attuazione. Le autorità nazionali restano, tuttavia, competenti per l'adozione di norme nazionali complementari più dettagliate, con qualsiasi altra azione appropriata, come stabilito all'art. 61 paragrafo 2, del Regolamento.

Tutte le regole sul conflitto di interessi sono uniformate all'insegna della prevenzione, per far sì che ogni situazione a rischio venga ad essere affrontata tempestivamente prima che possa dare luogo ad atti illeciti. Tali precetti, difatti, mirano a prevenire che un soggetto si trovi in una situazione di esercizio del proprio potere che possa pregiudicarne l'imparzialità di giudizio in base ad interessi personali, privilegiando una determinata scelta piuttosto che un'altra. Ove il conflitto d'interessi dovesse concretizzarsi, l'UE ritiene necessaria una valutazione d'impatto sull'esecuzione del suo bilancio, al fine di determinare i rimedi adeguati, quali l'annullamento della procedura di aggiudicazione, il recupero dei fondi erogati, la sospensione dei pagamenti.

Il concetto di conflitto d'interessi si riferisce ai casi in cui le persone che partecipano all'esecuzione del bilancio si trovano in una delle situazioni previste all'articolo 61 del Regolamento del 2018, ossia situazioni in cui la capacità delle persone in questione di esercitare il proprio ruolo in modo imparziale e obiettivo è compromessa da motivi familiari, affettivi, da affinità politica o nazionale, da interesse economico o da qualsiasi altro interesse personale diretto o indiretto. Nel contesto delle procedure di aggiudicazione, l'articolo 61 del Regolamento finanziario del 2018 si applica agli ordinatori, ai soggetti coinvolti nella procedura di aggiudicazione, ai responsabili della stessa e a coloro che partecipano alle fasi di preparazione, apertura e valutazione. Le regole sul conflitto di interessi definite all'articolo 61 non si applicano, invece, ai partecipanti alle gare d'appalto, ossia ai candidati, agli offerenti, ovvero ai richiedenti. Per ciò che riguarda i candidati ad una gara d'appalto, difatti, i tentativi di influenzare indebitamente una procedura di aggiudicazione o di ottenere informazioni riservate dovrebbero essere trattati come illecito amministrativo o quanto meno come grave illecito professionale e comportare l'esclusione dalla partecipazione alla gara, ferma restando un'eventuale responsabilità penale. Nel contesto specifico delle procedure di aggiudicazione il Regolamento[442] distingue quattro situazioni: conflitti d'interesse diretto o indiretto, a norma dell'articolo 61; tentativi di influenzare indebitamente una procedura di aggiudicazione o di ottenere informazioni riservate; partecipazione alla preparazione dei documenti utilizzati nella procedura di aggiudicazione; interessi professionali confliggenti. È

[442] Considerando 104 Regolamento finanziario UE n.1046/2018.

necessaria una valutazione caso per caso per confermare che la situazione di conflitto d'interessi possa incidere negativamente sull'esecuzione del contratto. In caso di conferma l'offerta corrispondente è respinta. La valutazione dovrebbe includere una procedura in contraddittorio con l'operatore interessato e dovrebbe basarsi su criteri oggettivi che confermino l'interesse confliggente, nel rispetto dei principi di non discriminazione, parità di trattamento e trasparenza.

5.4.2. Omogeneizzazione degli strumenti normativi europei sul conflitto di interessi

L'Unione europea ha conferito, nell'ultimo decennio, un'importanza primaria al conflitto di interessi con l'emanazione di regole più stringenti, preoccupandosi, altresì, di promuovere un'interpretazione ed applicazione uniformi delle normative, su tutto il territorio comunitario ed in ognuno dei Paesi membri. A tal fine la Commissione europea ha pubblicato numerose comunicazioni di orientamento, chiarendo i punti più controversi o ambigui di Regolamenti e Direttive in materia di conflitto di interessi e fornendo, altresì, esempi e vademecum[443] per facilitarne la lettura ed uniformarne l'applicazione.

Bisogna aggiungere, poi, che al fine di evitare i conflitti tra le norme del diritto dell'UE e quelle nazionali, le istituzioni dei Paesi membri chiamate concretamente ad applicare il diritto o a svolgere funzioni giurisdizionali devono ricorrere all'interpretazione del diritto nazionale conforme al diritto dell'Unione. L'obbligo di interpretazione conforme al diritto dell'UE viene elaborato per la prima volta nel 1984 dalla Corte di giustizia nella causa Von Colson e Kamann[444], e introdotto nell'ordinamento dell'UE.

La trasparenza è un elemento fondamentale per prevenire i conflitti d'interessi in qualsiasi fase dell'esecuzione del bilancio dell'UE. Le istituzioni dell'Unione e le autorità nazionali, a qualsiasi livello, devono elaborare misure omogenee nell'ambito dei loro sistemi di controllo per garantire

[443] Come il vademecum sugli appalti pubblici ed il vademecum sulle sovvenzioni, documenti redatti dal Servizio finanziario centrale della Commissione, Direzione generale del Bilancio.

[444] Causa 14/83, con sentenza del 10 aprile 1984, nella quale la Corte di Giustizia ha stabilito che le giurisdizioni nazionali sono obbligate ad interpretare ed applicare le norme interne di diritto civile in modo tale da garantire un'effettiva sanzione dei trattamenti discriminatori sulla base del sesso, in conformità con le Direttive dell'Unione, e nello specifico con la Direttiva 76/207/CEE. La Corte di giustizia ha individuato il fondamento giuridico dell'interpretazione conforme al diritto dell'Unione nel principio di leale cooperazione previsto ex articolo 4, paragrafo 3, TUE, in base al quale gli Stati membri sono tenuti ad adottare ogni misura di carattere generale o particolare atta ad assicurare l'esecuzione degli obblighi derivanti dal trattato sull'Unione europea o conseguenti agli atti delle istituzioni dell'Unione. Tra questi rientra anche l'obbligo degli organi nazionali di tener conto, nell'interpretare e applicare il diritto nazionale su cui prevale quello dell'Unione, del tenore letterale e delle finalità perseguite dal diritto dell'UE.

la trasparenza e la rendicontabilità. Una delle principali finalità della comunicazione della Commissione "Orientamenti sulla prevenzione e sulla gestione dei conflitti d'interessi a norma del regolamento finanziario"[445], è di "promuovere un'interpretazione e un'applicazione uniformi delle norme sulla prevenzione dei conflitti d'interessi per gli agenti finanziari e il personale delle istituzioni dell'UE che partecipano all'esecuzione, al monitoraggio e al controllo del bilancio dell'UE in regime di gestione diretta/indiretta/concorrente".

la dichiarazione di assenza di conflitti d'interessi ed una dichiarazione relativa agli interessi attuali e passati, sono strumenti necessari in tutto il territorio UE per individuare e gestire le situazioni di conflitto d'interessi. Per ciò che riguarda gli interessi passati, essi sono pertinenti nella misura in cui la persona continua ad avere obblighi o responsabilità derivanti da posizioni o impieghi pregressi. La dichiarazione di interessi passati può essere limitata, secondo la comunicazione della Commissione, ad un periodo di cinque anni o estendersi a tutto il periodo in cui la persona continua ad avere responsabilità o obblighi relativi a tali posizioni o impieghi pregressi.

Nell'ambito degli appalti l'uniformità dell'applicazione delle regole è un principio di primaria importanza, poiché un'attuazione difforme della normativa darebbe vita a disparità di trattamento dei candidati. A tal fine è stabilito dalla Commissione[446], che le amministrazioni aggiudicatrici degli Stati membri sono tenute a rispettare i principi fondamentali del trattato in generale e il principio della parità di trattamento in particolare. Di conseguenza il principio di trasparenza si applica, in questo contesto, per garantire che possa essere accertato il rispetto del principio della parità di trattamento obbligando gli Stati membri a provvedere affinché le amministrazioni aggiudicatrici adottino misure adeguate per prevenire, individuare e porre rimedio in modo efficace a conflitti di interessi e ad evitare ogni distorsione della concorrenza[447]. Nel contesto delle procedure di aggiudicazione in cui l'UE agisce in qualità di amministrazione aggiudicatrice o di erogatore, il conflitto di interessi viene individuato uniformemente nei casi in cui i soggetti coinvolti si trovino in quelle situazioni previste dall'art. 61 RF 2018, ossia quando la capacità di esercitare il proprio ruolo in modo imparziale e obiettivo sia compromessa "da motivi familiari, affettivi, da affinità politica o nazionale, da interesse economico o da qualsiasi altro

[445] Comunicazione della Commissione n. 2021/C 121/01.
[446] Id.
[447] In applicazione dell'art. 24 della Direttiva 2014/24/UE.

interesse personale diretto o indiretto"[448]. Il riferimento ad ogni interesse diretto o indiretto rende la formulazione molto ampia, includendo anche interessi non economici, quali favori o ospitalità, ovvero derivare dal coinvolgimento in organizzazioni o doveri di lealtà di qualsiasi origine. Il concetto di conflitto di interessi, così come definito all'articolo 61 RF 2018 non si applica ai partecipanti, ossia a candidati, offerenti o richiedenti, e non deve essere utilizzato in riferimento ad essi. Situazioni specifiche che coinvolgono i partecipanti possono, invece, essere qualificate come grave illecito professionale. Sono i casi in cui il partecipante: conclude accordi con terzi allo scopo di provocare distorsioni della concorrenza; tenta di influenzare indebitamente il processo decisionale dell'amministrazione aggiudicatrice nel corso di una procedura di appalto; cerca di ottenere informazioni riservate che possano conferirgli vantaggi indebiti nell'ambito della procedura[449].

Un punto controverso, spesso interpretato in maniera non omogenea dai singoli Paesi membri, ha riguardato i conflitti di interessi derivanti da rapporti familiari, poiché i contorni della definizione di famiglia non sono universalmente riconosciuti né delimitati nella legislazione dell'UE e nessun regolamento o direttiva ha mai chiarito se il concetto di famiglia debba essere circoscritto al solo nucleo di familiari conviventi, se riguardi soltanto coniuge, ascendenti e discendenti, ovvero se debba essere considerata una più ampia nozione di famiglia allargata. A tale riguardo la comunicazione della Commissione n. 2021/C 121/01 "Orientamenti sulla prevenzione e sulla gestione dei conflitti d'interessi a norma del regolamento finanziario", ha chiarito preliminarmente che da un rapporto familiare non debba derivare automaticamente un conflitto d'interessi. Ove, invece, l'imparzialità venisse compromessa, bisogna distinguere fra rapporti familiari ed affettivi, poiché per aversi un conflitto di interessi non occorre che vi sia anche un legame affettivo tra i familiari stessi. Secondo il documento di orientamento della Commissione, i rapporti qualificabili come vincoli di appartenenza a una famiglia possono variare fra Paesi membri e devono essere analizzati nel contesto giuridico e culturale. Viene chiarito, tuttavia, che i familiari debbano comprendere, oltre al coniuge ed ai parenti più stretti, anche i collaterali fino ai cugini di primo grado, nonché affini, ossia suoceri, cognati, generi e nuore, ed

[448] Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio del 18 luglio 2018 che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012.
[449] Casi elencati all'articolo 136, paragrafo 1, lettera c), RF 2018.

infine patrigni, matrigne e figliastri. La sussistenza di uno dei suddetti rapporti familiari dovrebbe essere considerata una situazione oggettivamente percepita come un conflitto d'interessi.

Conclusioni

L'universo occulto della corruzione non consente di poter elaborare delle statistiche utilizzando dati certi ed inequivocabili. Anche le statistiche giudiziarie forniscono un quadro soltanto parziale della diffusione del fenomeno, mostrando esclusivamente la sua parte emergente, mentre quella sommersa, perciò più insidiosa, rimane ignota. Un utile indicatore per stimare la diffusione della corruzione, nonostante ovvie distorsioni della realtà[450] è, pertanto, fornito dalla sua percezione fra i cittadini. Le rilevazioni di Transparency International rappresentano un credibile strumento riguardante la percezione della corruzione. Nell'ultima rilevazione del 2021 l'Italia occupa il quarantaduesimo posto su centottanta Paesi di tutto il mondo, mentre nell'Unione europea è diciassettesima su ventisette. Il dato incoraggiante di questa rilevazione consiste nel trend positivo del nostro Paese nell'ultimo decennio[451], soprattutto grazie alle normative che dal 2012 sono divenute sempre più accurate e severe in tema di corruzione. L'introduzione di un apparato di tutele per il whistleblower e di nuove fattispecie di reato più aderenti alla realtà[452], hanno fornito validi strumenti ai fini dell'individuazione dei fenomeni corruttivi ed hanno rappresentato un efficace deterrente, poiché le probabilità di non essere perseguiti penalmente o di subire sanzioni blande, sono notevolmente diminuite. A ciò va aggiunto l'ampliamento dei poteri di vigilanza e controllo, sanzionatori e di commissariamento dell'Autorità Nazionale Anti Corruzione. L'ANAC si è mostrata, negli anni, un vero e proprio cardine per ciò che riguarda il contrasto ai fenomeni illeciti ed alle irregolarità, in particolare nel settore degli appalti pubblici. Ciò che invece è mancato nelle recenti normative anticorruzione è un adeguato potenziamento dei c.d. reati sentinella, quali l'abuso d'ufficio, il falso in bilancio e alcuni reati tributari, nei quali è, spesso, celato l'evento corruttivo.

Bisogna tuttavia sottolineare anche altri due fattori fondamentali che hanno contribuito al conseguimento di risultati positivi: un sostanziale orientamento verso la prevenzione del fenomeno tramite un approccio di tipo manageriale alla gestione dei conflitti di interessi, e

[450] Secondo Lambsdorff J. G., *How corruption in government affects public welfare – A review of theories*, Center for Globalization and Europeanization of the Economy, Göttingen, 2001, p. 2 ss., la percezione può, ad esempio, cambiare rapidamente a seguito di scandali politici.

[451] Nel 2011 l'Italia era al sessantanovesimo posto con una valutazione di 3,9 su 10, mentre in Europa era al quartultimo, davanti solo a Grecia, Romania e Bulgaria. Nel panorama mondiale ha scalato, pertanto, ben 27 posizioni in un decennio. Tale progressione non è stata eguagliata da altri Paesi negli ultimi 10 anni.

[452] Ad esempio il traffico di influenze illecite (346 bis c.p.), l'induzione indebita a dare o promettere utilità (319 quater c.p.) e l'autoriciclaggio (648 ter-1 c.p.).

l'utilizzo delle più sofisticate tecnologie informatiche di intelligenza artificiale per l'individuazione di aree e situazioni ad alto rischio. Nell'ultimo decennio l'approccio giuridico del Paese all'attività di contrasto alla corruzione è, difatti, profondamente mutato, privilegiando la prevenzione nei confronti della repressione del fenomeno. La prevenzione dei fenomeni corruttivi individua il proprio fulcro nell'emersione del conflitto di interessi. Pur non essendovi una definizione univocamente riconosciuta di conflitto di interessi, appare convincente quella proposta dall'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico), secondo la quale: "Un conflitto di interessi implica un conflitto tra la missione pubblica e gli interessi privati di un funzionario pubblico, in cui quest'ultimo possiede a titolo privato interessi che potrebbero influire indebitamente sull'assolvimento dei suoi obblighi e delle sue responsabilità pubblici". Si tratta di situazioni in grado di compromettere, anche solo potenzialmente, l'imparzialità richiesta al dipendente pubblico[453] nell'esercizio del potere decisionale, in quanto portatore di interessi della sua sfera privata che potrebbero influenzare negativamente l'esercizio imparziale e obiettivo delle sue funzioni.

Per ciò che riguarda il conflitto di interessi nello specifico settore del procurement pubblico, esso si ha quando il personale di una stazione appaltante o un prestatore di servizi che interviene nello svolgimento della procedura di aggiudicazione o può influenzarne il risultato ha, direttamente o indirettamente, un interesse personale che può essere percepito come una minaccia alla sua imparzialità e indipendenza nel contesto della procedura. Costituiscono situazioni di conflitto di interessi quelle che determinano l'obbligo di astensione previste dall'articolo 7 del decreto del Presidente della Repubblica n. 62 del 16 aprile 2013[454]. Un conflitto di interessi non adeguatamente affrontato nell'ambito di una procedura d'appalto influisce sulla regolarità della stessa e comporta una violazione dei princìpi di trasparenza e parità di trattamento che una gara ad evidenza pubblica deve rispettare. Anche un conflitto di interessi soltanto potenziale, rischia

[453] Il dipendente pubblico in conflitto di interessi può avere qualunque mansione nella Pubblica Amministrazione ed essere gerarchicamente inserito in qualunque livello dell'organigramma dell'amministrazione. Può essere in conflitto di interessi il RUP, i titolari degli uffici competenti ad adottare i pareri, le valutazioni tecniche, gli atti endoprocedimentali e il provvedimento finale.

[454] Art. 7 comma 1 DPR n. 62 del 16 aprile 2013 (Obbligo di Astensione) "Il dipendente si astiene dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri, ovvero di suoi parenti, affini entro il secondo grado, del coniuge o di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, ovvero, di soggetti od organizzazioni con cui egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito significativi, ovvero di soggetti od organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di enti, associazioni anche non riconosciute, comitati, società o stabilimenti di cui sia amministratore o gerente o dirigente. Il dipendente si astiene in ogni altro caso in cui esistano gravi ragioni di convenienza. Sull'astensione decide il responsabile dell'ufficio di appartenenza.

di violare i princìpi di integrità ed imparzialità del processo decisionale dell'amministrazione, con una perdita di fiducia del cittadino nei confronti di quest'ultima, e conseguente danno di immagine.

L'utilizzo della tecnologia ed in particolare dei big data analytics in tale ambito, deve essere considerato come una grande opportunità e non come una minaccia, poiché permette di individuare aree di concentrazione di conflitti di interessi e a rischio di fenomeni corruttivi, e risolvere tali conflitti con una strategia di prevenzione. Perché non sia percepito come una minaccia, l'utilizzo dei big data per l'individuazione di situazioni anomale, le c.d. red flag, deve avvenire sempre nel pieno rispetto dei diritti umani e della privacy. Per ciò che riguarda i diritti umani è necessario tenere costantemente in considerazione la Costituzione repubblicana del nostro Paese e le convenzioni sovranazionali, in particolare la Convenzione Europea dei Diritti dell'Uomo. Con riguardo alla privacy è necessario, invece, un contemperamento di interessi, ossia l'esigenza dualistica di prevenire la corruzione tramite l'individuazione del conflitto di interessi, senza tuttavia comprimere in maniera eccessiva il diritto alla tutela dei dati personali. Il GDPR del 2016 ha un ruolo primario nel diritto di ogni individuo alla tutela dei propri dati, in quanto fissa delle regole a livello europeo, in difesa del diritto alla privacy contemperandolo con l'esigenza di trasparenza, ponendo altresì un limite alla valenza delle decisioni automatizzate.

Le nuove tecnologie hanno cambiato la vita di ogni essere umano, migliorandone la qualità, ma nel contempo hanno fatto sorgere problematiche etico-giuridiche non indifferenti[455]. Fra le innovazioni degli ultimi anni, in particolare, i big data analytics costituiscono una delle opportunità più rilevanti, se non rivoluzionarie, in campi quali la ricerca scientifica, l'offerta di beni e servizi, la medicina, assumendo anche un ruolo sociale nella trasmissione della conoscenza[456]. L'intelligenza artificiale e le tecniche di machine learning[457] unitamente all'utilizzo dei big data consentono, a differenza del passato, di assemblare grandi quantità di dati eterogenei provenienti da fonti profondamente differenti, analizzarle e correlarle celermente generando modelli predittivi in grado di comprendere combinazioni di valori da cui estrapolare previsioni e scenari estremamente precisi. È, tuttavia, necessaria una selezione e riordino dell'enorme quantità di dati

[455] Biancardo A., *Problematiche etico giuridiche relative all'utilizzo dell'intelligenza artificiale in ambito sanitario*, Jus, 30 giugno 2021.
[456] Secondo un recente studio di IDC (International Data Corporation) le informazioni digitali prodotte nel mondo raddoppiano ogni due anni, con un trend di crescita stimabile in 50 volte nei prossimi 10 anni.
[457] Il machine learning è stato definito da Arthur Samuel "la scienza che mette i computer in grado di imparare, senza essere stati esplicitamente programmati per questo".

per poter creare interpretazioni affidabili, poiché l'utilizzo non controllato dei big data e dei modi automatizzati per analizzarli[458], può presentare criticità nella trasmissione del sapere che viene prodotto, esponendo i destinatari dell'informazione a rischi legati all'uso distorto dei dati.

È da considerare attentamente anche un'altra questione. I modelli predittivi automatizzati più moderni sono spesso generati da una black box algoritmica, nel senso che i dati risultanti non sono associati alle logiche interne utilizzate dal sistema per elaborarli. In definitiva quando si utilizzano algoritmi c.d. *logic learning machine*, le logiche utilizzate dal modello predittivo sono generalmente ignote anche allo sviluppatore stesso dell'algoritmo, poiché il software effettua i suoi calcoli autonomamente in assenza di intervento umano basandosi sulle conoscenze pregresse, senza fornire la spiegazione dei passaggi dei calcoli e delle analisi per cui è giunto a quel determinato risultato. Il GDPR, Regolamento UE 2016/679, richiede che qualsiasi decisione frutto di modelli predittivi o derivante da un algoritmo di machine learning che possa avere delle implicazioni legali nei confronti di una persona, debba avere anche una spiegazione esplicita. Secondo il GDPR infatti: "le persone hanno il diritto di non essere soggette a decisioni basate esclusivamente su processi automatizzati"[459] e "i processi decisionali completamente automatizzati dovrebbero essere soggetti a salvaguardie, che dovrebbero includere informazioni specifiche da fornire alla persona interessata e al suo diritto di ottenere un intervento umano, di esprimere il suo punto di vista e di ottenere una spiegazione della decisione presa – in base a quali valutazioni – e di poter quindi contestare tale decisione"[460]. Non esiste una risposta sulla pericolosità reale o presunta relativa ad un'intelligenza artificiale che si possa sostituire alle decisioni umane, tuttavia dal GDPR traspare l'idea di una tecnologia che aiuti l'uomo nelle sue decisioni, ma non lo sostituisca mai completamente, lasciando a quest'ultimo un potere di vigilanza e di controllo, connotato da una flessibilità decisionale e una discrezionalità che la decisione automatizzata non può avere. Per ciò che riguarda, nello specifico, l'utilizzo dei big data a fini predittivi in Italia, lo scrivente non rileva, tuttavia, particolari pericoli derivanti dall'automatizzazione dei processi, poiché i dati estrapolati vengono elaborati unicamente al fine di una vigilanza più stretta in determinati ambiti o su determinati soggetti, e non implicano

[458] Cfr. Musacchio N., Guaita G., Ozzello A., Pellegrini M.A., Ponzani P., Zilich R., De Micheli A., *Intelligenza Artificiale e Big Data in ambito medico: prospettive, opportunità, criticità*, in *JAMD* vol. 21-3, ottobre 2018, p. 205, secondo cui "Il nuovo paradigma di una scienza che "simula il ragionamento umano" ha instillato dubbi sul fatto che questo fenomeno sia sotto il controllo umano".
[459] Art. 22 par. 1 GDPR.
[460] Art. 22 par. 3 GDPR.

decisioni giudiziarie o che possano in alcun modo limitare la libertà di una persona fisica. È, certo, sempre necessario un accurato controllo degli algoritmi e delle tecnologie di machine learning che possano in alcun modo violare il principio di eguaglianza o, peggio i diritti inviolabili dell'uomo tutelati rispettivamente dagli articoli 3 e 2 della Costituzione e dalle più importanti carte sovranazionali dei diritti umani, ma è questo, almeno nel nostro Paese, un rischio oggettivamente remoto.

Proprio per sfruttare al meglio le opportunità offerte dalla c.d. data revolution, anche in occasione della definizione dei nuovi Sustainable Development Goals[461], si è cercato di creare un clima di maggior fiducia negli utilizzatori di dati al fine di condividere le tecnologie e le innovazioni per il bene comune, organizzando e sviluppando piattaforme di analisi che utilizzino strumenti avanzati per esplorare i dati ed erigere un blocco di informazioni facilmente comprensibili, ma che nel contempo tutelino i diritti dell'uomo e preservino il dato da distorsioni e bias. Il rispetto dei diritti viene, pertanto, sempre tutelato, non solo a livello giudiziario, ma anche da parte di comitati etici e codici di comportamento e deontologici, nonché con l'individuazione di nuovi soggetti responsabili riguardo il trattamento e l'utilizzo delle informazioni. Tale sviluppo delle strategie per la valorizzazione dei dati nel rispetto dei diritti e soprattutto nella tutela dei dati personali legittima nuove figure professionali, quali il *chief data officer*, responsabile della governance dei dati dell'organizzazione anche nel settore pubblico.

L'attendibilità delle informazioni dei big data deve essere attentamente valutata. La problematica più rilevante riguarda l'interpretazione soggettiva, poiché il centro del processo di comprensione può passare attraverso l'identificazione di correlazioni false, distorsioni ed ambiguità semantiche. Il risultato estratto da un complesso di dati può essere fortemente minato dalle c.d. availability bias, cioè giustificazioni o teorizzazioni ex post del risultato dell'analisi data driven. I dati in rete devono, poi, essere contestualizzati temporalmente e nell'ambito in cui sono stati raccolti. Se i dati vengono ridotti ad un mero modello matematico, facilmente perderanno il loro contesto e quindi la loro validità. Tutto ciò oltre a creare dei potenziali pericoli, rischia di inficiare l'affidabilità del dato estratto e la riuscita delle strategie predisposte per ogni singolo scenario vagliato. Al fine

[461] I Sustainable Development Goals, definiti anche come Agenda 2030, sono una serie di obiettivi interconnessi, definiti dall'ONU come strategia "per ottenere un futuro migliore e più sostenibile per tutti", e ratificati da tutti i Paesi membri, poiché propongono sfide comuni a vantaggio di tutta l'umanità (salute, ambiente, energia sostenibile, giustizia, ecc.).

di ottenere risultati attendibili e strategie valide per l'amministrazione nell'ambito del conflitto di interessi nel procurement, è pertanto necessario:

a. un controllo continuo delle procedure riguardanti i big data, non solo da parte di autorità indipendenti, ma da parte dell'amministrazione e degli stessi utenti;
b. un confronto serrato con i comitati etici;
c. il rispetto pedissequo dei codici di comportamento da parte del personale;
d. una formazione continua in materia di tecnologia, digitalizzazione e big data.

Nel campo sanitario il conflitto di interessi ha provocato uno spreco di denaro, nonché tagli orizzontali della spesa pubblica, con una conseguente riduzione dei servizi offerti al paziente. Oltre alla necessità di rendere trasparenti le procedure e l'utilizzo delle risorse pubbliche, la soluzione può trovarsi nei maggiori controlli su spese e appalti, promozione della legalità e dell'etica per il personale sanitario, accreditamento delle strutture private in funzione dell'effettiva attività, aumento della concorrenza fra le case farmaceutiche, promozione sempre più ampia del whistleblowing, rispetto del divieto di pantouflage, distinzione chiara fra sanità pubblica e privata, modifica delle regole di finanziamento della spesa sanitaria, prevenzione del rischio di infiltrazioni criminali negli appalti.

Nel procurement pubblico le problematiche affrontate fino ad ora vengono ulteriormente amplificate, stante il ruolo primario, in tale ambito, ricoperto dalla trasparenza e dalla concorrenza, e la contemporanea esigenza di tutelare la privacy e i dati personali dei soggetti coinvolti nelle procedure di aggiudicazione, sia in qualità di candidati che di pubblici amministratori. Gli effetti positivi delle strategie preventive sul conflitto di interessi, predisposte grazie all'utilizzo dei big data e l'ausilio delle tecnologie di intelligenza artificiale, sono ormai irrinunciabili in un Paese come l'Italia, ove la maladministration ha raggiunto livelli elevatissimi e il conflitto di interessi e la corruzione rappresentano un vero e proprio fenomeno sociale, capillarmente diffuso ed endemico. Per non perdere quanto fino ad ora si è fatto, e per continuare lungo un sentiero virtuoso di riallineamento con gli altri membri dell'UE, è necessario potenziare la rete di controlli effettuati tramite l'incrocio di grandi quantità di dati ed incrementare ulteriormente i poteri di autorità indipendenti che possano verificare la regolarità delle procedure. Ma la verifica deve anche provenire dal basso, ossia dagli stessi concorrenti della procedura di aggiudicazione e da qualsiasi cittadino. Ciò è possibile soltanto con una maggiore

diffusione di piattaforme integrate, delle quali, oggi, se ne sono finalmente comprese le potenzialità. La questione più complessa resta, comunque, il contemperamento di esigenze di trasparenza con quelle riguardanti la tutela del dato personale. A prescindere dai dati aggregati, liberamente utilizzabili poiché alcun pericolo sorge rispetto al dato personale, il GDPR sembra aver individuato un buon compromesso fra trasparenza e protezione dei dati, predisponendo dei livelli minimi di tutela, riguardanti in particolare l'anonimizzazione, pseudonimizzazione, cancellazione e conservazione dei dati. Bisogna, tuttavia, avere la consapevolezza che qualunque norma, nonché le restrizioni dettate in materia di privacy non potranno pienamente difenderci dall'utilizzo non etico dei nostri dati da parte di coloro che ne hanno accesso. A tal fine è d'uopo ricordare che il commercio dei dati è ormai da anni una realtà, e la proprietà della maggior parte di essi è nelle mani di poche società private, colossi mondiali che non hanno alcun obbligo nel renderli disponibili.

I passi avanti degli ultimi anni per ciò che riguarda l'individuazione ed il contrasto del conflitto di interessi nel procurement pubblico sono notevoli. Ciò grazie alle normative che dal 2012 hanno cercato di combattere in maniera più incisiva la corruzione sul piano della prevenzione, ed alle tecnologie di intelligenza artificiale che hanno permesso di incrociare grandi quantità di dati per individuare campanelli d'allarme e situazioni anomale negli appalti. Diverse sono, tuttavia, le strade che possono essere seguite per contrastare in maniera ancor più netta le illegalità ed i conflitti di interessi, in un'ottica di trasparenza e pari opportunità dei concorrenti di una gara ad evidenza pubblica. Ciò non solo per un principio di eguaglianza di accesso ai vantaggi offerti dalla Pubblica Amministrazione, ma di efficienza ed efficacia stessa di quest'ultima, nel rispetto del principio di accountability. Tuttavia è necessario evitare di incorrere nell'errore di fondare i sistemi di supporto decisionale soltanto sull'analisi predittiva e le decisioni normative solo su metriche di performance, ma ogni scelta dovrebbe essere ponderata a più livelli di professionalità ed utilizzati strumenti di confronto multidisciplinari.

In tale ottica si può concludere osservando che gli strumenti più validi e moderni per un contrasto ancor più marcato alle situazioni di conflitto di interessi, senza intaccare i diritti della persona e la tutela dei dati personali, sono rappresentati dall'utilizzo sempre maggiore di piattaforme pubbliche integrate contenenti severe policy di consultazione stratificata, delle tecnologie blockchain e degli open data, ed una contemporanea maggior selezione della massa di dati eterogenei e non strutturati provenienti dalla rete. Tale selezione per l'individuazione dei fattori

di rischio inerenti al conflitto di interessi, dovrà essere effettuata in due fasi: una prima automatizzata per creare un blocco strutturato di dati utili, fruibili e possibilmente senza distorsioni, ed una successiva selezione posta in essere dall'uomo, che si possa concentrare sul controllo di situazioni ad elevato rischio di violazione dei diritti umani o di tutela del dato personale. L'attività di controllo dei dati e degli algoritmi che li processano deve essere sempre possibile da parte di ogni soggetto pubblico o privato, nonché da parte di autorità indipendenti, e non deve in alcun modo essere negata, in ossequio alle disposizioni del GDPR. Solo nel rispetto di tali regole le nuove tecnologie potranno continuare a rappresentare uno strumento di trasparenza ed eguaglianza, e non di derive antidemocratiche e di compressione dei diritti umani. L'impianto normativo dovrà, infine, continuare ad essere orientato verso un'ottica di prevenzione alla corruzione, di esclusione da ogni procedura per coloro che si trovino in situazioni di conflitto di interessi, di pieno rispetto del GDPR, con l'attribuzione di maggiori poteri e un'indipendenza ancora più ampia degli organi di controllo, ed uno spazio ancora maggiore e ben delineato per gli atti di soft law, in particolare i codici di comportamento, le linee guida e gli smart contract.

Bibliografia

- AA.VV. del Centro di ricerca coordinato – Studi sulla Giustizia, Giurisprudenza Univ. degli Studi di Milano, a cura di Sacchi R., *Conflitto di interessi e interessi in conflitto in una prospettiva interdisciplinare*, Editore Giuffré Francis Lefebvre, 2021.
- AA.VV., *Libro bianco sulla corruption in sanità*, in *ISPE-Sanità (Istituto per la Promozione sull'Etica in Sanità), 2014*.
- AA.VV., *La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal*, Azpilicueta, 20, 2008, pp. 13-41.
- AA.VV., a cura di Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, Giappichelli, 2019.
- AA.VV., a cura di Studio legale Mondini-Rusconi, *Big Data: privacy, gestione, tutele*, Altalex Editore, 2018.
- AA.VV., *Corruzione e sprechi in sanità*, progetto di Transparency International Italia, a cura di RISSC, in collaborazione con ISPE Sanità.
- AA.VV., *Legislazione anticorruzione e responsabilità nella pubblica amministrazione*, Cerioni F. - Sarcone V. (a cura di), Giuffré Francis Lefebvre, 2019.
- AA.VV., *Anticorruzione: il conflitto di interessi va dimostrato concretamente*, in *Enti locali online*, febbraio 2020.
- AGCOM, *Big data - Interim report*. *Indagine conoscitiva di cui alla delibera n. 217/17/CONS*, giugno 2018.
- AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, indagine avviata congiuntamente da: AGCM con provv. n. 26620 del 30 maggio 2017; AGCOM con delibera n. 217/17/CONS; Garante, sulle determinazioni adottate nell'adunanza collegiale dell'11 maggio 2017.
- Alanazi H.O., Abdullah A.H., Qureshi K.N., Ismail A.S, *Accurate and dynamic predictive model for better prediction in medicine and healthcare*, in *Irish Journal of Medical Science*, maggio 2018.
- Aliprandi S. (a cura di), *Il fenomeno open data. Indicazioni e norme per un mondo di dati aperti, Ledizioni*, 2014.
- Alongi A., Pompei F., *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Tab, 2021.

- Alpa G., Spangher G., *La nuova disciplina dei delitti di corruzione - Profili penali e processuali (L. 9 gennaio 2019, n. 3 c.d. 'spazzacorrotti')*, a cura di Flora G. e Marandola A., Pacini Giuridica, Pisa, 2019.
- Amatucci F., Mele S., *I processi di acquisto di beni e servizi nelle aziende sanitarie. Elementi di innovazione e modelli di accentramento*, II edizione, Egea, 2016.
- ANAC, *La Corruzione in Italia – Numeri, luoghi e contropartite del malaffare*, 2019, nell'ambito del progetto Misurazione del rischio di corruzione a livello territoriale e promozione della trasparenza, PON "Governance e Capacità Istituzionale 2014-2020".
- Atti G., La quarta rivoluzione industriale: verso la supply chain digitale. Il futuro degli acquisti pubblici e privati nell'era digitale, Franco Angeli Editore, 2018.
- Babuta A., *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*, in *Royal United Services Institute for Defence and Security Studies*, 2017.
- Babuta A., *Pseudomysation is likely to be the only way to perform big data analytics on personal datasets while complying with data protection law*.
- Bacci A., *Lean healthcare management*, Ipsoa, 2017.
- Baldassarre F., Labroca A.S., *Public procurement. Gli acquisti pubblici fra vincoli giuridici e opportunità gestionali*, Franco Angeli Editore, 2013.
- Balestreri A., Venanzi D., Conflitti di interessi e finanza. Come individuarli e prevenirli, McGraw-Hill Editore, gennaio 2021.
- Banta D., *What is technology assessment?*, in *International Journal Technology Assessment Health Care*, 2009, n. 25 suppl. 1.
- Battaglini R., Giordano M.T., *Blockchain e smart contract*, Giuffré, 2019.
- Battiston S., *Smart city public procurement. Percorso operativo attraverso il Codice dei contratti pubblici*, Giappichelli Editore, 2021.
- Beaglehole R., *Public health in the new era: improving health through collective action. The Lancet*.
- Beam A.L., Kohane I.S., *Big Data and Machine Learning in Health Care*, in *JAMA (Journal of the American Medical Association)*, 2018, 319:1317-1318.
- Bernasconi A., Codenotti B., Resta G., *Metodi matematici in complessità computazionale*, Springer, 1999.

- Berrettini A., *Conflitto d'interessi e contratti pubblici: un difficile equilibrio tra (in)certezza del diritto e tassatività delle situazioni conflittuali*, in *Federalismi.it*, 8 luglio 2020.
- Bertocchini A., Giachi A., Tronu P., *Il procurement pubblico del digitale: dal planning all'execution*, Promo PA Fondazione di Anitec-Assinform, ottobre 2021.
- Bincoletto G., *La Privacy by Design: un'analisi comparata nell'era digitale*, in *The Trento Law and Technology Research Group*, paper n. 35.
- Birritteri E., *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri (Análisis de Big Data y compliance anticorrupción Cuestiones críticas de la práctica actual y escenarios futuros),* in *DPC*, 2/2019, pp. 289 ss.
- Boccaccini P., *Anonimizzazione e pseudonimizzazione: potenzialità, rischi e punti di attenzione*, in *Cybersecurity 360*, novembre 2021.
- Bolognini L. (a cura di), *Privacy e libero mercato*, Giuffré, 2021.
- Bonfanti A., *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws - Rivista di diritto dei media*, 3/2018.
- Borsari R., *La corruzione pubblica. Ragioni per un cambiamento della prospettiva penale*, G. Giappichelli Editore, 2020.
- Brioschi C.A., *La corruzione. Una storia culturale*, Guanda, 2018.
- Bustin G., *Accountability: The Key to Driving a High-Performance Culture*, 2014.
- Buttarelli G., *Le sfide dei Big Data tra evoluzione tecnologica, etica e interessi collettivi*, in *Gnosis*, n. 2, 2017, pp. 31-39.
- 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*, *Rivista di diritto dei media* Rivista, 2/2018.
- Califano L., *Privacy: affermazione e pratica di un diritto fondamentale*, Collana Crispel, 2016.
- Canonico P., Tomo A., Hinna A., Giusino L. (a cura di), *La digitalizzazione della Pubblica Amministrazione*, Egea Editore, gennaio 2022.
- Cantone R., *Il sistema della prevenzione della corruzione in Italia*, in *Diritto penale contemporaneo*, 27 novembre 2017.
- Cantone R., Merloni F., *Codice dell'anticorruzione e della trasparenza*, Maggioli, 2018.
- Capparelli O., Lanzino L., *Modelli di gestione del rischio e compliance ex d.lgs. 231/2001*, Wolters Kluwer, ottobre 2016.

- Cardetta A., *Il legame big data – intelligenza artificiale nel contrasto alla corruzione*, 2019. https://www.ictsecuritymagazine.com/articoli/il-legame-big-data-intelligenza-artificiale-nel-contrasto-allacorruzione/
- Caringella F., *Manuale dei contratti pubblici. Principi e applicazioni*, Dike giuridica, ottobre 2019.
- Carloni E., *I codici di comportamento*, in *Il lavoro nelle pubbliche Amministrazione*, riv. trim., Giappichelli, 2017.
- Carney G., *Working Paper, Conflict of interest: Legislators, Minister and Publical Officers*, in www.trasparency.org, 1998.
- Cartabellotta N., *Diritto alla salute e riforma del Titolo V*, in *Salute Internazionale*, 13 maggio 2015.
- Cartolano P., *Il conflitto di interessi rilevante nel settore degli appalti pubblici*, in *Mediappalti*, 12 ottobre 2020.
- Cascavilla A., Galli G., *La blockchain: possibili utilizzi per l'efficienza delle pubbliche amministrazioni*, in *Osservatorio CPI*, Univ. Cattolica del Sacro Cuore di Milano, 5 marzo 2020.
- Cassese S., *"Maladministration" e rimedi*, in *Il Foro Italiano*, 1992.
- Cassiani O., *La gestione del rischio in sanità. Processo sistematico di identificazione, valutazione e trattamento dei rischi attuali e potenziali*, Edizioni Accademiche Italiane, febbraio 2017.
- Cataleta A., *Gestire i limiti del GDPR per costruire il futuro della società digitale*, in *Agenda Digitale*, 04/03/2021.
- Cavallo Perin R. (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, in *Quaderni del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino*, 2021.
- Cavicchi I., *Il medico tra due conflitti: l'economia che determina e la società determinante*, in *Annuario Italiano Med. Int.*, 17 (suppl. 1), 2002.
- Cavicchi I., *Implicazioni della neutralità tra scienza ed economia*, in *Annuario Italiano Med. Int.* 18 (suppl. 1), 2003.
- Ciclosi F., *La protezione dei dati e la gestione del rischio nella pubblica amministrazione*, Pigliapoco S. (a cura di), Maggioli, 2019.
- Cingari F., *Repressione e prevenzione della corruzione pubblica. Verso un modello di contrasto "integrato"*, G. Giappichelli Editore, Torino, 2012.

- Cirillo A., *La sfida del procurement pubblico: stare al passo con le imprese*, in *A.D.*, procurement dell'innovazione, 18 febbraio 2019.
- Colangelo R., *Una visione sistemica del procurement pubblico*, in *Contributo per la definizione del progetto laboratorio MAAP*, Milano 2018.
- Commissione europea, *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, 2011.
- Conio P., *Digitalizzazione dei contratti pubblici: cosa prevede il Decreto 148/2021 e cosa manca per una reale attuazione*, in *ForumPA*, 12 novembre 2021.
- Contessa C., Ubaldi A., *Manuale dell'anticorruzione e della trasparenza*, La tribuna, 2021.
- Corradino M., Galli D., Gentile D., Lenoci M.C., Malinconico C., *I contratti pubblici*, Ipsoa, 2017.
- Costantino F., *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Diritto pubblico*, Il Mulino, 1/2019.
- Cristea Uivaru L., *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*, Barcelona, 2018, pp. 44 ss.
- Crocetti E., *Percezione dell'esistenza di un conflitto di interessi in chi opera in strutture di sanità pubblica*, in E&P, gennaio-febbraio 2019.
- Crawford K., *The Hidden Biases in Big Data. Harvard Business Review*, disponibile in: https://hbr.org/2013/04/the-hidden-biases-in-big-data, 01 aprile 2013.
- Cuccuru P., *Blockchain e automazione contrattuale. Riflessioni sugli smart contract*, in *La nuova Giurisprudenza Civile Commentata*, 2017.
- Cucumile P., *Il trattamento dei dati sensibili alla luce del principio di trasparenza, del C.A.D. e del GDPR. Il necessario bilanciamento degli interessi nel rapporto tra la normativa sulla trasparenza amministrativa e quella posta a tutela dei dati personali. Le modifiche normative e gli interventi dell'Autorità Garante*, in *Cammino Diritto*, n. 11/2018.
- Cuffaro V., D'Orazio R., Ricciuto V., *I dati personali nel diritto europeo*, Giappichelli, 2019.
- D'Acquisto G., Naldi M., Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza, Giappichelli, 2017.
- D'Agostino L., *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101*, in *Archivio penale*, n. 1, 2019, pp. 1-58.
- D'Angelo G., *Conflitto di interessi ed esercizio della funzione amministrativa*, G. Giappichelli Editore, 2020.

- Dal Pozzo F.R., *La tutela dei dati personali nella giurisprudenza della Corte di giustizia*, in Eurojus, 2018, Relazione tenuta al I convegno annuale dell'Associazione italiana studiosi di diritto dell'Unione europea (AISDUE), Roma, 26-27 ottobre 2018.
- Davidoff F., De Angelis C.D., Drazen J.M., Hoey J., Højgaard L., Horton R., Kotzin S., Nicholls M.G., Nylenna M., Overbeke A.J., Sox H.C., Van Der Weyden M.B., Wilkes M.S., *Sponsorship, authorship, and accountability*, in *Lancet*; 358, 2001.
- Davigo P.C., *Il sistema della corruzione*, Laterza, 2007.
- Davigo P.C., Mannozzi G., *La corruzione in Italia. Percezione sociale e controllo penale*, Laterza, 2017.
- De Mauro A., *Big Data Analytics. Analizzare e interpretare dati con il machine learning*, Apogeo, 2019.
- Della Morte G., *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale Scientifica, 2018.
- Della Porta D., *La corruzione come sistema. Meccanismi, dinamiche, attori*, Il Mulino, 2021.
- Della Torre G., *Politica e amministrazione della spesa pubblica: controlli, trasparenza e lotta alla corruzione*, Atti del LIX convegno di studi di scienza dell'amministrazione, Giuffré, anno 2014.
- De Nicola A., Rotunno I., *Il Whistleblowing*, Cons. dir. AODV, luglio 2019.
- De Nictolis R., *Gli appalti pubblici dell'emergenza sanitaria*, Zanichelli Editore, 2021.
- De Robbio A., *Dati aperti nella pubblica amministrazione tra crescita e trasparenza*, DigitaliaWeb, Rivista del digitale nei beni culturali, 2013, p.38 ss.
- Di Carlo E., *Il conflitto di interessi nelle aziende. Linee guida per imprese, amministrazioni pubbliche e non-profit*, G. Giappichelli Editore, 2020.
- Di Gennaro G., Lombardo E., Riccio G., Ruffolo U., Uricchio A.F., *Intelligenza artificiale e politiche di sicurezza urbana: verso quali modelli?*, Cacucci editore, 2020.
- Di Paola N., *Blockchain e supply chain management*, CEDAM, 2018.
- Di Rienzo M., Ferrarini A., *L'uso degli scenari nella valutazione dei conflitti di interessi potenziali*, in *Spazioetico*, 2020.
- Di Rienzo M., Ferrarini A., *La gestione del conflitto di interessi nei contratti pubblici*, in *Spazioetico*, marzo 2021.
- Di Rienzo M., Ferrarini A., *La valutazione del conflitto di interessi nella gestione dei contratti pubblici – Due casi di studio*, in *Azienditalia*, maggio 2019.

- Di Sangro M.V., *Public procurement in sanità. Criticità e sfide per un futuro resiliente*, in *ICom*, 3 giugno 2021, consultabile alla pagina web https://www.i-com.it/2021/06/03/public-procurement-sanita.
- Eri O., *E-procurement e gestione della catena di approvvigionamento*, Edizioni Sapienza, agosto 2021.
- European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*.
- Fabiano N., *GDPR e privacy. Consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity*, goWare, maggio 2019.
- Falcone M., *Big Data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista trimestrale di diritto pubblico*, n. 3, 2017, pp. 601-639.
- Falcone M., *La big data analytics per conoscere, misurare e prevenire la corruzione*, in *Gnaldi M. - Ponti B.*, Milano, Franco Angeli, 2018, pp. 90-110.
- Ferguson A., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, NY Pr, 2017.
- Ferragina P., Luccio F., *Il pensiero computazionale. Dagli algoritmi al coding*, Il Mulino, dicembre 2017.
- Fiorentino L., La Chimia A.M. (a cura di), *Il procurement delle pubbliche amministrazioni tra innovazione e sostenibilità*, Il Mulino, aprile 2021.
- Foà S., *La nuova trasparenza amministrativa,* in *Diritto Amministrativo*, fascicolo 1, 2017.
- Formici G., *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Giappichelli Editore, 2021.
- Foglia Manzillo F., *Modelli sanzionatori nel rischio conflittuale. Dal conflitto all'interferenza di interessi*, Edizioni Scientifiche Italiane, 2020.
- Fraschini G., Parisi N., Rinoldi D., *Il whistleblowing. Nuovo strumento di lotta alla corruzione*, II edizione, Bonanno, Roma, 2011.
- Gaffuri F., *Il conflitto di interessi nell'esercizio del potere amministrativo*, G. Giappichelli Editore, 2018.
- Gallone G., *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Diritto dell'economia*, 3/2019.

- Garante per la protezione dei dati personali, *Big data e privacy. La nuova geografia dei poteri*, atti del convegno 30 gennaio 2017, Garante della privacy, Servizio relazioni esterne e media (a cura di).
- Garofoli R., *La nuova disciplina dei reati contro la P.A.*, in *D.P.C.*, 2012.
- Giambelluca A., *Procurement sanitario: gli insegnamenti da trarre dopo la pandemia*, in *Policy and procurement in healthcare*, 1 novembre 2021.
- Giribaldi D., *Discriminazione algoritmica. Intelligenza artificiale, tutti i pregiudizi (bias) che la rendono pericolosa*, in *Agenda Digitale*, 26 febbraio 2019.
- Giunta F., *Il conflitto d'interessi nel campo medico: dal controllo penale al dovere di trasparenza*, in *Dir. penale e processo*, 2004.
- Graffuri F., *Il conflitto di interessi nell'esercizio del potere amministrativo*, G. Giappichelli Editore, 2018.
- Gramunt Fombuena M.D., *El tratamiento de la información genética en la Ley de Investigación Biomédica, in Protección de datos personales en la sociedad de la información y la vigilancia*, 2011, pp. 176-186.
- Grupo de trabajo del artículo 29*, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 679/2016*, adoptado el 28 de noviembre de 2017 (17/ES, WP 259).
- Guaineri R., *La nuova legge inglese anticorruzione (Bribery Act 2010)*, in *Diritto Penale Contemporaneo*, 15 aprile 2011.
- Guccione C., *I requisiti degli operatori economici*, in *Giornale di diritto amministrativo*, aprile 2016.
- Guzzo A., *Data breach nel GDPR: cos'è e come fare segnalazione e prevenzione*, in *Agenda Digitale*, 28 maggio 2018.
- Hansen M.M., Miron-Shatz T., Lau A.Y., Paton C., *Big Data in Science and Healthcare: A Review of Recent Literature and Perspectives*. Contribution in *IMIA Social Media Working Group. Yearb Med Inform*, 21-6-2014.
- Health Equality Europe, edizione italiana La Torre G., Monteduro A., Kheiraoui F. (a cura di), *Comprendere l'Health Technology Assessment (HTA)*, Editore Prex s.p.a., 2009.
- Iaselli M., *L'e-procurement. L'acquisizione di beni e servizi della P.A. nel quadro del piano di e-government*, Liguori Editore, 2005;
- Iaselli M., *La tutela dei dati personali in ambito sanitario*, Giuffré Francis Lefebvre, 2020.

- Interlandi M., *Il nuovo codice dei contratti pubblici nella prospettiva dell'e-procurement*, in *Gazzetta Amministrativa*, n. 1, 2018.
- IOM (Institute of Medicine), *Conflict of interest in medical research, education, and practice*, Washington, DC, The National Academies Press, 2009.
- Kossow N., Dykes V., *Blockchain, bitcoin and corruption. A review of the linkages*, in *Transparency International Anti-Corruption Helpdesk Answer*, 22 january 2018.
- Kraft T.J., *Big Data Analytics, Rising Crime, and Fourth Amendment Protections*, *in University of Illinois Journal of Law, Technology & Policy*, 2017, pp. 249 ss.
- Kremer J., *The end of freedom in public places? Privacy problems arising from surveillance of the European public space*, Univ. Helsinki, 2017.
- Lacava C., *I criteri di aggiudicazione*, in *Giornale di diritto amministrativo*, 4/2016.
- Lalli A., Moreschini A., Ricci M., *L'ANAC e la disciplina dei conflitti di interessi*, working paper 3, Edizioni Scientifiche Italiane.
- Lenzer J., *Big data's big bias: bringing noise and conflicts to US drug regulation*, in *BMJ (British Medical Journal)*, 2017, 358:j3275.
- Livelli F.M.R., *Piattaforme di public procurement, come garantire la sicurezza nei processi d'acquisto*, in *Agenda Digitale*, 21 dicembre 2021.
- Lombardi D., Pioggia A., *La prevenzione della corruzione nel conferimento degli incarichi in ambito sanitario*, 2015.
- Lombardo E., *Intelligenza Artificiale e Human Intelligence per prevenire i crimini*, Società Italiana Intelligence, 2020.
- Lorè F., *Il trattamento dei dati personali nella pubblica amministrazione tra Open data, Big Data e privacy*, in *Ratio Iuris*, 07/2019.
- Lubrano E., *Il conflitto di interessi nell'esercizio dell'attività amministrativa*, Giappichelli Editore, 2018.
- Lucca M., *Il conflitto di interessi del progettista e della stazione appaltante nell'area a rischio "Contratti Pubblici"*, in *Appalti & Contratti*, novembre 2021.
- Lugmayr A., Stockleben B., Scheib C., Mailaparampil M. (2017), *Cognitive big data: survey and review on big data research and its implications. What is really "new" in big data?*, in *Journal of Knowledge Management*, 21(1).
- Lynskey O., *Criminal justice profling and EU data protection law: precarious protection from predictive policing*, in *International Journal of Law in Context*, n. 15, 2019, pp. 162-176.

- Lysons K., Farrington B., *Procurement and supply chain management*, Pearson Ed. Limited, febbraio 2020.
- Maglio M., *Manuale di diritto alla protezione dati personali*, Maggioli Editore, 2017.
- Malem Segna J.F., *Globalizzazione, commercio internazionale e corruzione*, Il Mulino 2004.
- Malavasi M., *La regolamentazione dei flussi informativi nel Modello Organizzativo ex d.lgs. 231/2001*, in *La Responsabilità Amministrativa delle Società e degli Enti*, 2010, vol. I.
- Manca F., Angius E.D., *Management e performance nella sanità pubblica*, Ipsoa, 2018.
- Marchetta C., *La legislazione italiana sul conflitto di interessi. La legge 20 luglio 2004, n.215. Orientamenti applicativi, criticità e prospettive di riforma*, Giuffré, 2013.
- Martella A., Campo E., Ciccarese L., *Gli algoritmi come costruzione sociale. Neutralità, potere e opacità*, in *The Lab's Quarterly*, n. 4/2018.
- Massaro A., Sorbello P., Giraldi A., Grossi L., Notaro L., *Intelligenza artificiale e giustizia penale*, dicembre 2020.
- Mattarella B.G., *Disciplina dei contratti pubblici e prevenzione della corruzione*, Atti del sessantunesimo Convegno di Studi Amministrativi, Varenna, 2015;
- Merloni F., *La nuova disciplina degli incarichi pubblici*, in *Giornale Diritto Amministrativo*, 2013, p. 8 ss.
- Merloni F., *I piani anticorruzione e i codici di comportamento*, in *DPP*, 2013, 8S, 4 ss.
- Milanovic M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Era*, in *Harvard International Law Journal*, 2015, p. 56 ss.
- Monteduro F., Brunelli S., Buratti A., *La corruzione. Definizione, misurazione e impatti economici*, Formez PA, Gangemi Editore, Roma, marzo 2013.
- Morabito C., *La chiave del crimine*, in *Polizia Moderna*, luglio 2015.
- Moses L.B., Chan J., *Algorithmic Prediction in Policing. Assumptions, Evaluation, and Accountability*, in *Policing and Society*, 2016.
- Musacchio N., Guaita G., Ozzello A., Pellegrini M.A., Ponzani P., Zilich R., De Micheli A., *Intelligenza Artificiale e Big Data in ambito medico: prospettive, opportunità, criticità*, in *JAMD* vol. 21-3, ottobre 2018, p. 204 ss.
- Nicoletti B., *Procurement 4.0 e trasformazione digitale*, Franco Angeli, 2019.
- Nicotra I.A., *L'autorità nazionale anticorruzione tra prevenzione e attività regolatoria*, Giappichelli Editore, 2016.

- Nicotra I.A., *Il conflitto di interessi come declinazione del principio costituzionale d'imparzialità*, in *Rivista Associazione Italiana Costituzionalisti*, n. 3/2020, pubblicato il 25/06/2020.
- Nino M., *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, 2013.
- Nuccio M.R., *Conflitto di interessi e autonomia negozi*ale, E.S.I. 2016.
- Orefice M., *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, 2018.
- Ottolia A., *Big Data e innovazione computazionale*, Torino, Giappichelli, 2017.
- Pagliarin C., Laimer S., Perathoner C. (a cura di), Contratti pubblici e innovazione, Giuffrè Editore, luglio 2021.
- Pajno A., *La nuova disciplina dei contratti pubblici tra esigenze di semplificazione, rilancio dell'economia e contrasto alla corruzione*, in *Rivista italiana diritto pubblico com.*, fascicolo 5, 2015.
- Parrotta A., Razzante R., *Il sistema di segnalazione interna. Il whistleblowing nell'assetto anticorruzione, antiriciclaggio e nella prevenzione da responsabilità degli Enti*, Pacini Giuridica, 2019.
- Patroni Griffi F., *Gli strumenti di prevenzione nel contrasto alla corruzione*, in *Federalismi*, 14/2014.
- Pedreschi D., Giannotti F., Guidotti R., Monreale A., Pappalardo L., Ruggieri S., Turini F., Open the Black Box. Data-Driven Explanation of Black Box Decision Systems, in *ArXiv Preprint*, n. 1/2018.
- Pellissero M., *La nuova disciplina della corruzione tra repressione e prevenzione*, in *La legge anticorruzione*, Torino, 2012.
- Perry W.L.,Price C.C., McInnis B., Smith S.C., Hollywood J.S., *Predictive Policing. The role of crime forecasting in the law enforcement operations*, RAND corporation, 2013.
- Pertici A., Trapani M. (a cura di), *La prevenzione della corruzione. Quadro normativo e strumenti di un sistema in evoluzione, Atti del convegno, Pisa, 5 ottobre 2018*, G. Giappichelli Editore, aprile 2019.
- Pintus E., *Il procurement nelle aziende sanitarie pubbliche*, Gruppo di studio Astrid coord. Fiorentino L., 2019.
- Pitaro V., *Using Data Analytics to Boost Compliance Program Efectiveness*, in *The Anti-corruption Report* (www.anti-corruption.com), v. 7, n. 13, june 2018.

- Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.
- Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.
- Pizzetti F., *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli Editore, 2021.
- Pizzorno A., *La corruzione nel sistema politico,* 1992, Bologna, il Mulino, p. 13 ss.
- Pizzuti P., *Whistleblowing e rapporto di lavoro*, Studi di diritto del lavoro, G. Giappichelli Editore, dicembre 2019.
- Polidoro D., *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio Penale*, n. 3/2020.
- Pope J., *Confronting corruption: The elements of a national integrity system, Transparency International Source Book*, TI, 2000.
- Puente A., *La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal*, Azpilicueta, 20, 2008.
- Quattrocolo S., *Artificial intelligence, Computational Modelling and Criminal Proceedings – A framework for a european legal discussion*, Springer, 2020.
- Rausand M., Haugen S., *Risk Assessment. Theory, methods and applications*, Wiley, 22 aprile 2020.
- Recuero Linares M., *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*, Madrid, 2019.
- Resta E., *Gli appalti in house. Il caso delle sanità service*, Cacucci, 2018.
- Rivoiro C., Dirindin N., *Il ruolo del conflitto di interessi nella tutela della salute*, Paper for the Espanet Conference "Sfide alla cittadinanza e trasformazione dei corsi di vita: precarietà, invecchiamento e migrazioni", Università degli Studi di Torino, Torino, 18 - 20 settembre 2014.
- Rizzo S., Serravalle L., Lucchini G., Silvi R., Visani F., *La gestione degli acquisti. Strategia, implementazione, controllo*, Hoepli, 2010.
- Rugani A., *I profili penali del whistleblowing alla luce della l. 30 novembre 2017 n. 179,* in *Legislazione penale,* 2018.
- Russo T., Oriolo A., La lotta alla corruzione nella legalità reticolare. Il sistema penale multilivello, F. Angeli Editore, 2022.

- Saleem T.J., Chishti M.A*., Big data analytics for Internet of things*, Wiley, edizione in inglese, 2021.
- Salomone G., Conflitto di interessi e pubblica amministrazione: il divieto di pantouflage, Editore DBI, 2021.
- Santosuosso A., *Intelligenza artificiale e diritto*, Mondadori Università, 2020, p. 99 ss.
- SceMaps (State Capture Estimation and Monitoring of Anticorruption Policies at the Sectoral level) – Analytics and data, https://scemaps.eu.
- Sciarrone R., *Politica e corruzione. Partiti e reti di affari da Tangentopoli a oggi*, Donzelli, 2017.
- Seaver N., *Algorithms as culture: some tactics for the ethnography of algorithmic systems*, in *Big Data & Society*, N. 4/2017.
- Selvaggi N., *Compliance, sicurezza informatica e nuove tecnologie*, relazione Congresso dell'Associazione Internazionale di Diritto Penale – *Gruppo Italiano su "Nuove tecnologie e giustizia penale. Problemi aperti e future sfide"*, Teramo, 22-23 marzo 2019.
- Serrano Pérez M.M., *Salud pública, epidemiología y protección de datos*, et. al. *Tratado de derecho sanitario*, 2013. Vol. II, pp. 1091-1113.
- Severino P., *Legalità, prevenzione e repressione nella lotta alla corruzione*, in *Archivio Penale*, n. 3, 2016, pp. 1-8.
- Severino P., *Strategie di contrasto alla corruzione nel panorama interno e internazionale*, Luiss Open, 29 marzo 2019.
- Smith R., *Conflitto di interessi in medicina e nelle riviste mediche*, in *Focus - Bollettino di farmacovigilanza*, novembre 2002.
- Soffiantini M. (a cura di), *Privacy. Protezione e trattamento dei dati*, Ipsoa, 2016.
- Storto A., Bolognino D., Bonura H., *I contratti pubblici dopo la conversione del decreto Sblocca Cantieri*, Editore La Tribuna, 2019.
- Stroud M., *Official Police Business: Does predictive policing actually work? Crime forecasting tools are taking off, but good data is hard to find*, in *The Verge*, maggio 2016.
- Tartaglia Polcini G., *La corruzione tra realtà e rappresentazione*, Minerva, Bologna, 2018.
- Tayebi M.A., Glässer U., *Social network analysis in predictive policing*, Springer, 2016.
- Tea A., *La tutela per chi segnala illeciti e irregolarità nel rapporto di lavoro*, in *Diritto e pratica del Lavoro*, n. 46, 2017.

- Tescaroli L., *La cd. legge spazzacorrotti: analisi e problematiche delle novità sostanziali e processuali della legge n. 3 del 2019*, in *Questione giustizia – magistratura democratica*, settembre 2019.
- Thompson D.F., *Understanding financial conflicts of interest*, in *New England Journal of Medicine*, 1993.
- Thompson D.F., *Restoring responsibility: ethics in government, business and healthcare*, Cambridge U.K., 2005, Cambridge University Press, pp. 290 ss.
- Thompson J.D., *Organization in action*, 2009.
- Tortora A., *La prevenzione della corruzione. Un sistema in continua,* Giappichelli, 2018.
- Tosi E., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019.
- Transparency International Italia, *Linee guida per la predisposizione di procedure in materia di whistleblowing*, 2016.
- Transparency International Italia, *Direttiva europea sul whistleblowing 1937/2019. Analisi e raccomandazioni di Transparency International Italia*, 2021.
- Trapani M., *La prevenzione e il controllo della corruzione e dell'etica pubblica mediante l'utilizzo delle nuove tecnologie*, in *Forum di Quaderni Costituzionali*, 15 aprile 2018, pp. 1-13.
- Troncoso Reigada A., *Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, Leioa: UPV/EHU y Dykinson, n. 49, 2018, pp. 187-266.
- Tsarapatsanis D. - Preoţiuc-Pietro D. – Lampos V. – Aletras N., *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ computer science*, ottobre 2016.
- Ubaldi A., *Whistleblowing: aggiornate le Linee Guida ANAC*, in *Il Quotidiano Giuridico*, 12 luglio 2021.
- Valeriani E., *Public procurement. Mercato, comportamenti, contratti e conflitti*, Istituto Editoriale Cisalpino, dicembre 2013.
- Vannucci A., *Come combattere la corruzione in Italia?*, in *Quaderni di Sociologia*, 2019.
- Vannucci A., *La sicurezza nell'integrità. Politiche anticorruzione, maladministration e tutela dei diritti*, in *SINAPPSI - Connessioni tra ricerca e politiche pubbliche*, n. 2/2020.

- Vannucci A., Della Porta D., *La corruzione come sistema. Meccanismi, dinamiche, attori*, Il Mulino, 2021.
- Venturi M., *KeyCrime. La chiave del crimine*, in *Profiling*, 14/01/2010.
- Watcher S., Mittelstadt B., *A right to Reasonable Inferences: Re-Tinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2019, fasc. 2, pp. 24 ss.
- Weigel U., Reucker M., *The strategic procurement practice guide*, Springer, 2018.
- Wolfe S., Worth M., Dreyfus S., Brown A.J., *Whistleblower Protection Laws in G20 Countries - Priorities for Action*, 2014.
- Zeno-Zencovich V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *La rivista di diritto dei media*, 2018, fasc. 2, pp. 1-7.
- Ziccardi G., *Crittografia e pseudonimizzazione nel GDPR*, ipsoa.it, 17 marzo 2018.
- Zwiebel M., *Measuring Compliance: Gathering and Analyzing Data*, in *The Anti-corruption Report (www.anti-corruption.com)*, v. 6 n. 18, september 2017.

Fonti normative, giurisprudenziali, convenzioni, atti

- Costituzione repubblicana art. 24;
- Costituzione repubblicana art. 32;
- Costituzione repubblicana art. 97;
- Costituzione repubblicana art. 117;
- Legge n. 241 del 7 agosto 1990, “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”;
- Legge n. 20 del 14 gennaio 1994 “Disposizioni in materia di giurisdizione e controllo della Corte dei conti”;
- Legge n. 145 del 15 luglio 2002, “Disposizioni per il riordino della dirigenza statale e per favorire lo scambio di esperienze e l'interazione tra pubblico e privato”;
- Legge n. 215 del 2004, “Norme in materia di risoluzione dei conflitti di interessi”;
- Legge n. 124 del 23 luglio 2008 (c.d. Lodo Alfano), “Disposizioni in materia di sospensione del processo penale nei confronti delle alte cariche dello Stato”;
- Legge n. 116 del 3 agosto 2009, “Ratifica ed esecuzione della Convenzione dell’Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell’ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale”;
- Legge n. 51 del 7 aprile 2010 (c.d. legittimo impedimento), “Disposizioni in materia di impedimento a comparire in udienza”;
- Legge n. 110 del 28 giugno 2012, “Ratifica ed esecuzione della Convenzione penale sulla corruzione, fatta a Strasburgo il 27 gennaio 1999”;
- Legge n. 190 del 2012 (c.d. legge Severino), “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione”;
- Legge n. 124 del 7 agosto 2015, “Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche”;
- Legge n. 167 del 20 novembre 2017 (c.d. legge europea 2017), recante “Disposizioni per l’adempimento degli obblighi derivanti dall’appartenenza dell’Italia all’Unione europea”;
- Legge n. 179 del 30 novembre 2017, recante “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato”;

- Legge n. 3 del 2019 (c.d. Spazzacorrotti), “Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici”;
- Codice dell’Amministrazione Digitale (CAD), d.lgs. n. 82 del 7 marzo 2005, modificato e integrato con d.lgs. n. 179 del 22 agosto 2016 e con d.lgs. n. 217 del 13 dicembre 2017;
- Codice penale art. 314;
- Codice penale art. 317;
- Codice penale art. 318;
- Codice penale art. 319;
- Codice penale art. 319 ter;
- Codice penale art. 319 quater;
- Codice penale art. 320;
- Codice penale art. 321;
- Codice penale art. 322;
- Codice penale art. 323;
- Codice penale art. 323 ter;
- Codice penale art. 346 bis;
- Codice di procedura penale art. 266;
- Codice di procedura penale art. 329;
- Codice di procedura penale art. 407;
- D.lgs. n. 165 del 2001, “Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche”;
- D.lgs. n. 61 dell’11 aprile 2002, “Disciplina degli illeciti penali e amministrativi riguardanti le società commerciali, a norma dell’articolo 11 della legge 3 ottobre 2001, n. 366”;
- D.lgs. n. 196 del 30 giugno 2003, c.d. Codice in materia di protezione dei dati personali;
- D.lgs. n. 109 del 30 maggio 2008, “Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE”;
- D.lgs. n. 235 del 31 dicembre 2012, “Testo unico delle disposizioni in materia di incandidabilità e di divieto di ricoprire cariche elettive e di Governo conseguenti a sentenze definitive di

condanna per delitti non colposi, a norma dell'articolo 1, comma 63, della legge 6 novembre 2012, n. 190";

- D.lgs. n. 33 del 2013 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle Pubbliche Amministrazioni";
- D.lgs. n. 39 dell'8 aprile 2013, recante "Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190";
- D.lgs. n. 50 del 18 aprile 2016 (c.d. Codice dei contratti pubblici);
- D.lgs. n. 97 del 25 maggio 2016 (c.d. Freedom of Information Act);
- D.lgs. n. 51 del 18 maggio 2018, 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 o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- D.lgs. n. 101 dell'8 agosto 2018, recante "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)";
- D.l. n. 44 del 31 marzo 2005, convertito con modificazioni dalla legge 31 maggio 2005, n. 88;
- D.l. n. 138 del 2011, convertito con modificazioni dalla legge 14 settembre 2011, n. 148;
- D.l. n. 90 del 24 giugno 2014, convertito con modificazioni dalla legge 11 agosto 2014, n. 114;
- D.l. n. 32 del 2019 (c.d. Sblocca cantieri) convertito in legge n. 55 del 2019;
- D.l. n. 34 del 19 maggio 2020 (c.d. decreto Rilancio) convertito in legge n. 77 del 17 luglio 2020 recante misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19;
- D.l. n. 77 del 31 maggio 2021, "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure";
- D.l. n. 132 del 30 settembre 2021 convertito in legge n. 178 del 23 novembre 2021;
- D.l. n. 139 del 2021 (c.d. Decreto Capienze);
- D.P.R. n. 62 del 16 aprile 2013;

- Decreto ministeriale n. 148 del 12 agosto 2021;
- Dichiarazione Universale dei Diritti dell'Uomo, art. 12;
- Carta dei diritti fondamentali dell'Unione europea, art. 8;
- Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali (CEDU);
- Convenzione ONU contro la corruzione del 31 ottobre 2003 (c.d. Convenzione di Merida);
- Convenzione penale contro la corruzione del Consiglio d'Europa del 27 gennaio 1999 (c.d. Convenzione di Strasburgo);
- GDPR - General Data Protection Regulation, 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, approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
- Direttiva 95/46/CE "regolamento generale sulla protezione dei dati";
- Direttive comunitarie 2014/23/UE, 2014/24/UE e 2014/25/UE;
- Direttiva europea 2016/680, 27 aprile 2016, 4 maggio 2016;
- Direttiva europea 2016/1148, 6 luglio 2016;
- Direttiva UE n. 1937 del 23 ottobre 2019, riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione".
- Direttiva UE n. 2019/1024 del 20 giugno 2019;
- Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE;
- Parlamento europeo, Risoluzione del 20 novembre 2002, paragrafo 38;
- Parlamento europeo, Risoluzione del 3 ottobre 2018 sulle "tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione";
- Parlamento europeo, Report on fundamental rights implications of big data: privacy, data protection, non discrimination, security and law-enforcement, 2016/2225(INI), Committee on Civil Liberties, Justice and Home Affairs, 20 febbraio 2017;
- Parlamento europeo, Risoluzione del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL));

- Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", Strasburgo, 28 gennaio 1981, modificata dal Trattato del Consiglio d'Europa n. 223, Strasburgo, 10 ottobre 2018 (c.d. Convenzione 108+);
- Commissione europea, Relazione sullo Stato di diritto 2020. Capitolo sulla situazione dello Stato di diritto in Spagna, Bruxelles, 30/09/2020;
- Raccomandazione OCSE [C(2017)140];
- Corte costituzionale, sentenza n. 103 del 2007;
- Corte costituzionale, sentenza n. 161 del 2008;
- Corte costituzionale, sentenza n. 23 del 22 febbraio 2019;
- Corte costituzionale, sentenza n. 20 del 23 gennaio 2019;
- Cassazione sez. lavoro, sentenza n. 11015 del 2017;
- Cassazione penale, sez. VI, 31 gennaio-27 febbraio 2018, sentenze n. 9041 e 9047;
- Cassazione penale, sez. V, sentenza n. 35792 del 2018;
- Cassazione, sentenza n. 5741 del 13 febbraio 2020;
- Consiglio di Stato, sez. IV, n. 3649 del 2000;
- Consiglio di Stato, sez. III, sentenza n. 355 del 14 gennaio 2019;
- Consiglio di Stato, Sez. cons. atti norm., n. 667 del 5 marzo 2019;
- Consiglio di Stato, sentenza n. 2270 del 08 aprile 2019;
- Consiglio di Stato, sez. III, sentenza n. 6150 del 12 settembre 2019;
- Consiglio di Stato, sez. V, sentenza n. 7389 del 28 ottobre 2019;
- Consiglio di Stato, sez. V, 14 maggio 2020, n. 3048.
- Consiglio di Stato, sez. III, sentenza n. 5151 del 20 agosto 2020;
- Tribunale di Bologna, sez. Lavoro, CGIL contro Deliveroo, ordinanza 31 dicembre 2020;
- Corte europea dei diritti dell'uomo, Szabadságjogokért vs. Hungary, 14 April 2009;
- Corte europea dei diritti dell'uomo, S. and Marper vs. the United Kingdom, ric. 30562/04 e 30566/04 del 2008;
- CGUE, Corte di giustizia UE, causa Digital Rights Ireland (CGUE C-293/12);
- CGUE, Corte di giustizia UE, Tele2 Sverige AB c. Postoch telestyrelsen, C-203/15, 21/12/2016;
- CGUE, Corte di giustizia UE, causa C-582/14, Patrick Breyer c. Bundesrepublik Deutschland, 2016;

- CGUE, Corte di giustizia UE, Grande Sezione, sentenza del 13 maggio 2014, causa C-131/12, Google Spain e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González;
- CGUE, Corte di giustizia UE, sentenza del 2 marzo 2021, causa C-746/18, H.K. contro Prokuratuur;
- CGUE, Corte di giustizia UE, cause riunite C-203/15 e C-698/15;
- Corte Suprema del Wisconsin, 13 luglio 2016, State o Wisconsin vs. Eric L. Loomis;
- ANAC - Autorità Nazionale Anticorruzione, Aggiornamento 2015 al Piano Nazionale Anticorruzione, Determinazione n. 12 del 28 ottobre 2015;
- ANAC - Autorità Nazionale Anticorruzione, Delibera numero 75/2013 Linee guida ANAC;
- ANAC - Autorità Nazionale Anticorruzione, Delibera n. 88 dell'8 febbraio 2017;
- ANAC - Autorità Nazionale Anticorruzione, Delibera dell'8 marzo 2017;
- ANAC - Autorità Nazionale Anticorruzione, Delibera n. 358 del 29 marzo 2017 "Linee Guida per l'adozione dei Codici di comportamento negli enti del Servizio Sanitario Nazionale".
- ANAC - Autorità Nazionale Anticorruzione, Delibera n. 469 del 9 giugno 2021 "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)";
- ANAC - Autorità Nazionale Anticorruzione, linee guida per l'adozione dei Codici di comportamento nel SSN, approvate in data 20 settembre 2016.
- ANAC - Autorità Nazionale Anticorruzione, Delibera Linee guida ANAC n. 15 del 5 giugno 2019;
- Circolare n. 1 del Dipartimento della Funzione Pubblica del 25/01/2013;
- Ministero della Giustizia, Circolare del 7 dicembre 2020 - Responsabile della prevenzione della corruzione e della trasparenza - Tutela del dipendente pubblico che effettua segnalazioni di illeciti o irregolarità nell'interesse dell'integrità della pubblica amministrazione, ai sensi dell'art. 54-bis del d.lgs. n. 165/2001 (cd. whistleblowing);
- AGCOM, Big data - Interim report. Indagine conoscitiva di cui alla delibera n. 217/17/CONS, giugno 2018;
- Garante per la Protezione dei Dati Personali, Parere sullo schema di "Linee guida - La Sicurezza nel procurement ICT" predisposto da AgID - n. 16 del 30 gennaio 2020 [9283857];
- Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015 [3881513];
- Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. del 10 giugno 2021, Registro dei provvedimenti n. 234;

- CEPEJ (Council of Europe, European commission for the efficiency of justice, “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment”, Strasburgo, 3-4 dicembre 2018;
- Comitato nazionale di bioetica, 2006, Conflitti di interesse nella ricerca biomedica e nella pratica clinica, Presidenza del Consiglio dei Ministri, 8 giugno 2006.

La borsa di dottorato è stata cofinanziata con risorse del
Programma Operativo Nazionale Ricerca e Innovazione 2014-2020 (CCI 2014IT16M2OP005),
Fondo Sociale Europeo, Azione I.1 "Dottorati Innovativi con caratterizzazione Industriale"

UNIONE EUROPEA
Fondo Sociale Europeo

Ministero dell'Istruzione, dell'Università e della Ricerca